HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Konfigurationsleitfaden
HiLCOS Rel. 9.12

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (*www.hirschmann.com*.)

Hirschmann Automation and Control GmbH

Stuttgarter Str. 45-51

Deutschland

72654 Neckartenzlingen

Tel.: +49 1805 141538

Rel. 9.12 - 05/16 – 10.5.16

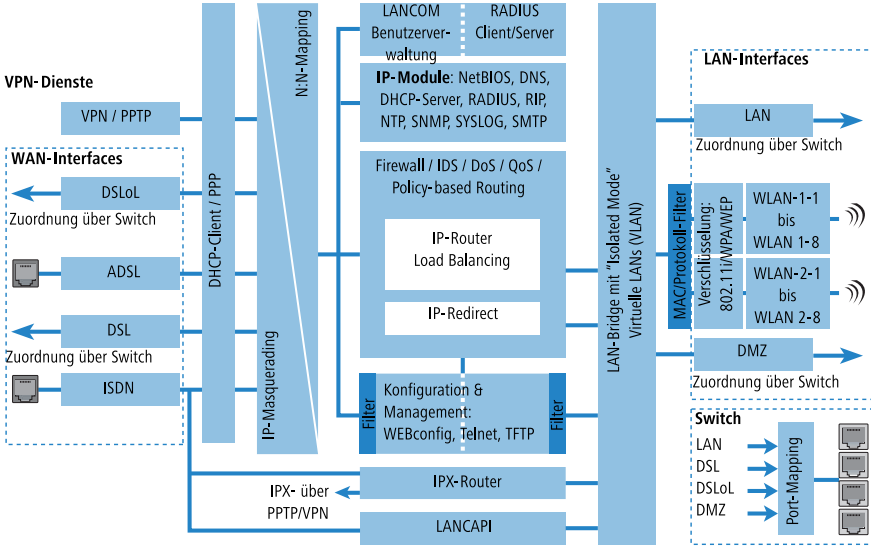
Inhalt

1 System-Design

Das Hirschmann-Betriebssystem HiLCOS ist aus einer Vielzahl von verschiedenen Software-Modulen aufgebaut; die Hirschmann-Geräte selbst verfügen über unterschiedliche Schnittstellen (Interfaces) zum (W)WAN und zum (W)LAN hin. Je nach Anwendung laufen die Daten auf dem Weg von einem Interface zum anderen über verschiedene Module.

Das folgende Blockschaltbild zeigt **ganz** abstrakt die generelle Anordnung der Hirschmann-Interfaces und HiLCOS-Module. Die Beschreibungen der einzelnen Funktionen im weiteren Verlauf dieses Referenzhandbuchs greifen diese Darstellung jeweils auf, um die wichtigen Verbindungen der jeweiligen Anwendungen darzustellen und die daraus resultierenden Konsequenzen abzuleiten.

So kann dieses Schaubild z. B. verdeutlichen, bei welchen Datenströmen die Firewall zum Einsatz kommt oder an welcher Stelle bei einer Adressumsetzung (IP-Masquerading oder N:N-Mapping) welche Adressen gültig sind.



Hinweise zu den einzelnen Modulen und Interfaces:

- Der IP-Router sorgt für das Routing der Daten auf IP-Verbindungen zwischen den Interfaces aus WLAN und WAN.
- Beim IP-Redirect werden Anfragen an ausgewählte Dienste im (W)LAN gezielt auf bestimmte Rechner umgeleitet.
- Die Firewall (mit den Diensten "Intrusion Detection", "Denial of Service" und "Quality of Service") umschließt den IP-Router wie eine Hülle. Alle Verbindungen über den IP-Router gehen also automatisch auch durch die Firewall.
- Als Schnittstellen ins LAN stellen die Geräte ein separates LAN-Interface oder einen integrierten Switch mit mehreren LAN-Interfaces bereit.
- Geräte mit Wireless-Modul bieten daneben zusätzlich eine oder je nach Modell auch zwei Funkschnittstellen für die Anbindung von Wireless LANs. Jede Funkschnittstelle kann je nach Modell bis zu 816 verschiedene WLAN-Netzwerke aufbauen ("Multi-SSID").
- Mit der DMZ-Schnittstelle kann bei einigen Modellen eine demilitarisierte Zone (DMZ) eingerichtet werden, die auch physikalisch in der LAN-Bridge von den anderen LAN-Interfaces getrennt ist.
- Die LAN-Bridge verfügt über einen Protokoll-Filter, der das Sperren von dedizierten Protokollen auf dem LAN ermöglicht. Darüber hinaus können durch den "Isolated Mode" einzelne LAN-Interfaces voneinander getrennt werden. Durch den Einsatz der VLAN-Funktionen können in der LAN-Bridge virtuelle LANs eingerichtet werden, die auf einer physikalischen Verkabelung den Betrieb von mehreren logischen Netzen erlaubt.
- Mit den verschiedenen IP-Modulen (NetBIOS, DNS, DHCP-Server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP) können die Anwendungen über den IP-Router oder direkt über die LAN-Bridge kommunizieren.
- Die Funktionen "IP-Masquerading" und "N:N-Mapping" sorgen für die geeignete Umsetzung von IP-Adressen zwischen den privaten und dem öffentlichen IP-Bereichen oder auch zwischen mehreren privaten Netzwerken.
- Auf die Dienste für Konfiguration und Management der Geräte (WEBconfig, SSH, Telnet, TFTP, SCP, LL2M) kann von LAN- und auch von WAN-Seite aus (bei entsprechender Berechtigung) direkt zugegriffen werden. Diese Dienste sind durch Filter und Login-Sperre geschützt, es erfolgt hier jedoch **kein** Durchlauf durch die Firewall. Ein direktes "Durchgreifen" aus dem

WAN in das LAN (oder umgekehrt) **über** die internen Dienste als Umweg um die Firewall ist jedoch **nicht** möglich.

- IPX-Router und LANCAPI greifen auf der WAN-Seite nur auf das ISDN-Interface zu. Beide Module sind unabhängig von der Firewall, die nur den Datenverkehr durch den IP-Router überwacht. Für IPX über VPN kann der IPX-Router zusätzlich direkt auf das PPTP/VPN-Modul zugreifen.
- Die VPN-Dienste (inklusive PPTP) erlauben das Verschlüsseln der Daten im Internet und damit den Aufbau von virtuellen privaten Netzwerken über öffentliche Datenverbindungen.
- Mit DSL, ADSL und ISDN stehen je nach Modell verschiedene WAN-Interfaces zur Verfügung.
- Das DSLoL-Interface (DSL over LAN) ist kein physikalisches WAN-Interface, sondern eher eine "virtuelle WAN-Schnittstelle". Mit der entsprechenden Einstellung im LCOS kann bei einigen Modellen ein LAN-Interface **zusätzlich** als DSL-Interface genutzt werden.

2 Konfiguration

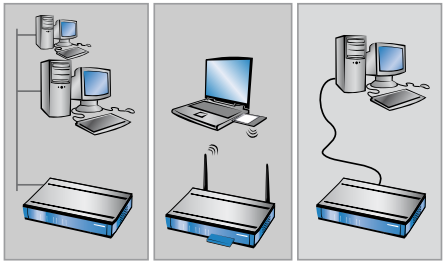
In diesem Kapitel erhalten Sie einen Überblick, mit welchen Mitteln und über welche Wege Sie auf das Gerät zugreifen können, um Einstellungen vorzunehmen. Sie finden Beschreibungen zu folgenden Themen:

- Konfigurationstools
- Kontroll- und Diagnosefunktionen von Gerät und Software
- Sicherung und Wiederherstellung kompletter Konfigurationen
- Installation neuer Firmware im Gerät

2.1 Mittel und Wege für die Konfiguration

Das Gerät unterstützt verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration. Je nach verfügbaren Anschlüssen lässt sich das Gerät auf verschiedenen Zugangswegen erreichen:

- über das angeschlossene Netzwerk (sowohl [W]LAN als auch WAN; auch "Inband" genannt) [1, 2];
- über die serielle Konfigurationsschnittstelle (Config-Schnittstelle; auch "Outband" genannt) [3];



Was unterscheidet diese Wege?

Die oben gelisteten Zugangswege unterscheiden sich einerseits in ihrer möglichen Verfügbarkeit und andererseits in ihren Anforderungen an zusätzliche Hard- und Software:

- Die Inband-Konfiguration benötigt neben dem ohnehin vorhandenen Rechner im LAN, WAN oder WLAN nur noch eine geeignete Software, beispielsweise LANconfig oder einen Webbrowser für die Konfiguration über WEBconfig (vgl. *Software zur Konfiguration* auf Seite 37). Die Inband-Konfiguration ist jedoch z. B. nicht mehr möglich, wenn das übertragende Netzwerk gestört ist.
- Die Outband-Konfiguration ist durch den separaten Übertragungsweg immer verfügbar. Sie benötigt zusätzlich zur Konfigurationssoftware noch einen Rechner mit serieller Schnittstelle.

2.2 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines Geräts einstellen. LANconfig benötigt einen Konfigurationsrechner mit Windows 98 oder höher. Weitere Informationen finden Sie im Kapitel *LANconfig - Geräte konfigurieren* auf Seite 208.
- **WEBconfig** – diese Software ist fest in das HiLCOS eines Geräts eingebaut. WEBconfig ist dadurch betriebssystemunabhängig; auf dem Konfigurationsrechner wird nur ein Webbrowser vorausgesetzt. Weitere Informationen finden Sie im Kapitel *WEBconfig* auf Seite 38.
- **Terminalprogramm** – alternativ zu LANconfig können Sie auch Terminalprogramme (wie z. B. HyperTerminal oder PuTTY) verwenden, um ein Gerät über die Kommandozeile zu konfigurieren. Je nach Funktionsumfang des Programms kann die Kommunikation dabei wahlweise über die serielle Schnittstelle oder innerhalb eines IP-Netzwerks erfolgen. Innerhalb von IP-Netzwerken stehen Ihnen die Protokolle Telnet, SSH oder das Dateiübertragungs-Protokoll TFTP zur Auswahl.

- **SNMP Management-Programm** – alternativ zu LANconfig können Sie auch geräteunabhängige Programme zum Management von IP-Netzwerken verwenden, die auf dem SNMP-Protokoll basieren.

Die folgende Tabelle zeigt, über welchen Weg Sie mit den jeweiligen Mitteln auf die Konfiguration zugreifen können:

Verwendete Software	*[W]LAN, WAN (Inband)*	*Config-Schnittstelle (Outband)*
LANconfig	Ja	Ja
WEBconfig	Ja	Nein
Serial-Client	Nein	Ja
Telnet-Client	Ja	Nein
SSH-Client	Ja	Nein
TFTP-Client	Ja	Nein
SNMP Management-Programm	Ja	Nein

Tabelle 1: Übersicht der Konfigurationsmittel in Abhängigkeit der Konfigurationswege

Hinweis: Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen. Wenn Sie beispielsweise in LANconfig Einstellungen ändern, hat dies auch direkte Auswirkungen auf die Werte unter WEBconfig und Telnet.

2.2.1 LANconfig

Informationen zur Konfiguration der Geräte mit LANconfig finden Sie separat im LCMS-Kapitel *LANconfig - Geräte konfigurieren* auf Seite 208.

2.2.2 WEBconfig

Mit WEBconfig stellen Ihnen die Geräte eine grafische Benutzeroberfläche bereit, die direkt in das HiLCOS integriert ist. Dadurch kann die Konfiguration der Geräte aus der Ferne und/oder unabhängig vom verwendeten Betriebssystem Ihres Rechners erfolgen. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen.

Zugang zum Gerät mit WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich das Gerät ansprechen lässt. Das Verhalten der Geräte sowie ihre Erreichbarkeit zur Konfiguration über einen Webbrowser hängen davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen. Der Zugriff mit WEBconfig erfolgt entweder über die IP-Adresse des Gerätes, über den Namen des Gerätes (sofern bereits zugewiesen) bzw. sogar über einen beliebigen Namen, falls das Gerät noch nicht konfiguriert wurde.

Nach dem Einschalten prüfen unkonfigurierte Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

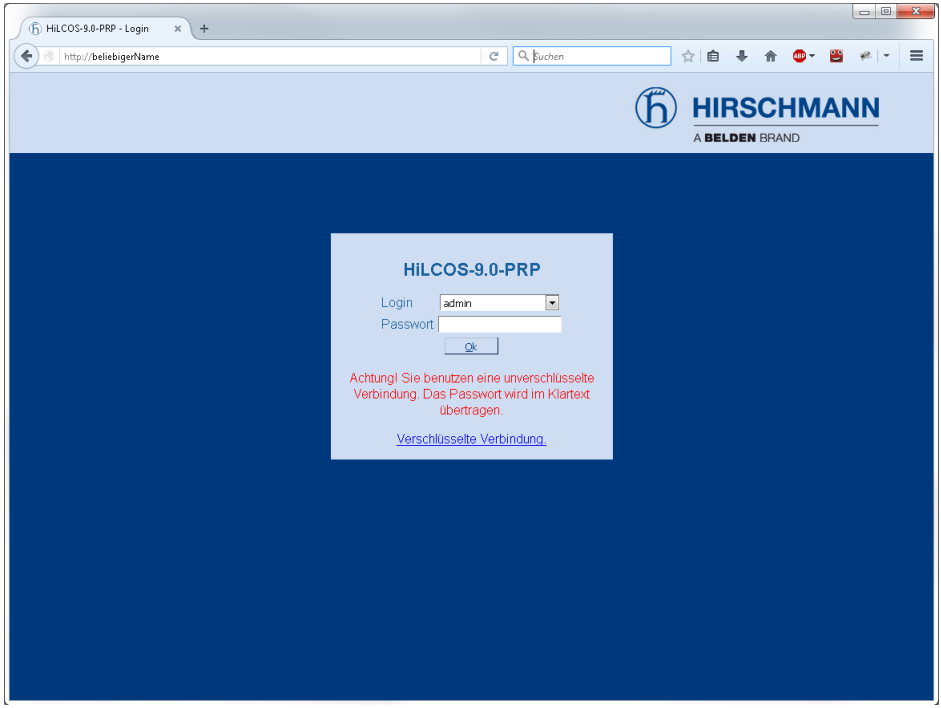
Hinweis: Wenn Sie ein WLAN-Gerät von einem WLAN-Controller zentral verwalten lassen, schaltet das WLAN-Gerät beim Zuweisen der WLAN-Konfiguration ebenfalls den DHCP-Server vom Auto-Modus in den Client-Modus um.

Netz ohne DHCP-Server

In einem Netz ohne DHCP-Server schalten unkonfigurierte Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechnern im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP). In dieser Konstellation kann das Gerät von jedem Rechner mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter der IP-Adresse **172.23.56.254** erreicht werden.

Hinweis: Im werksseitigen Auslieferungszustand mit aktiviertem DHCP-Server leitet das Gerät alle eingehenden DNS-Anfragen an den internen Webserver weiter. Dadurch können unkonfigurierte Geräte einfach durch

Eingabe eines beliebigen Namens in die Adresszeile eines Webbrowsers angesprochen und in Betrieb genommen werden.



Falls der Konfigurations-Rechner seine IP-Adresse nicht vom DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start** / **Ausführen** / **cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000, Windows XP oder Windows Vista, mit **Start** / **Ausführen** / **cmd** und dem Befehl **winipcfg** an der Eingabeaufforderung unter Windows Me oder Windows 9x bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das Gerät unter der Adresse **x.x.x.254** (die “x” stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Diese IP-Adresse ist aber zunächst nicht bekannt; die Erreichbarkeit des Gerätes hängt von der Namensauflösung ab:

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem DHCP-Server aus, kann das Gerät durch Eingabe der MAC-Adresse (z. B. `00a057xxxxxx`) erreicht werden.

  Hinweis: Die MAC-Adresse finden Sie auf einem Aufkleber auf der Geräteunterseite.

- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall haben Sie folgende Optionen, um die IP-Adresse des Gerätes zu ermitteln:
  - Sie nutzen von einem anderen erreichbaren Gerät aus die WEBconfig-Funktion **Andere Geräte suchen/anzeigen**, oder alternativ die LANconfig-Funktion **Geräte suchen**.
  - Sie machen die per DHCP an das Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig und versuchen, das Gerät mit dieser IP-Adresse direkt zu erreichen.
  - Sie schließen einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät an.

Anmeldung am Gerät

Rufen Sie WEBconfig über die vom DHCP-Server vergebene IP-Adresse bzw. den vom DNS-Server vergebenen Namen auf. Wenn Sie beim Zugriff auf das Gerät zur Eingabe von Benutzername und Kennwort aufgefordert werden, tragen Sie Ihre persönlichen Werte in die entsprechenden Felder der Eingabemaske ein. Achten Sie dabei auf Groß- und Kleinschreibung.

Falls Sie den allgemeinen Konfigurationszugang ("root") verwenden, tragen Sie nur das entsprechende **Passwort** ein. Das **Login**-Feld für den Benutzernamen bleibt in diesem Fall leer.

Falls Sie sich erstmalig am Gerät anmelden bzw. noch keine weiteren Administratoren konfiguriert sind, blendet die Eingabemaske das Login-Feld automatisch aus.

Hinweis: Der Login-Dialog bietet alternativ einen Link für eine verschlüsselte Verbindung über HTTPS. Nutzen Sie nach Möglichkeit immer die HTTPS-Verbindung mit erhöhter Sicherheit; insbesondere, wenn Sie aus externen Netzen auf das Gerät zugreifen. Dabei können Sie die verschlüsselte Verbindung auch direkt mit `https://<IP-Adresse oder Gerätename>` herstellen.

Hinweis: Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden. Überprüfen Sie dabei auch, ob Sie sich noch im aktuellen Entwicklungszweig befinden, da manche Browser automatische Updates nur in bestimmten Versionsbereichen durchführen oder Updates nicht mehr anzeigen, wenn die Unterstützung für bestimmte Betriebssysteme ausgelaufen ist. In diesem Fall empfiehlt sich dringend der Wechsel auf einen alternativen Webbrowser.

Setup-Wizards

Mit den Setup-Wizards haben Sie die Möglichkeit, schnell und komfortabel die häufige Einstellungen für ein Gerät vorzunehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein. Die einzelnen Einrichtungsschritte sind mit denen von LANconfig identisch.

Das Gerät speichert die getätigten Einstellungen erst dann, wenn Sie die Eingaben auf der letzten Seite eines Assistenten bestätigen. Die Verfügbarkeit einzelner Assistenten variiert zwischen einzelnen Gerätetypen (Access Point, WLAN Controller, usw.).

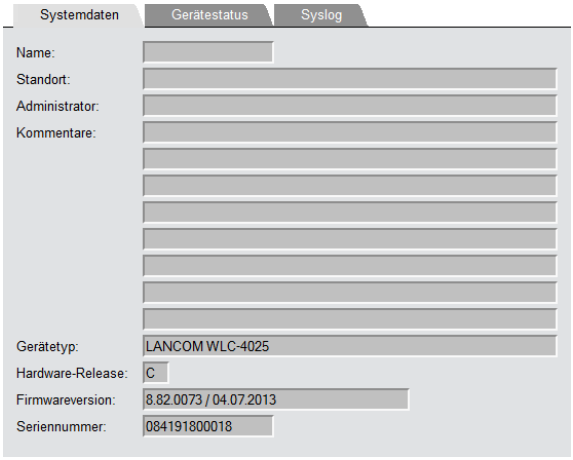
Hinweis: Auf Geräten mit VPN-Funktion lassen sich VPN-Client-Einwahlzugänge wie Advanced-VPN-Client oder myVPN auch über WEBconfig anlegen. Die 1-Click-VPN-Konfiguration ist in WEBconfig durch die Beschränkungen des Browserzugriffs nicht verfügbar.

Systeminformation

Ihr Gerät zeigt Ihnen im Menübereich **Systeminformation** die wichtigsten Daten zur Soft- und Hardware Ihres Gerät, physischen Verbindungen sowie die Syslog-Tabelle an.

Systemdaten

Auf der Seite der Systeminformationen finden Sie auf der Registerkarte **Systemdaten** allgemeine Informationen über das Gerät, den Standort, die Firmware-Version, die Seriennummer etc.



Gerätestatus

Auf der Registerkarte **Gerätestatus** finden Sie umfangreiche Informationen über den aktuellen Betriebszustand des Gerätes. Dazu gehört z. B. die visuelle Darstellung der Schnittstellen mit Angabe der darauf aktiven Netzwerke. Über entsprechende Links können relevante weitere Statistiken aufgerufen werden (z. B. DHCP-Tabelle). Bei wesentlichen Mängeln in der Konfiguration (z. B. ungültige Zeiteinstellung) wird ein direkter Link zu den entsprechenden Konfigurationsparametern angeboten.

Systemdaten | Gerätestatus | Syslog

Schnittstelle/Port	Status/Modus	Information
CPU-Last	Aktuell: 0.80%	
Speicher	Gesamt: 121.7 MBytes Frei: 100.6 MBytes	
ETH-1		
ETH-2		
ETH-3		
ETH-4		
Uplink		Zuordnung: LAN-1 Privat-Modus: nein Verbindung-aufgebaut: ja Anschluss: 100 Mbit Full-Duplex Auto-Verhandlung: Abgeschlossen Flusssteuerung: ja MDI-Modus: MDIX
LAN-1	Durchsatz: 312 B	
LAN-2	Durchsatz: 0 B	

Den Umfang der auf dieser Seite angezeigten Informationen definieren Sie im Setup-Menü unter **HTTP** > **Geräteinformation-anzeigen**. Dabei legen Sie über eine Indexnummer auch die Reihenfolge der Anzeige fest.

Geräteinformation-anzeigen

Geräte-Information	Position
CPU	1
Speicher	2
Ethernet-Ports	7
Durchsatz(Ethernet)	10
Router	11
Firewall	12
DHCP	13
DNS	14
VPN	15
Verbindungen	16
SCEP-CA	17
WLAN-Controller	18
Uhrzeit	19
IPv4-Adressen	20
Betriebszeit	25

Syslog

Das Gerät legt Syslog-Informationen im Arbeitsspeicher ab (siehe dazu *Das SYSLOG-Modul* auf Seite 411). Die letzten Ereignisse können Sie zur Diagnose über WEBconfig auf der Registerkarte **Gerätestatus** einsehen.

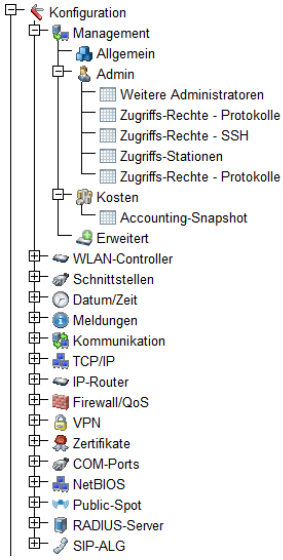
Systemdaten | Gerätestatus | Syslog

Idx.	Zeit	Quelle	Level	Meldung
1	2013-08-20 12:57:16	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 78.35.59.79.
2	2013-08-20 12:57:11	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 78.35.59.79.
3	2013-08-20 12:57:06	AUTHPRIV	Hinweis	Webconfig: user logout from 78.35.59.79
4	1900-02-10 01:27:11	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 78.35.59.79.
5	1900-02-10 01:25:46	KERN	Warnung	SNTP: Request failed, restart poll timer.
6	1900-02-10 01:23:22	AUTHPRIV	Hinweis	Webconfig: user logout from 78.35.59.79
7	1900-02-10 01:19:53	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 78.35.59.79.
8	1900-02-10 01:19:45	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 78.35.59.79.
9	1900-02-10 01:10:46	KERN	Warnung	last message repeated 1060 times
10	1900-01-30 00:10:46	KERN	Warnung	SNTP: Request failed, restart poll timer.
11	1900-01-30 00:10:23	AUTHPRIV	Hinweis	User from 192.168.2.254 via Telnet-SSL logged out
12	1900-01-30 00:10:22	LOCAL2	Hinweis	Download from 192.168.2.254 via Telnet-SSL succeeded
13	1900-01-30 00:10:21	LOCAL2	Hinweis	Configuration download started from 192.168.2.254 via Telnet-SSL
14	1900-01-30 00:10:19	AUTHPRIV	Hinweis	Login from 192.168.2.254 via Telnet-SSL
15	1900-01-30 00:10:12	AUTHPRIV	Hinweis	Webconfig: user logout from 89.0.145.139
16	1900-01-30 00:10:06	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 89.0.145.139.

Hinweis: Zeitstempel beginnend mit '1900-…' weisen auf eine nicht oder nicht korrekt gesetzte Uhrzeit hin.

Konfiguration

Der Menübereich **Konfiguration** bietet dieselben Konfigurationsparameter in der gleichen Struktur an wie LANconfig.



HiLCOS-Menübaum

Der Menübereich **HiLCOS-Menübaum** bietet die Konfigurations- und Statusparameter in der gleichen Struktur an wie unter Telnet. Die einzelnen Zweige des Menübaums gliedern sich in Menüpunkte, Tabellen, Parameter und Aktionen. Tabellen gruppieren Sätze von Parametern; Menüpunkte gruppieren Tabellen, einzelne Parameter und Aktionen.

Darüber hinaus verfügt der Menübaum über ein kontextsensitives Hilfesystem: Mit einem Klick auf das Fragezeichen neben einem Eintrag können Sie für jeden Menüpunkt, jede Tabelle und jeden Parameter eine eigene Hilfeseite aufrufen. Weitere Informationen zu den einzelnen Einträgen finden Sie außerdem in der Menüreferenz.

Status

Im **Status**-Menü speichert das Gerät alle Statuswerte. Statuswerte (gespeichert in den dazugehörigen Statusparametern) sind reine Informationswerte, die sich nur auslesen und nicht verändern lassen.

Ein Teil der Statuswerte wird direkt oder indirekt durch die im Setup-Menü gesetzten Parameter beeinflusst und hält nur in bestimmen Einstellungsszenarien tatsächlich auch Werte vor (die DHCP-Tabelle z. B. zeigt nur dann Werte, wenn der geräteinterne DHCP-Server aktiviert und auch im Einsatz ist). Ein anderer Teil ist nicht durch Setup-Parameter beeinflussbar (z. B. die Hardware-Informationen). Einige Menüpunkte beinhalten außerdem Aktionen bzw. Analysefunktionen, die Sie manuell ausführen müssen, bevor das Gerät Ihnen Ergebnisse dazu anzeigt.

Setup

Im **Setup**-Menü speichert das Gerät alle einstellbaren Parameter. Setup-Parameter stellen die Konfigurationsbasis eines Gerätes dar; alle Einstellungen, die Sie in LANconfig oder WEBconfig vornehmen, werden letztendlich in den Parametern des Setup-Menüs gespeichert.

Da für den ordnungsgemäßen Betrieb und die Funktionsweise zahlreiche Parameter erforderlich sind, die jedoch nicht alle einer stetigen Änderung bedürfen (z. B. durch Normen und Standards festgelegte Unter- und Obergrenzen), finden Sie in diesem Menü auch Parameter vor, für die es im LANconfig keine Einstellungsmöglichkeit gibt. Normalerweise müssen diese

Parameter nicht verändert werden; in einigen Fällen kann es jedoch sinnvoll oder erforderlich sein, bestimmte Vorgabewerte den eigenen individuellen Bedürfnissen entsprechend anzupassen.

Hinweis: Diese "Experteneinstellungen" erfordern in vielen Fällen ein fundiertes Hintergrundwissen über die Funktionsweise und Zusammenhänge der einzelnen Module des HiLCOS sowie der technischen Standards. Nicht selten müssen Parameter auch an mehreren Stellen im Setup-Menü verändert werden, um eine bestimmte Konfiguration zu erreichen. Nehmen Sie Einstellungen im Setup-Menü deshalb nur dann vor, wenn die Dokumentation oder der Support Sie explizit dazu auffordert oder Sie mit den technischen Standards und Normen hinter einer Funktion vertraut sind!

Firmware

Im **Firmware**-Menü rufen Sie Informationen zur aktuellen Firmware-Version ab, konfigurieren Firmsafe und schalten ggf. auf eine andere Firmware um (lesen Sie dazu auch *FirmSafe* auf Seite 103), und laden bei Bedarf eine neue Firmware in das Gerät. Alternativ können Sie auch das *Dateimanagement* verwenden, um eine andere Firmware ins Gerät zu laden.

Sonstiges

Über dieses Menü können Sie manuell die Verbindung zu einer Gegenstelle aufbauen oder beenden, das Gerät neu starten sowie (an der Konsole) eine neue Firmware hochladen.

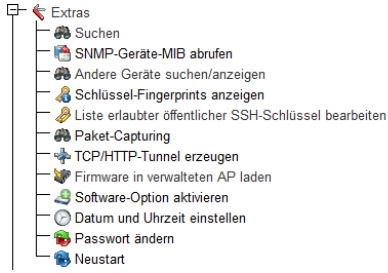
Dateimanagement

Im Menübereich **Dateimanagement** finden Sie alle Aktionen, mit denen Sie Dateien (wie z. B. Konfigurationsdateien und -skripte; aber auch Zertifikate, Templates und Logos) aus dem Gerät herunter oder in das Gerät hochladen. Darüber hinaus können Sie hierüber auch eine andere Firmware in das Gerät einspielen.

In das Gerät hochgeladene Zertifikate oder Dateien können Sie anschließend im Status-Menü unter **Dateisystem** einsehen.

Extras

Im Menübereich **Extras** finden Sie einige Funktionen, welche die Konfiguration der Geräte erleichtern; je nach Gerät aber auch einige Sonderfunktionen und spezielle Analysemodule bereitstellen, die sich keinem der bisherigen Menüpunkte sinnvoll zuordnen lassen.



Hinweis: Der Funktionsumfang dieses Menübereiches variiert je nach Gerätetyp.

Suchen

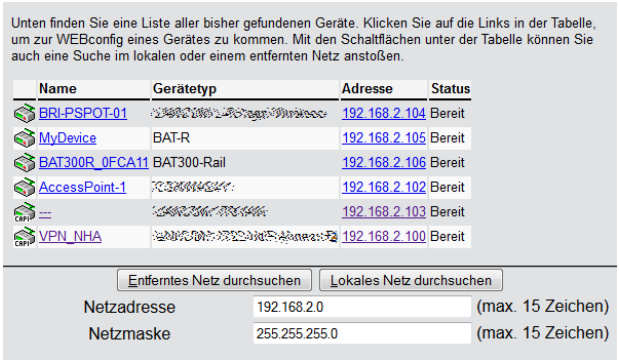
Mit der Suchfunktion durchsuchen Sie den HiLCOS-Menübaum und darin die Namen aller Parameter suchen. Falls Sie also zu einem bestimmten Status- oder Konfigurationsparameter den Namen kennen, aber nicht wissen, über welches Menü dieser Eintrag zu erreichen ist, können Sie die gewünschte Stelle auf diese Weise schnell auffinden.

SNMP-Geräte-MIB abrufen

Über diesen Menüpunkt laden Sie die gerätespezifische *.mib-Datei (Management Information Base) herunter, welche benötigen, um das Gerät in einer alternativen SNMP Management-Software zu überwachen und zu verwalten. Weitere Informationen dazu finden Sie unter *SNMP Management-Programm* auf Seite 86.

Andere Geräte suchen/anzeigen

Mit der Funktion zum Suchen und Anzeigen können Sie andere Geräte in Ihrem Netzwerk suchen und über einen entsprechenden Link direkt auf die Konfigurationsseite der gefundenen Geräte wechseln. Diese Funktion ähnelt somit der Funktion **Geräte suchen** in LANconfig.



Schlüssel-Fingerprints anzeigen

Diese Seite zeigt Ihnen eine Übersicht der Fingerprints aller im Gerät werksseitig vorhandenen Kryptographie-Schlüssel an. Mehr dazu erfahren Sie unter *Geräteinterne SSH-/SSL-Schlüssel* auf Seite 142.

Erlaubte öffentliche SSH Schlüssel

Diese Seite zeigt Ihnen eine Übersicht dem vom Gerät akzeptierten öffentlichen Schlüssel (SSH Public-Keys), anhand derer eine Public-Key-Authentifizierung möglich ist. WEBconfig gibt die Übersicht als Textfeld aus, wodurch Sie als Alternative zum Datei-Upload im Bereich Dateimanagement jederzeit weitere Schlüssel hinzufügen und oder bestehende bearbeiten können.

Mehr zu dem Thema und zur Schlüssel-Syntax finden Sie im und um das Kapitel *Syntax und Benutzer öffentlicher Schlüssel anpassen* auf Seite 150.

Hinweis: Neue Schlüssel tragen Sie in eine eigene Zeile ein; Zeilenumbrüche im Schlüssel-String selbst sind nicht erlaubt.

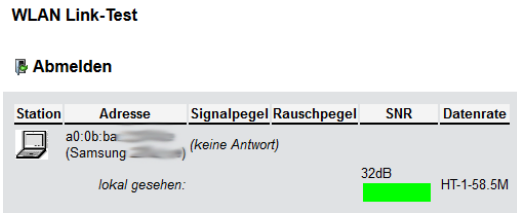
Paket-Capturing

Öffnet die Konfigurationsseite für das Paket-Capturing. Mehr über diese Funktion erfahren Sie unter *Paket-Capturing* auf Seite 406.

WLAN Link-Test

Dieser Menüpunkt nur auf Geräten mit WLAN-Modul verfügbar.

Diese Seite zeigt die Ergebnisse des WLAN Link-Tests an. Der WLAN Link-Test prüft die Verbindung zu verbundenen WLAN Clients.



Spectral Scan

Dieser Menüpunkt nur auf ausgewählten Geräten verfügbar.

Öffnet die Konfigurationsseite für Spectral Scan. Mehr über diese Funktion erfahren Sie unter *Spectral Scan* auf Seite 1207.

TCP/HTTP-Tunnel erzeugen

Öffnet die Konfigurationsseite für das HTTP-Tunneling via TCP/IP. Mehr über diese Funktion erfahren Sie unter *TCP-Port-Tunnel* auf Seite 202.

Firmware in verwalteten AP laden

Dieser Menüpunkt nur auf WLAN-Controllern (WLCs) verfügbar.

Auf dieser Seite haben Sie die Möglichkeit, per Fernzugriff die Firmware auf einem vom WLC verwalteten AP manuell zu aktualisieren. Dies kann z. B. sinnvoll sein, um auf ausgewählten APs den Produktiveinsatz einer Firmware vorab zu testen. Wählen Sie dazu einen AP anhand seiner MAC-Adresse aus und wählen Sie die entsptechende Firmware-Datei. Klicken Sie anschließend auf **Starte Upload**, um die Firmware in den AP zu laden.

Hinweis: Beachten Sie, dass dieser Vorgang die Firmwareverwaltung in der AP-Tabelle für den ausgewählten AP deaktiviert. Dies verhindert, dass der WLC ggf. automatisch eine andere Firmware einspielt. Die Firmware-Verwaltung lässt sich im Setup-Menü unter **WLAN-Management** > **AP-Konfiguration** > **Verwalte-Firmware** jederzeit wieder aktivieren.

Damit der Access Point die geladene Firmware auch verwendet, müssen Sie anschließend einen Neustart des Gerätes durchführen. Durch Aktivieren der Einstellung **AP nach Aktualisierung der Firmware neustarten** veranlassen Sie einen automatischen Neustart, sobald der Firmware-Upload abgeschlossen ist.

Software-Option aktivieren

Sofern für Ihr Gerät zusätzliche Software-Optionen verfügbar sind, haben Sie nach Erwerb des dazugehörigen Aktivierungs- bzw. Registrierungsschlüssels auf dieser Seite die Möglichkeit, die dazugehörige(n) Option(en) freizuschalten.

Hinweis: Registrierungsschlüssel sind stets gerätespezifisch und lassen sich nicht auf andere Geräte übertragen. Heben Sie einen Schlüssel nach erfolgreicher Eingabe dennoch gut auf, um bei Bedarf (z. B. nach einer Reparatur) eine Option erneut freizuschalten.

Datum und Uhrzeit einstellen

Auf dieser Seite stellen Sie manuell das aktuelle Datum und die Uhrzeit ein. Alternativ können Sie auch einen Zeitserver verwenden, um die Uhrzeit zukünftig automatisch aktuell zu halten. Mehr dazu finden Sie unter *Zeit-Server für das lokale Netz* auf Seite 1676.

Hinweis: Das explizite Setzen von Datum und Uhrzeit ist für die korrekte Funktionsweise einiger Module (z. B. das Syslog- oder das Public Spot-Modul) unabdingbar!

Passwort ändern

Über diese Seite ändern Sie das Passwort für Ihren Benutzer-Account.

Neustart

Über diese Seite veranlassen Sie nach einem Klick auf die dazugehörige Schaltfläche einen Neustart des Gerätes. Dieser Befehl ist identisch mit dem unter **HiLCOS-Menübaum** > **Sonstiges** > **Kaltstart**.

HTTP-Sitzung

Im Menübereich **HTTP-Sitzung** passen Sie die Darstellung der WEBconfig-Oberfläche zur besseren Anzeige an Ihr Ausgabegerät an; so z. B. lässt sich die Auflösung verringern oder der Kontrast verstärken.

Abmelden vom Gerät

Mit einem Klick auf den Menüpunkt **Abmelden** beenden Sie Ihre aktuelle WEBconfig-Sitzung und kehren zur Anmeldemaske des Gerätes zurück.

2.2.3 Terminalprogramm

Ihr Gerät unterstützt den kommandozeilen-basierten Zugriff durch ein Terminalprogramm über verschiedene Schnittstellen (wie [W]LAN, WAN oder Serial) und Protokolle (wie Telnet, SSH oder TFTP) hinweg. Durch die Installation eines geeigneten Clients haben Sie somit die Möglichkeit, unabhängig von einer grafischen Benutzeroberfläche an der HiLCOS-Konsole Gerätedaten auslesen, zu verändern und zu analysieren, und mittels selbstgeschriebener Skripte diese Vorgänge für mehrere Geräte zu automatisieren, um z. B. via Fernkonfiguration mehrere Geräte in einem Arbeitsschritt zu warten.

Hinweis: In Windows-Versionen 7 oder neuer ist der Telnet-Client kein fester Bestandteil des Systems mehr. Sie können diesen Client aber manuell nachinstallieren, oder auf eine alternative Software wie z. B. den freien Multi-Protokoll-Client PuTTY ausweichen. PuTTY selbst ist sowohl für Windows- als auch Linux-Betriebssysteme erhältlich.

Terminalsitzung starten

Bei vielen Betriebssystemen starten Sie eine Terminalsitzung an der Kommandozeile mit einer Befehlskombination aus dem verwendeten Protokoll und der zu verbindenen IP-Adresse. Je nach Protokoll oder Client kann es jedoch einzelne Abweichungen geben. Die genaue Syntax entnehmen Sie bitte daher der dazugehörigen System- bzw. Programmdokumentation.

Nachfolgend finden Sie für ausgewählte Protokolle und Systeme gängige Befehle:

Telnet

Aus der Windows-Kommandozeile oder dem Linux-Terminal starten Sie eine Telnet-Sitzung mit dem Befehl `telnet <host>`. Telnet baut dann eine (unverschlüsselte) Verbindung zum Gerät mit der eingegebenen IP-Adresse auf. Nach der Eingabe des Passworts (sofern Sie eines zum Schutz der Konfiguration vereinbart haben) stehen Ihnen alle Konfigurationsbefehle zur Verfügung.

Hinweis: Linux-Systeme unterstützen auch Telnet-Sitzungen über SSL-verschlüsselte Verbindungen. Je nach Distribution ist es dazu ggf. erforderlich, die Standard-Telnet-Anwendung durch eine SSL-fähige Version zu ersetzen bzw. einen SSL-fähigen Clienten nachzuinstallieren (z. B. telnet-ssl). Bei Distributionen mit integrierter Telnet-über-SSL-Unterstützung starten Sie eine verschlüsselte Telnet-Verbindung mit dem Befehl `telnet -z ssl <host> <port>`.

SSH

In Windows ist standardmäßig kein SSH-Client integriert. Unter Linux-Systemen nutzen Sie den Befehl `ssh <login-name>@<host>`, um eine verschlüs-

selte Verbindung zum Gerät herstellen und die bei der Konfiguration übertragenen Daten so vor dem Abhören innerhalb des Netzwerks schützen.

Sprache der Konsole ändern

Die Konsole Ihres Gerätes stellt Ihnen verschiedene Sprachen zur Verfügung. Werkseitig ist das Gerät auf 'Englisch' als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation sind Pfadangaben jedoch in ihrer deutschen Form angegeben. Um die Konsolensprache temporär (d. h. für die Dauer der Sitzung) zu verändern, verwenden Sie an der Konsole den `lang`-Befehl, gefolgt von der dazuhörigen Sprache oder deren Anfangsbuchstabe(n); also z. B. `lang Deutsch` oder `lang de`.

Folgende Spracheingaben werden derzeit von der Konsole unterstützt:

- `Deutsch`
- `English`

Um die bei der Anmeldung gewählte Standard-Sprache **dauerhaft** zu verändern, legen Sie im Setup-Menü unter **Config** > **Sprache** die gewünschte Sprache fest. Die in dem dazugehörigen Auswahlmenü befindlichen Sprachen stellen alle möglichen Spracheingaben dar, die Ihr Gerät zum gegenwärtigen Zeitpunkt unterstützt.

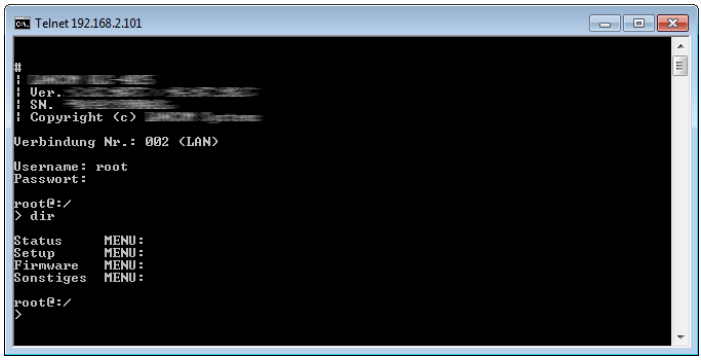
Terminalsitzung beenden oder abbrechen

Um eine Terminalsitzung zu beenden, geben Sie an der Konsole den Befehl `exit`.

Unter Linux-Systemen und manchen Clients (wie z. B. PuTTY) können Sie darüber hinaus die Tastenkombination `Strg+C` verwenden, um eine Terminalsitzung abzubrechen, falls ein Beenden mittels `exit` nicht möglich ist (z. B. während des Anmeldevorgangs mit Passworteingabe).

Die Menüstruktur der Konsole

Das HiLCOS-Kommandozeilen-Interface (die Konsole) ist wie folgt strukturiert:



Status

Enthält die Zustände und Statistiken aller internen Module des Gerätes sowie den Direktzugriff auf das Dateisystem

Setup

Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes

Firmware

Beinhaltet das Firmware-Management

Sonstiges

Enthält Aktionen für Verbindungsauf- und -abbau, Reset, Reboot und Upload

Befehle für die Konsole

Das HiLCOS-Kommandozeilen-Interface wird mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient. Die verfügbaren Menübefehle lassen sich z. T. auch durch Aufrufen des HELP-Kommandos auf der Kommandozeile anzeigen.

Hinweis: Die verfügbaren Befehle sind abhängig vom Funktionsumfang des jeweiligen Gerätes.

Wichtig: Zum Ausführen einiger Befehle sind spezielle Rechte erforderlich, die beim jeweiligen Befehl aufgeführt sind. Befehle ohne Angabe von Rechten besitzen keine Einschränkungen.

Befehl	*Beschreibung*
`tab`	Zur Verwendung in Skript-Dateien: Setzt für ein nachfolgendes Kommando in einer Tabelle die Reihenfolge der Spalten für die Argumente, falls die Spalten in der Tabelle vom Standard abweichen (z. B. eine zusätzliche Spalte). **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`readmib`	Anzeige der SNMP Management Information Base. Nur auf Geräten ohne Unified-MIB vorhanden. **Zugriffsrecht**: Supervisor-Read,Local-Admin-Read
`readstatus`	Gibt den Status aller SNMP-IDs des Gerätes aus.
`writeflash`	Laden einer neuen Firmware-Datei (nur via TFTP). **Zugriffsrecht**: Supervisor-Write
`loadfile [-a <Adresse>] [-s <Server-IP-Adresse>] [-n] [-f <Dateiname>] [-o <Dateiname>] [-c <Dateiname>] [-p <Dateiname>] [-d <Passphrase>] [-C n|d] [-m <Version>] [-u] [-x <Dateiname>] [-i]`	Lädt ein Zertifikatsdatei in das Gerät. Mögliche Optionsschalter sind: ▶ `-a`: Bestimmt die Quelladresse der Datei: – `a.b.c.d`: Quell-IP-Adresse – `INT`: Adresse des ersten Intranet-Interfaces als Quelladresse verwenden – `DMZ`: Adresse des ersten DMZ-Interfaces als Quelladresse verwenden – `LBx`: Loopback-Adresse x (0..f) als Quelladresse verwenden – `<Schnittstelle>`: Adresse des LAN-Interfaces <Schnittstelle> als Quelladresse verwenden ▶ `-s`: Adresse des TFTP Servers ▶ `-n`: Server-Namen auf SSL/TLS-Verbindungen ignorieren ▶ `-f`: <Dateiname> der Konfigurationsdatei auf dem TFTP-Server ▶ `-o`: Zieldatei <Dateiname> für Datei-Download ▶ `-c`: Datei <Dateiname> mit Root-Zertifikat für HTTPS ▶ `-p`: Datei <Dateiname> mit unverschlüsseltem PKCS#12-Container für HTTPS CA-Zertifikate und/oder Client-seitige Authentisierung ▶ `-d`: <Passphrase>, um heruntergeladenen, verschlüsselten PKCS#12-Container zu entschlüsseln ▶ `-C`: Überprüfe, ob Firmware neuer (`n`) als oder unterschiedlich (`d`) zu der momentan vorhandenen ist ▶ `-m`: Minimal-<Version> für Firmware setzen ▶ `-u`: Firmware-Datei unbedingt herunterladen, Versionsüberprüfung überspringen. ▶ `-x`: Datei <Dateiname> mit zusätzlichen CA-Zertifikaten zur Überprüfung bei HTTPS, der Wert 'none' verhindert das Laden der Standardzertifikate ▶ `-i`: Sende Sysinfo als POST request (nur bei HTTP(S))

Befehl	*Beschreibung*
	Hinweis: Die Optionen [-f] und [-s] sowie die URL sind nicht gleichzeitig nutzbar. Für HTTP(S)-Downloads müssen Sie die Quelle mittels URL spezifizieren. Die Maximallänge der URL beträgt 252 Zeichen. **Zugriffsrecht**: Supervisor-Write
`language`	Wählt eine Sprache für die CLI-Anzeige aus. Der Befehl `language ?` listet die verfügbaren Sprachen auf.
`ssh [-?|h] [-<a|b> Loopback-Adresse] [-p Port] [-C] [-j Keepalive-Intervall] <Host>`	Stellt eine SSH-Verbindung zum <Host> her. Mögliche Optionsschalter sind: ▶ `-?|h`: gibt den Hilfetext aus. ▶ `-a|b`: erlaubt die Angabe einer Route bzw. Loopback-Adresse, die das Gerät verwenden soll, wenn das Ziel auf mehreren Routen erreichbar ist. Die Funktion von `-a` und `-b` ist identisch. `-b` ist die übliche Option eines OpenSSH-Clients auf UNIX-Systemen, während einige andere im HiLCOS eingebaute Kommandos das `-a` zur Angabe einer Loopback-Adresse benutzen. ▶ `-p`: bestimmt den <Port> des Hosts ▶ `-C`: erzwingt eine komprimierte Datenübertragung ▶ `-j`: gibt an, in welchen Abständen der Client ein Keepalive senden soll.
`telnet <Adresse>`	Stellt eine Telnet-Verbindung zur angegebenen <Adresse> her.
`sshkeygen [-h] [-q] [-t dsa|rsa|ecdsa] [-b <bits>] [-f <Dateiname>] [-R <Hostname>]`	Erzeugt oder löscht SSH-Schlüssel im Gerät. Mögliche Optionsschalter sind: ▶ `-h`: Zeigt eine kurze Hilfe der möglichen Parameter. ▶ `-q`: Das Gerät überschreibt bereits existierende Schlüssel ohne Rückfrage (Quiet-Modus) ▶ `-t`: Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln: – RSA – DSA – ECDSA ▶ `-b`: Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit. ▶ `-f`: Über diesen Parametern geben Sie den Mountingpoint der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Mountingpoints hängt davon ab, was für einen Schlüssel Sie erzeugen. Zur Auswahl stehen Ihnen in diesem Fall: – **ssh_rsakey** für RSA-Schlüssel

Befehl	*Beschreibung*
	– **ssh_dsakey** für DSA-Schlüssel – **ssh_ecdsakey** für ECDSA-Schlüssel **Hinweis:** Weitere Informationen zu geräteinternen SSH/SSL-Schlüsseln finden Sie im Kapitel *Geräteinterne SSH-/SSL-Schlüssel* auf Seite 142
`sshcopyid`	Zur Speicherung des SSH-Public-Keys per SSH **Zugriffsrecht**: Supervisor-Write
`enable <Parameter>`	Erweitert die Rechte von angemeldeten TACACS+-Benutzern. Mögliche Parameter sind: ▶ `0`: Keine Rechte ▶ `1`: Read-Only ▶ `3`: Read-Write ▶ `5`: Read-Only-Limited Admin ▶ `7`: Read-Write-Limited Admin ▶ `9`: Read-Only Admin ▶ `11`: Read-Write Admin ▶ `15`: Supervisor (Root)
`bootconfig [-s (1|2|all)] [-r (1|2|all)]`	Ermöglicht das Speichern und Löschen von Boot-Konfigurationen. Mögliche Optionen sind: ▶ `-s`: Speichert die aktuelle Konfiguration eines Gerätes wahlweise als kundenspezifische Standard-Einstellung (1), Rollout-Konfiguration (2) oder beides (all). ▶ `-r`: Löscht wahlweise die aktuelle kundenspezifische Standard-Einstellung (1), die Rollout-Konfiguration (2) oder beide (all). **Zugriffsrecht**: Supervisor-Write **Hinweis:** Weitere Informationen zu Boot-Konfigurationen finden Sie im Kapitel *Alternative Boot-Config* auf Seite 97
`lspci`	Ausgabe von Informationen über PCI-Geräte **Zugriffsrecht**: Supervisor-Read
`beginscript [-u] [-C d]`	Versetzt eine Konsolensitzung in den Skript-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM des Geräts übertragen, sondern zunächst in den Skript-Speicher. Mögliche Optionsschalter sind: ▶ `-u`: Erzwingt die unbedingte ("**u**nconditional") Ausführung eines Skriptes oder einer Konfiguration. ▶ `-C d`: Überspringt die standardmäßige Differenzprüfung ("**C**heck for **d**ifference"). Gilt auch, wenn die Option `-u` gesetzt ist. **Zugriffsrecht**: Supervisor-Write

Befehl	*Beschreibung*
`unmount [-?][-f] <Volume>`	Gibt die aktuelle Volumetabelle aus. ▶ `-f`: Gibt das angegebene Volume frei. <Volume> kann die Volume-ID oder ein beliebiger Mountpunkt sein. ▶ `-?`: Gibt den Hilfetext aus.
`cd <Path>`	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z. B. `cd ../..` kann verkürzt werden zu `cd ...` etc.
`default [-r] <Path>`	Setzt einzelne Parameter, Tabellen oder ganze Menübäume in die Grundkonfiguration zurück. Zeigt <Path> auf einen Zweig des Menübaums, muss zwingend die Option `-r` (recursive) angegeben werden. **Zugriffsrecht**: Supervisor-Write
`del|delete|rm [<Path>] <Row>|*`	Löscht die Tabellenzeile <Row> in der aktuellen Tabelle bzw. in der mittels <Path> im Zweig des Menübaums referenzierten Tabelle. Als <Row> geben Sie dabei die Nummer der Zeile an. Das Wildcard-Zeichen `*` leert eine Tabelle, z. B. `del Config/Cron-Tabelle *`. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`deletebootlog`	Löscht den Inhalt des persistenten Bootlog-Speichers.
`dir|list|ls|llong|l [-a] [-r] [-s] [<Path>] [<Filter>]`	Zeigt den Inhalt des aktuellen Verzeichnisses an. Mögliche Optionsschalter sind: ▶ `-a`: Gibt zusätzlich zu den Inhalten der Abfrage auch die zugehörigen SNMP-IDs aus. Dabei beginnt die Ausgabe mit der SNMP-ID des Gerätes, gefolgt von der SNMP-ID des aktuellen Menüs. Vor den einzelnen Einträgen finden Sie dann die SNMP-IDs der Unterpunkte. ▶ `-r`: Listet auch alle Unterverzeichnisse sowie die darin befindlichen Tabellen auf. ▶ `-s`: Sortiert die Anzeige des aktuelles Verzeichnisses; gruppiert nach Unterverzeichnissen, Tabellen, Werten und Aktionen; jeweils in aufsteigender alphabetischer Reihenfolge.
`do <Path> [<Parameter>]`	Führt die angegebene Aktion im aktuellen bzw. referenzierten Verzeichnis aus, z. B. `do Sonstiges/Kaltstart`. Sofern die Aktion über zusätzliche Parameter verfügt, lassen sich diese nachfolgend angeben.
`echo <Argument>`	Gibt ein Argument auf der Konsole aus.
`exit|quit|x`	Beendet die Terminalsitzung.
`feature <Code>`	Schaltet eine Software-Option mit dem angegebenen Aktivierungsschlüssel frei. **Zugriffsrecht**: Supervisor-Write

Befehl	*Beschreibung*
`flash yes|no`	Regelt die Speicherung von Konfigurationsänderungen über die Kommandozeile. Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (`yes` bzw. `ja`) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (`no` bzw. `nein`), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird. **Zugriffsrecht**: Supervisor-Write
`getenv <Name>`	Gibt den Wert der betreffenden Umgebungsvariable aus (ohne Zeilenvorschub). Beachten Sie dazu auch den Befehl 'printenv'.
`history`	Zeigt eine Liste der letzen ausgeführten Befehle. Mit dem Befehl `!#` können die Befehle der Liste unter Ihrer Nummer (#) direkt aufgerufen werden: Mit `!3` wird z. B. der dritte Befehl der Liste ausgeführt.
`iperf [-s|-c <Host>] [-u] [-p <Port>] [-B <Interface>] [-c] [-b [<Bandw>/]<Bandw>[kKmM]] [-l <Length>] [-t <Time>] [-d] [-r] [-L <Port>] [-h]`	Startet iPerf auf dem Gerät, um eine Bandbreitenmessung mit einer iPerf2-Gegenstelle durchzuführen. Mögliche Optionsschalter sind: ▶ **Client/Server** – `-u, --udp`: Verwendet UDP statt TCP. – `-p, --port <Port>`: Verbindet mit oder erwartet Datenpakete auf diesem Port (Standard: 5001). – `-B, --bind <Interface>`: Erlaubt die Verbindung nur über die angegebene Schnittstelle (IP-Adresse oder Schnittstellenname). ▶ **Server-spezifisch** – `-s, --server`: Startet iPerf im Server-Modus und wartet auf die Kontaktaufnahme durch einen iPerf-Client. ▶ **Client-spezifisch** – `-c, --client <Host>`: Startet iPerf im Client-Modus und verbindet mit dem iPerf-Server <Host> (IP-Adresse oder DNS-Name). – `-b, --bandwidth [<Bandw>/]<Bandw>{kKmM}`: Begrenzung der Bandbreite bei der Analyse einer UDP-Verbindung im [Down-]/Up-Stream. Die Angabe erfolgt in Kilo- (kK) oder Megabyte (mM) pro Sekunde (Standard: 1 Mbps). – `-l, --len <Length>`: Bestimmt die Länge der UDP-Datenpakete. – `-t, --time <Time>`: Bestimmt die Dauer der Verbindung in Sekunden (Standard: 10 Sekunden). – `-d, --dualtest`: Der Test erfolgt bidirektional: iPerf-Server und -Client senden und empfangen dabei gleichzeitig. – `-r, --tradeoff`: Der Test erfolgt sequentiell: iPerf-Server und -Client senden und empfangen nacheinander.

Befehl	*Beschreibung*
	– `-L, --listenport <Port>`: Gibt den Port an, auf dem das Gerät im bidirektionalen Betrieb Datenpakete vom entfernten iPerf-Server erwartet (Standard: 5001). ▶ **Verschiedenes** – `-h, --help`: Gibt den Hilfetext aus.
`killscript <Name>`	Löscht den noch nicht verarbeiteten Inhalt einer Skript-Session. Die Skript-Session wählen Sie über deren Namen aus. **Zugriffsrecht**: Supervisor-Write
`linktest`	Nur auf WLAN-Geräten verfügbar. Zeigt die Ergebnisse des WLAN Link-Tests an. **Zugriffsrecht**: Supervisor-Write **Ausführungsrecht**: WLAN-Linktest
`ll2mdetect`	Sucht Geräte per LL2M im LAN. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Befehle für den LL2M-Client* auf Seite 88. **Zugriffsrecht**: Supervisor-Write
`ll2mexec`	Sendet ein Kommando per LL2M an ein Gerät im LAN. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Befehle für den LL2M-Client* auf Seite 88. **Zugriffsrecht**: Supervisor-Write
`loadconfig (-s <Server IP-Address> -f <Filename>)|<URL>`	Lädt eine Konfigurationsdatei via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 117. **Zugriffsrecht**: Supervisor-Write
`loadfirmware (-s <Server IP-Address> -f <Filename>)|<URL>`	Lädt eine Firmware via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 117. **Zugriffsrecht**: Supervisor-Write
`loadscript (-s <Server IP-Address> -f <Filename>)|<URL>`	Lädt ein Konfigurationsskript via TFTP in das Gerät. Geben Sie dazu wahlweise die Server-Adresse und den Dateinamen oder die komplette URL an. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 117. **Zugriffsrecht**: Supervisor-Write
`setpass|passwd [-n <new> <old>]`	Ändert das Passwort des aktuellen Benutzerkontos. Um das Passwort ohne die darauf folgende Eingabeaufforderung zu ändern,

Befehl	*Beschreibung*
	verwenden Sie den Optionsschalter `-n` mit Angabe des neuen und alten Passworts
`setpass|passwd [-u <User>][-n <new> <old>]`	Ändert das Passwort des aktuellen Benutzerkontos. Um das Passwort ohne die darauf folgende Eingabeaufforderung zu ändern, verwenden Sie den Optionsschalter `-n` mit Angabe des neuen und alten Passwortes. Um bei aktivierter TACACS+-Authentifizierung das Passwort des lokalen Benutzerkontos zu ändern, verwenden Sie den Optionsschalter `-u` mit dem Namen des entsprechenden Benutzers. Existiert der lokale Benutzer nicht oder fehlt die Angabe des Benutzernamens, bricht der Befehl ab. Der Benutzer benötigt außerdem Supervisorrechte bzw. die TACACS-Authorisierung muss aktiv sein.
`ping <IPv4-Address|Hostname>` `ping -6 <IPv6-Address>%<Scope>`	Sendet einen ICMP echo request an die angegebene IP-Adresse. Weitere Informationen zu dem Befehl und den Besonderheiten beim Anpingen von IPv6-Adressen finden Sie im Kapitel *Übersicht der Parameter im ping-Befehl* auf Seite 69.
`printenv`	Gibt eine Übersicht aller Umgebungsvariablen und deren Werte aus.
`readconfig`	Gibt die komplette Konfiguration in Form der Geräte-Syntax aus. **Zugriffsrecht**: Supervisor-Read
`readconfig [-h] [-s <password>]`	Gibt die komplette Konfiguration in Form der Geräte-Syntax aus. ▶ `-h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme. ▶ `-s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes. **Zugriffsrecht**: Supervisor-Read
`readscript [-n] [-d] [-i] [-c] [-m]`	Erzeugt eine Textausgabe aller Befehle und Parameter, die für die Konfiguration des Gerätes im aktuellen Zustand benötigt werden. Dabei können Sie folgende Optionsschalter angeben: ▶ `-n`: Die Textausgabe erfolgt nur auf numerischer Basis ohne Bezeichner auf. Die Ausgabe enthält somit nur die aktuellen Zustandswerte der Konfiguration sowie die zugehörigen SNMP-IDs. ▶ `-d`: Nimmt die Default-Werte in die Textausgabe mit auf. ▶ `-i`: Nimmt die Bezeichnungen der Tabellen-Felder in die Textausgabe mit auf. ▶ `-c`: Nimmt eventuelle Kommentare, die sich in der Skriptdatei befinden, in die Textausgabe mit auf. ▶ `-m`: Die Textausgabe erfolgt in einer kompakten, am Bildschirm jedoch schwer lesbaren Darstellung (ohne Einrückungen). **Zugriffsrecht**: Supervisor-Read

Befehl	*Beschreibung*
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>]`	Erzeugt eine Textausgabe aller Befehle und Parameter, die für die Konfiguration des Gerätes im aktuellen Zustand benötigt werden. Dabei können Sie folgende Optionsschalter angeben: ▶ `-n`: Die Textausgabe erfolgt nur auf numerischer Basis ohne Bezeichner. Die Ausgabe enthält somit nur die aktuellen Zustandswerte der Konfiguration sowie die zugehörigen SNMP-IDs. ▶ `-d`: Nimmt die Default-Werte in die Textausgabe mit auf. ▶ `-i`: Nimmt die Bezeichnungen der Tabellen-Felder in die Textausgabe mit auf. ▶ `-c`: Nimmt eventuelle Kommentare, die sich in der Skriptdatei befinden, in die Textausgabe mit auf. ▶ `-m`: Die Textausgabe erfolgt in einer kompakten, am Bildschirm jedoch schwer lesbaren Darstellung (ohne Einrückungen). ▶ `-h`: Ergänzt die Skriptdatei um eine Prüfsumme. ▶ `-s <password>`: Verschlüsselt die Skriptdatei auf Basis des angegebenen Passwortes. **Zugriffsrecht**: Supervisor-Read
`release [-x] *|<Interface_1…Interface_n>`	Der DHCPv6-Client gibt seine IPv6-Adresse und/oder sein Präfix an den DHCPv6-Server zurück. Anschließend fragt er erneut den DHCPv6-Server nach einer Adresse oder einem Präfix. Je nach Provider vergibt der Server dem Client eine neue oder die vorherige Adresse. Ob der Client eine andere Adresse oder ein anderes Präfix erhält, bestimmt alleine der Server. Der Optionsschalter `-x` unterdrückt eine Bestätigungsmeldung. Der Platzhalter * wendet das Kommando auf alle Interfaces und Präfix-Delegationen an. Alternativ können Sie ein oder mehrere spezifische Interfaces angeben.
`repeat <Interval> <Command>`	IPv6-Adressfreigabe: Wiederholt das angegebene Kommando alle `<Interval>` Sekunden, bis der Vorgang durch neue Eingaben beendet wird.
`rollout (-r|-remove) <RelatedFile>`	Löscht die Dateien des benutzerdefinierten Rollout-Assistenten aus dem Dateisystem des Gerätes. Mögliche Dateien sind: ▶ `wizard`: Löscht den Assistenten ▶ `template`: Löscht das Template ▶ `logo`: Löscht das Logo ▶ `alle`: Löscht den Assistenten, das Template und das Logo **Zugriffsrecht**: Supervisor-Write
`sleep [-u] <Value><Suffix>`	Verzögert die Verarbeitung der Konfigurationsbefehle um eine bestimmte Zeitspanne oder terminiert sie auf einen bestimmten Zeitpunkt. Als `<Suffix>` sind `s`, `m` oder `h` für Sekunden, Minuten oder Stunden erlaubt; ohne Suffix arbeitet der Befehl in Millisekunden. Mit dem Optionsschalter `-u` nimmt das `sleep`-Kommando Zeitpunkte

Befehl	*Beschreibung*
	im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch) entgegen. Die Parametrierung als Termin wird nur akzeptiert, wenn die Systemzeit gesetzt ist.
`stop`	Beendet den PING-Befehl
`add|set [<Path>] <Value(s)>`	Setzt einen Konfigurationsparameter auf einen bestimmten Wert. Handelt es sich beim Konfigurationsparameter um einen Tabellenwert, so muss für jede Spalte ein Wert angegeben werden. Dabei übernimmt das Zeichen * als Eingabewert einen vorhandenen Tabelleneintrag unverändert. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`add|set [<Path>] ?`	Listet alle möglichen Eingabewerte für einen Konfigurationsparameter auf. Wird kein spezifischer Pfad angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`setenv <Name> <Value>`	Setzt eine Umgebungsvariable auf den angegebenen Wert. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`show <Options> <Filter>`	Zeigt ausgewählte interne Daten, wie z. B. die letzten Boot-Vorgänge (`bootlog`), Firewall-Filterregeln (`filter`), VPN-Regeln (VPN) oder die Speicherauslastung (`mem`, `heap`). Über zusätzliche Filter-Argumente lässt sich die Ausgabe weiter einschränken. Um eine Übersicht aller möglichen Optionen zu erhalten, geben Sie `show ?` ein. Für die Anzeige IPv6-spezifischer Daten lesen Sie auch das Kapitel *Übersicht der IPv6-spezifischen show-Befehle* auf Seite 76. **Zugriffsrecht**: Supervisor-Read,Local-Admin-Read
`sysinfo`	Zeigt Systeminformationen an (z. B. Hardware-Release, Softwareversion, MAC-Adresse, Seriennummer etc.).
`testmail <From> <To_1…To_n> [<Realname> <Subject> <Body>]`	Verschickt eine Test-E-Mail. Notwendige Angaben sind eine Absendeadresse und Empfängeradresse; Realname, Betreffzeile und Nachrichteninhalt sind optional. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`time <DateTime>`	Setzt einen Zeitpunkt im Format `MM/DD/YYYY hh:mm:ss` (englisch) oder im Format `TT.MM.JJJJ hh:mm:ss` (deutsch). **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write **Ausführungsrecht**: Time-Wizard

Befehl	*Beschreibung*
`trace <Parameter> <Filter>`	Startet einen Trace-Befehl zur Ausgaben von Diagnose-Daten. Über zusätzliche Filter-Argumente lässt sich die Ausgabe weiter einschränken. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Übersicht der Parameter im trace-Befehl* auf Seite 71. **Zugriffsrecht**: Supervisor-Read,Limited-Admin-Read,Limited-Admin-Write
`unsetenv <Name>`	Löscht die angegebene Umgebungsvariable. **Zugriffsrecht**: Supervisor-Write,Local-Admin-Write,Limited-Admin-Write
`who`	Listet aktive Konfigurationssitzungen auf.
`writeconfig [-u] [-C d]`	Schreibt eine neue Konfiguration in Form der Geräte-Syntax in das Gerät. Das System interpretiert alle folgenden Zeilen solange als Konfigurationswerte, bis zwei Leerzeilen auftreten. Mögliche Optionsschalter sind: ▶ `-u`: Erzwingt die unbedingte ("**u**nconditional") Ausführung eines Skriptes oder einer Konfiguration. ▶ `-C d`: Überspringt die standardmäßige Differenzprüfung ("**C**heck for **d**ifference"). Gilt auch, wenn die Option `-u` gesetzt ist. **Zugriffsrecht**: Supervisor-Write
`!!`	Letztes Kommando wiederholen
`!<num>`	Kommando <num> wiederholen
`!<prefix>`	Letztes mit <prefix> beginnendes Kommando wiederholen
`#<blank>`	Kommentar

Tabelle 2: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Legende

- Zeichen- und Klammernregelung:
  - Objekte – hier: dynamische oder situationsabhängige Eingaben – stehen in spitzen Klammern.
  - Runde Klammern gruppieren Befehlsbestandteile zur besseren Übersicht.
  - Vertikale Striche (Pipes) trennen alternative Eingaben.
  - Eckigen Klammern beschreiben optionale Schalter.

  Somit sind alle Befehlsbestandteile, die nicht in eckigen Klammern stehen, notwendigen Angaben zuzurechnen.

- `<Path>`:
  - Beschreibt den Pfadnamen für ein Menü, eine Tabelle oder einen Parameter, getrennt durch "/" oder "\".
  - `..` bedeutet: eine Ebene höher.
  - `.` bedeutet: aktuelle Ebene.
- `<Value>`:
  - Beschreibt einen möglichen Eingabewert.
  - `""` ist ein leerer Eingabewert.
- `<Name>`:
  - Beschreibt eine Zeichensequenz von [0…9] [A…Z] [a…z] [_].
  - Das erste Zeichen darf keine Ziffer sein.
  - Es gibt keine Unterscheidung zwischen Groß- und Kleinschreibung.
- `<Filter>`:
  - Die Ausgaben einiger Kommandos können durch die Angabe eines Filterausdrucks eingeschränkt werden. Die Filterung erfolgt dabei nicht zeilenweise, sondern blockweise abhängig vom jeweiligen Kommando.
  - Ein Filterausdruck beginnt mit einem alleinstehenden '@' und endet entweder am Zeilenende oder an einem alleinstehenden ';', welches das aktuelle Kommando abschliesst.
  - Ein Filterausdruck besteht des weiteren aus einem oder mehreren Suchmustern, die durch Leerzeichen voneinander getrennt sind und denen entweder kein Operator ('Oder'-Muster) oder einer der Operatoren '+' ('Und'- Muster) oder '-' ('Nicht'-Muster) vorangestellt ist.
  - Bei der Ausführung des Kommandos wird ein Informationsblock genau dann ausgegeben, wenn mindestens eines der 'Oder'-Muster, alle 'Und'-Muster und keines der 'Nicht'-Muster passen. Dabei wird die Groß- und Kleinschreibung nicht beachtet.
  - Soll ein Suchmuster Zeichen enthalten, die zur Strukturierung in der Filtersyntax verwendet werden (z. B. Leerzeichen), dann kann das Suchmuster als Ganzes mit "" umschlossen werden. Alternativ kann den speziellen Zeichen ein '\' vorangestellt werden. Wenn ein "" oder ein '\' gesucht werden soll, muss diesem ein '\' vorangestellt werden.

    Hinweis: Es reicht die Eingabe des eindeutigen Wortanfangs.

- Beispiele für den Einsatz des Ausgabefilters finden Sie im Abschnitt *Trace-Ausgabe filtern* auf Seite 378.

Erläuterungen zur Adressierung, Schreibweise und Befehlseingabe

- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden, solange sie eindeutig sind. Zum Beispiel kann der Befehl `sysinfo` zu `sys` verkürzt werden, oder aber `cd Management` zu `c ma`. Die Eingabe `cd /s` dagegen ist ungültig, da dieser Eingabe sowohl `cd /Setup` als auch `cd /Status` entspräche.
- Verzeichnisse können über die entsprechende SNMP-ID angesprochen werden. Der Befehl `cd /2/8/10/2` bewirkt z. B. das gleiche wie `cd /Setup/IP-Router/Firewall/Regel-Tabelle`.
- Mehrere Werte in einer Tabellezeile können mit **einem** Befehl verändert werden, z. B. in der Regeltabelle der IPv4-Firewall:
  - `set WINS UDP` setzt das Protokoll der Regel WINS auf UDP.
  - `set WINS UDP ANYHOST` setzt das Protokoll der Regel WINS auf UDP und die Destination auf ANYHOST.
  - `set WINS * ANYHOST` setzt ebenfalls die Destination der Regel WINS auf ANYHOST, durch das Sternchen wird das Protokoll unverändert übernommen.
- Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an. Die Destination hat in der Regeltabelle der Firewall z.B. die Nummer 4:
  - `set WINS {4} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST.
  - `set WINS {destination} ANYHOST` setzt auch die Destination der Regel WINS auf ANYHOST.
  - `set WINS {dest} ANYHOST` setzt die Destination der Regel WINS auf ANYHOST, weil die Angabe von `dest` hier ausreichend für eine eindeutige Spaltenbezeichnung ist.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.

Kommandospezifische Hilfe

- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Optionsschalter aufgerufen wird. Zum Beispiel zeigt der Aufruf `ping ?` die Optionen des eingebauten PING-Kommandos an.
- Eine vollständige Auflistung der zur Verfügung stehenden Kommandozeilen-Befehle erhalten Sie durch die Eingabe von `help` oder `?`.

Übersicht der Parameter im ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Telnet- oder Terminal-Verbindung sendet ein "ICMP Echo-Request"-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem "ICMP Echo-Reply". Ist der Zielrechner nicht erreichbar, antwortet das letzte Gerät vor dem Host mit "Network unreachable" (Netzwerk nicht erreichbar) oder "Host unreachable" (Gegenstelle nicht erreichbar).

Die Syntax des Ping-Kommandos lautet wie folgt:

```
ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] Destination
```

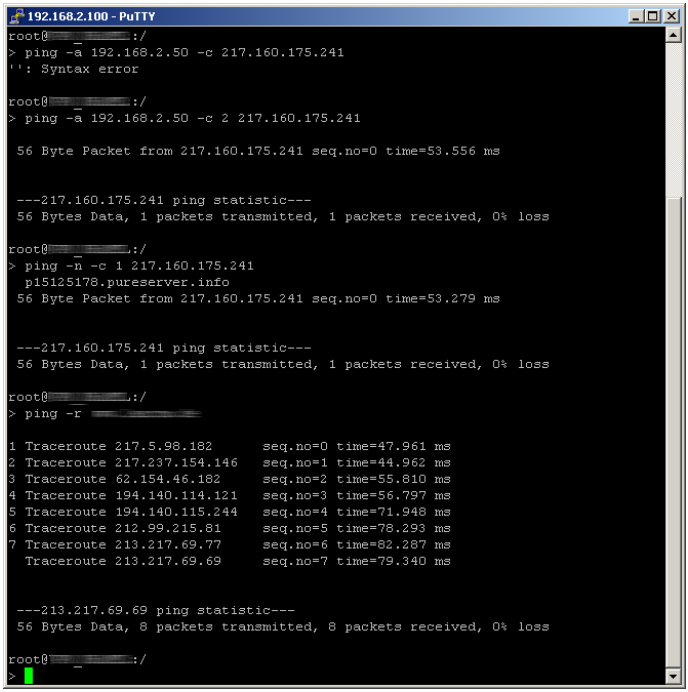
Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Parameter	*Bedeutung*
`-a a.b.c.d`	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Gerätes)
`-a INT`	Setzt die Intranet-Adresse des Gerätes als Absenderadresse
`-a DMZ`	Setzt die DMZ-Adresse des Gerätes als Absenderadresse
`-a LBx`	Setzt eine der 16 Loopback-Adressen im Gerät als Absenderadresse. Gültige Werte für x sind die Hexadezimalen Werte 0-f
`-6 <IPv6-Address>%<Scope>`	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus.
	Der Parameter-Bereich ist bei IPv6 von zentraler Bedeutung: Da ein IPv6-Gerät sich mit mehreren Schnittstellen (logisch oder physikalisch) pro Schnittstelle eine Link-Lokale-Adresse (fe80::/10) teilt, müssen Sie beim Ping auf eine Link-Lokale-Adresse immer den Bereich (Scope) angeben. Nur so kann das Ping-Kommando die Schnittstelle bestimmen, über die es das Paket senden soll.

Parameter	*Bedeutung*
	Den Namen der Schnittstelle trennen Sie durch ein Prozentzeichen (%) von der IPv6-Adresse. **Beispiele:** ▶ `ping -6 fe80::1%INTRANET` Ping auf die Link-Lokale-Adresse "fe80::1", die über die Schnittstelle bzw. das Netz "INTRANET" zu erreichen ist. ▶ `ping -6 2001:db8::1` Ping auf die globale IPv6-Adresse "2001:db8::1".
`-6 <Loopback-Interface>`	Setzt ein IPv6-Loopback-Interface als Absenderadresse.
`-f`	flood ping: Sendet große Anzahl von Ping-Signalen in kurzer Zeit. Kann z. B. zum Testen der Netzwerkbandbreite genutzt werden. ACHTUNG: flood ping kann leicht als DoS Angriff fehlinterpretiert werden.
`-n`	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück
`-o`	Schickt nach einer Antwort sofort eine weitere Anfrage
`-q`	Ping-Kommando liefert keine Ausgaben auf der Konsole
`-r`	Wechselt in Traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt
`-s n`	Setze Größe der Pakete auf n Byte (max. 65500)
`-i n`	Zeit zwischen den einzelnen Paketen in Sekunden
`-c n`	Sende n Ping-Signale
`Destination`	Adresse oder Hostnamen des Zielcomputers

Parameter	*Bedeutung*
`stop /<RETURN>`	Die Eingabe von “stop” oder das Drücken der RETURN-Taste beenden das Ping-Kommando

Tabelle 3: Übersicht aller optionalen Parameter im ping-Befehl



Übersicht der Parameter im trace-Befehl

Hinweis: Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Kommandozeile angezeigt werden.

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`Status`	Status-Meldungen der Verbindungen
`Fehler`	Fehler-Meldungen der Verbindungen
`PPP`	Verhandlung des PPP-Protokolls

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`LCR`	Least-Cost-Router
`Script`	Script-Verhandlung
`Firewall`	Zeigt die Aktionen der Firewall
`RIP`	IP Routing Information Protocol
`ARP`	Address Resolution Protocol
`ICMP`	Internet Control Message Protocol
`IP-Masquerading`	Vorgänge im Masquerading-Modul
`DHCP`	Dynamic Host Configuration Protocol
`NetBIOS`	NetBIOS-Verwaltung
`DNS`	Domain Name Service Protocol
`Paket-Dump`	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
`ATM-Cell`	ATM-Paketebene
`ATM-Error`	ATM-Fehler
`SMTP-Client`	E-Mail-Verarbeitung des integrierten Mail-Clients
`Mail-Client`	E-Mail-Verarbeitung des integrierten Mail-Clients
`SNTP`	Simple Network Time Protokoll
`NTP`	Timeserver Trace
`Connact`	Meldungen aus dem Aktivitätsprotokoll
`Cron`	Aktivitäten der Zeitautomatik (Cron-Tabelle)
`RADIUS`	RADIUS-Trace
`Serial`	Informationen über den Zustand der seriellen Schnittstelle
`USB`	Informationen über den Zustand der USB-Schnittstelle
`Load-Balancer`	Informationen zum Load Balancing
`VRRP`	Informationen über das Virtual Router Redundancy Protocol
`Ethernet`	Informationen über die Ethernet-Schnittstellen
`VLAN`	Informationen über virtuelle Netzwerke
`IGMP`	Informationen über das Internet Group Management Protocol
`WLAN`	Informationen über die Aktivitäten in den Funknetzwerken

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`WLAN-ACL`	Status-Meldungen über MAC-Filterregeln. **Hinweis:** Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.
`IAPP`	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
`DFS`	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
`Bridge`	Informationen über die WLAN-Bridge
`EAP`	Trace zum EAP, dem bei WPA/802.11i und 802.1x verwendeten Protokoll zur Schlüsselaushandlung
`Spgtree`	Informationen zum Spanning Tree Protokoll
`LANAUTH`	LAN-Authentifizierung (z. B. Public Spot)
`SIP-Packet`	SIP-Informationen, die zwischen einem VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
`VPN-Status`	IPSec und IKE Verhandlungen
`VPN-Packet`	IPSec und IKE Pakete
`GRE`	Meldungen zu GRE-Tunneln
`XML-Interface-PbSpot`	Meldungen des Public-Spot-XML-Interfaces
`hnat`	Informationen zum Hardware-NAT
`IPv6-Config`	Informationen über die IPv6-Konfiguration
`IPv6-Firewall`	Ereignisse der IPv6-Firewall
`IPv6-Interfaces`	Informationen der IPv6-Schnittstellen
`IPv6-LAN-Packet`	Datenpakete über die IPv6-LAN-Verbindung
`IPv6-Router`	Informationen über das IPv6-Routing
`IPv6-WAN-Packet`	Datenpakete über die IPv6-WAN-Verbindung

Tabelle 4: Übersicht aller durchführbaren Traces

Übersicht der capwap-Parameter im show-Befehl

Über die Kommandozeile lassen sich folgende Informationen zum CAPWAP-Dienst aufrufen:

Parameter	*Bedeutung*
`-addresses [<IfcNum>]`	Zeigt die Adresstabellen eines einzelnen oder aller WLC-Tunnel. Im Falle eines einzelnen WLC-Tunnels geben Sie für `<IfcNum>` die Nummer der logischen WLC-Tunnel-Schnittstelle an, z. B. `10`.
`-groups`	Zeigt Informationen zu einzelnen oder allen vorhandenen Zuweisungs-/Tag-Gruppen.

Tabelle 5: Übersicht aller capwap-Parameter im show-Befehl

Den Befehl `show capwap groups` erweitern Sie um die nachfolgend gelisteten Parameter, wodurch sich der Umfang der angezeigten Informationen regulieren lässt:

Parameter	*Bedeutung*
`all`	Zeigt die im Setup-Menü konfigurierten Namen und die geräteinternen Namen sämtlicher eingerichteten Zuweisungs-/Tag-Gruppen sowie der Default-Gruppe. Die Default-Gruppe stellt eine interne Gruppe dar, die sämtliche APs enthält.
`<group1> <group2> <…>`	Zeigt alle APs der betreffenden Zuweisungs-/Tag-Gruppen.
`-l <location>`	Zeigt alle APs des betreffenden Standorts.
`-c <country>`	Zeigt alle APs des betreffenden Landes.
`-i <city>`	Zeigt alle APs der betreffenden Stadt.
`-s <street>`	Zeigt alle APs des betreffenden Straßen.
`-b <building>`	Zeigt alle APs des betreffenden Gebäudes.
`-f <floor>`	Zeigt alle APs der betreffenden Etage.
`-r <room>`	Zeigt alle APs der betreffenden Raumbezeichnung.
`-d <device>`	Zeigt alle APs, die den angegebenen Gerätenamen tragen.
`-v <firmware>`	Zeigt alle APs, welche die angegebene Firmware besitzen. Geben Sie dazu für `<firmware>` die Versionsnummer gefolgt von der Build-Nummer an, z. B. `9.00.0001`.
`-x <firmware>`	Zeigt alle APs, deren Firmware-Version kleiner ist als die auf dem aktuellen Gerät installierte.
`-y <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder kleiner ist als die auf dem aktuellen Gerät installierte.
`-z <firmware>`	Zeigt alle APs, deren Firmware-Version größer ist als die auf dem aktuellen Gerät installierte.
`-t <firmware>`	Zeigt alle APs, deren Firmware-Version gleich groß oder größer ist als die auf dem aktuellen Gerät installierte.

Parameter	*Bedeutung*
`-n <intranet>`	Zeigt alle APs, deren IP zur angegebenen Intranet-Adresse gehört.
`-p <profile>`	Zeigt alle APs, denen das angegebene WLAN-Profil zugeordnet ist.
`rmgrp <group1 intern_name> <group2 intern_name> …`	Löscht die Gruppe(n) mit dem angegebenen internen Namen aus dem Arbeitsspeicher des Gerätes. Nutzen Sie diesen Befehl, um die Arbeitsspeicher freizugeben, falls eine zu hohe Zahl von Gruppen die Perfomanz des Gerätes verschlechtert. Der Eintrag im Setup-Menü bleibt von dieser Aktion unberührt.
`resetgrps`	Löscht alle Gruppen bis auf die Default-Gruppe.

Tabelle 6: Übersicht aller 'capwap group'-Parameter im show-Befehl

Für die Standort-Informationen wertet das Gerät die in der Access-Point-Tabelle unter **Standort** eingetragenen Informationen aus. Folgende Feld-Bezeichnungen stehen Ihnen zur Verfügung:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

Der Standort-Eintrag `co=Deutschland,ci=Aachen` z. B. ermöglicht Ihnen, über den Befehl `+show capwap group -i Aachen` an der Konsole alle vom WLC verwalteten APs in Aachen aufzulisten.

Befehlsbeispiele

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```

Übersicht der IPv6-spezifischen show-Befehle

Über die Kommandozeile besteht die Möglichkeit, diverse IPv6-Funktionen abzufragen. Folgende Kommando-Funktionen stehen Ihnen zur Verfügung:

- *IPv6-Adressen*: `show ipv6-adresses`
- *IPv6-Präfixe*: `show ipv6-prefixes`
- *IPv6-Interfaces*: `show ipv6-interfaces`
- *IPv6-Neighbour Cache*: `show ipv6-neighbour-cache`
- *IPv6-DHCP-Server*: `show dhcp6-server`
- *IPv6-DHCP-Client*: `show dhcpv6-client`
- *IPv6-Route*: `show ipv6-route`

Darüber hinaus lässt sich die IPv6-Kommunikation über das `trace`-Kommando mitverfolgen.

IPv6-Adressen

Der Befehl `show ipv6-adresses` zeigt eine aktuelle Liste der genutzten IPv6-Adressen. Diese ist nach Interfaces sortiert. Hierbei ist zu beachten, dass ein Interface mehrere IPv6-Adressen haben kann. Eine dieser Adressen ist immer die Link lokale Adresse, welche mit `fe80:` beginnt.

Die Ausgabe ist folgendermaßen formatiert:

```
<Interface> :
<IPv6-Adresse>, <Status>, <Attribut>, (<Typ>)
```

Ausgabe	*Erläuterung*
Interface	Der Name des Interfaces
IPv6-Adresse	Die IPv6-Adresse
Status	Das Statusfeld kann folgende Werte beinhalten: ▶ TENTATIVE Die Duplicate Address Detection (DAD) prüft die Adresse momentan. Sie steht daher einer Verwendung für Unicast noch nicht zu Verfügung. ▶ PREFERRED Die Adresse ist gültig ▶ DEPRICATED

Ausgabe	*Erläuterung*
	Die Adresse ist noch gültig, befindet sich aber im Status der Abkündigung. Eine Adresse mit dem Status PREFERRED wird für die Kommunikation bevorzugt. ▶ INVALID Die Adresse ist ungültig und kann nicht zur Kommunikation genutzt werden. Eine Adresse erhält diesen Status, nachdem die Lifetime ausgelaufen ist.
Attribut	Zeigt ein Attribut der IPv6-Adresse an. Mögliche Attribute sind: ▶ None keine besonderen Eigenschaften ▶ (ANYCAST) es handelt sich um eine Anycast-Adresse ▶ (AUTO CONFIG) es handelt sich um eine über die Autokonfiguration bezogene Adresse ▶ (NO DAD PERFORMED) es wird keine DAD durchgeführt
Type	Der Typ der IP-Adresse

Tabelle 7: Bestandteile der Kommandozeilenausgabe `show ipv6-adresses`

IPv6-Präfixe

Der Befehl `show ipv6-prefixes` zeigt alle bekannten Präfixe an. Die Sortierung erfolgt nach folgenden Kriterien:

Delegated prefixes
Alle Präfixe, die der Router delegiert bekommen hat.

Advertised prefixes
Alle Präfixe, die der Router in seinen Router-Advertisements ankündigt.

Deprecated prefixes
Alle Präfixe, die derzeit abgekündigt werden. Diese sind noch funktional, werden allerdings nach einem bestimmten Zeitrahmen gelöscht.

IPv6-Interfaces

Der Befehl `show ipv6-interfaces` zeigt eine Liste der IPv6 Interfaces und deren jeweiligen Status.

Die Ausgabe ist folgendermaßen formatiert:

<Interface> : <Status>, <Forwarding>, <Firewall>

Ausgabe	*Erläuterung*
Interface	Der Name des Interfaces
Status	Der Status des Interfaces. Mögliche Einträge sind: ▶ oper Status is up ▶ oper Status is down
Forwarding	Der Forwarding Status des Interfaces. Mögliche Einträge sind: ▶ forwarding is enabled ▶ forwarding is disabled
Firewall	Der Status der Firewall. Mögliche Einträge sind: ▶ firewall is enabled ▶ firewall is disabled

Tabelle 8: Bestandteile der Kommandozeilenausgabe `show ipv6-interfaces`

IPv6-Neighbour Cache

Der Befehl `show ipv6-neighbour-cache` zeigt den aktuellen Neighbour Cache an.

Die Ausgabe ist folgendermaßen formatiert:

```
<IPv6-Adresse> iface <Interface> lladdr <MAC-Adresse> (<Switchport>)
<Gerätetyp> <Status> src <Quelle>
```

Ausgabe	*Erläuterung*
IPv6-Adresse	Die IPv6-Adresse des benachbarten Gerätes
Interface	Das Interface, über das der Nachbar erreichbar ist
MAC-Adresse	Die MAC-Adresse des Nachbarn
Switchport	Der Switchport, auf dem der Nachbar festgestellt wurde
Gerätetyp	Gerätetyp des Nachbarn (Host oder Router)
Status	Der Status der Verbindung zum benachbarten Gerät. Mögliche Einträge sind: ▶ INCOMPLETE Die Auflösung der Adresse ist noch im Gange und die Link Layer Adresse des Nachbarn wurde noch nicht bestimmt.

Ausgabe	*Erläuterung*
	▶ REACHABLE Der Nachbar ist in den letzten zehn Sekunden erreichbar gewesen. ▶ STALE Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber eine Aktualisierung wird erst durchgeführt, wenn versucht wird ihn zu erreichen. ▶ DELAY Der Nachbar ist nicht länger als REACHABLE qualifiziert, aber es wurden vor kurzem Daten an ihn gesendet und auf Verifikation durch andere Protokolle gewartet. ▶ PROBE Der Nachbar ist nicht länger als REACHABLE qualifiziert. Es werden Neighbour Solicitation Probes an ihn gesendet um die Erreichbarkeit zu bestätigen.
Quelle	Die IPv6-Adresse, über die der Nachbar entdeckt wurde.

Tabelle 9: Bestandteile der Kommandozeilenausgabe `show ipv6-neighbour-cache`

IPv6-DHCP-Server

Der Befehl `show dhcpv6-server` zeigt den aktuellen Status des DHCP-Servers. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Server aktiv ist, welche DNS-Server und Präfixe er hat sowie welche Präferenz er für die Clients besitzt.

IPv6-DHCP-Client

Der Befehl `show dhcpv6-client` zeigt den aktuellen Status des DHCP-Clients. Die Anzeige beinhaltet Informationen darüber, auf welchem Interface der Client aktiv ist sowie darüber, welche DNS-Server und Präfixe er hat.

IPv6-Route

Der Befehl `show ipv6-route` zeigt die vollständige Routing-Tabelle für IPv6 an. Die Anzeigen kennzeichet die im Router fest eingetragenen Routen durch den Anhang [static] und die dynamisch gelernten Routen durch den Anhang [connected]. Die Loopback-Adresse ist durch [loopback] gekennzeichnet. Weitere automatisch generierte Adressen sind mit [local] markiert.

Umgebungsvariablen

Umgebungsvariablen sind geräteeigene globale Variablen mit vordefinierten Werten, die Sie überall an der Kommandozeile als dynamische Platzhalter einfügen können. Eine Übersicht der Umgebungsvariablen sowie deren Werte können Sie sich über die entsprechenden Kommandozeilen-Befehle ausgeben lassen (siehe unten).

Alle vordefinierten Umgebungsvariablen beginnen mit zwei Unterstrichen. In den Befehlen an der Kommandozeile leiten Sie die Variablen mit einem vorangestellten Dollarzeichen ein.

Variablenname	*Inhalt*
`__BLDDEVICE`	Das Sub-Projekt des Gerätes. Das Sub-Projekt besteht in der Regel aus einer Zeichenkette ohne Leerzeichen und steht für das Hardware-Modell des aktuellen Gerätes.
`__DEVICE`	Der Typ des Gerätes, so wie er z. B. in LANconfig oder auf dem Typenschild des Gerätes angezeigt wird.
`__FWBUILD`	Die Build-Nummer der aktuell im Gerät verwendeten Firmware. Die Build-Nummer ist eine vierstellige Zahl.
`__FWVERSION`	Die Versionsbezeichnung der aktuell im Gerät verwendeten Firmware in der Form 'x.yy'. Die Firmware-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
`__LDRBUILD`	Die Build-Nummer des aktuell im Gerät installierten Loaders. Die Build-Nummer ist eine vierstellige Zahl.
`__LDRVERSION`	Die Versionsbezeichnung des aktuell im Gerät installierten Loaders in der Form 'x.yy'. Die Loader-Version besteht aus der Major-Release vor dem Punkt und der Minor-Release nach dem Punkt.
`__MACADDRESS`	Der Typ des Gerätes, angegeben als 12-stellige Zeichenkette hexadezimaler Werte in Kleinschreibung ohne Trennzeichen.
`__SERIALNO`	Die Seriennummer des Gerätes.
`__SYSNAME`	Die Systembezeichnung des Gerätes.

Tabelle 10: Übersicht aller Umgebungsvariablen

Nutzen Sie die folgenden Befehle in der Kommandozeile, um Umgebungsvariablen anzuzeigen oder zu verändern:

- `printenv`: Zeigt alle Umgebungsvariablen und deren aktuelle Werte an. Wenn Sie einer oder mehrerne Umgebungsvariablen mit dem Befehl `setenv` einen Wert zugewiesen haben, zeigt die Ausgabe des Befehls

`printenv` im oberen Teil den benutzerdefinierten Wert und im unteren Teil den Standardwert an.

- `echo $__device`: Zeigt den aktuellen Werte einer einzelnen Umgebungsvariablen an, in diesem Beispiel den Wert der Variablen '__DEVICE'.
- `setenv __device MeinWert`: Setzt den Wert einer Umgebungsvariablen auf den gewünschten Wert.
- `unsetenv __device`: Setzt den Wert einer Umgebungsvariablen auf den Standardwert zurück.

Tastenkombinationen für die Kommendozeile

Mit den folgenden Tastenkürzel lassen sich die Befehle auf der Kommandozeile bearbeiten. Die "ESC key sequences" zeigen zum Vergleich die Tastenkombinationen, die auf typischen VT100/ANSI-Terminals verwendet werden.

Tastenkürzel	*Esc key sequences*	*Beschreibung*
Pfeil nach oben	ESC [A	Springt in der Liste der letzten ausgeführten Befehle eine Position nach oben, in Richtung älterer Befehle.
Pfeil nach unten	ESC [B	Springt in der Liste der letzten ausgeführten Befehle eine Position nach unten, in Richtung neuerer Befehle.
Pfeil nach rechts	Ctrl-F ESC [C	Bewegt die Einfügemarke eine Position nach rechts.
Pfeil nach links	Ctrl-B ESC [D	Bewegt die Einfügemarke eine Position nach links.
Home oder Pos1	Ctrl-A ESC [A ESC [1˜ (	Bewegt die Einfügemarke an das erste Zeichen der Zeile.
Ende	Ctrl-E ESC [F ESC OF ESC [4˜	Bewegt die Einfügemarke an das letzte Zeichen der Zeile.
Einfg	ESC [ESC [2˜	Schaltet um zwischen Einfügemodus und Überschreibemodus.
Entf	Ctrl-D ESC <BS> ESC [3˜	Löscht das Zeichen an der aktuellen Position der Einfügemarke oder beendet die Terminalsitzung, wenn die Zeile leer ist.
erase	<BS><DEL>	Löscht das nächste Zeichen links neben der Einfügemarke.
erase-bol	Ctrl-U	Löscht alle Zeichen links neben der Einfügemarke.
erase-eol	Ctrl-K	Löscht alle Zeichen rechts neben der Einfügemarke.
Tabulator		Komplettiert die Eingabe von der aktuellen Position der Einfügemarke zu einem Befehl oder Pfad der LCOS-Menüstruktur:

Tastenkürzel	*Esc key sequences*	*Beschreibung*
		1. Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. **2.** Wenn es mehrere Möglichkeiten gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Mit einem erneuten Druck auf die Tab-Taste wird eine Liste mit allen Möglichkeiten angezeigt, mit denen die Eingabe vervollständigt werden kann. Geben Sie dann z. B. einen weiteren Buchstaben ein, um ein eindeutiges Vervollständigen der Eingabe zu ermöglichen. **3.** Wenn es keine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird dies durch einen Hinweiston beim Drücken der Tab-Taste angezeigt. Es werden keine weiteren Aktionen ausgeführt. Weitere Informationen zu den Besonderheiten der Tab-Taste beim Skripten finden Sie gesondert im Abschnitt *Tab-Kommando beim Scripting* auf Seite 82.

Tabelle 11: Übersicht der Tastaturbefehle für die Kommandozeile

Tab-Kommando beim Scripting

Das `tab`-Kommando aktiviert beim Scripten die gewünschten Spalten einer Tabelle für das nachfolgende `set`-Kommando.

Bei der Konfiguration über ein Kommandozeilen-Tool ergänzen Sie das set-Kommando in der Regel durch die Werte, die Sie den entsprechenden Spalten des Tabelleneintrags zuweisen möchten.

Die Werte für die Performance-Einstellungen eines WLAN-Interfaces setzen Sie z. B. wie folgt:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?

Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 chars from: 1234567890

> set WLAN-1 Yes *
```

In diesem Beispiel umfasst die Tabelle Performance drei Spalten:

- Ifc, also die gewünschte Schnittstelle

- Aktivieren oder Deaktivieren von QoS
- gewünschter Wert für das TX-Bursting

Mit dem Kommando `set WLAN-1 Yes *` aktivieren Sie für das Interface WLAN-1 die QoS-Funktion, den Wert für Tx-Bursting lassen Sie durch die Angabe des * unverändert.

Diese Schreibweise des `set`-Kommandos eignet sich gut für Tabellen mit wenigen Spalten. Tabellen mit sehr vielen Spalten hingegen stellen eine große Herausforderung dar. Die Tabelle unter **Setup** > **Interfaces** > **WLAN** > **Transmission** umfasst z. B. 22 Einträge:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?

Possible Entries for columns in Transmission:
[1][Ifc]               : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17), WLAN-1-4
 (18), WLAN-1-5 (19), WLAN-1-6 (20), WLAN-1-7 (21), WLAN-1-8 (22)
[2][Packet-Size]        : 5 chars from: 1234567890
[3][Min-Tx-Rate]        : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M
(8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[9][Max-Tx-Rate]        : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6), 6M
(8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[4][Basic-Rate]         : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M (9),
 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[19][EAPOL-Rate]        : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M (6),
 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15),
 HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35),
 HT-2-13M (36), HT-2-26M (37), HT-2-39M (38), HT-2-52M (39), HT-2-78M (40),
 HT-2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]      : 3 chars from: 1234567890
[11][Soft-Retries]      : 3 chars from: 1234567890
[7][11b-Preamble]       : Auto (0), Long (1)
[16][Min-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3),
 MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15 (8)
[17][Max-HT-MCS]        : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10 (3),
 MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15 (8)
[23][Use-STBC]          : No (0), Yes (1)
[24][Use-LDPC]          : No (0), Yes (1)
[13][Short-Guard-Interval]  : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]   : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
```

```
[20][Max-Aggr.-Packet-Count]    : 2 chars from: 1234567890
[6][RTS-Threshold]      : 5 chars from: 1234567890
[10][Min-Frag-Len]      : 5 chars from: 1234567890
[21][ProbeRsp-Retries]  : 3 chars from: 1234567890
```

Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 * * * * * * * * * * * * No
```

Hinweis: Die Sternchen für die Werte nach der Spalte für das Short-Guard-Interval sind in diesem Beispiel nicht erforderlich, die Spalten werden automatisch beim Setzen der neuen Werte ignoriert.

Alternativ zu dieser eher unübersichtlichen und fehleranfälligen Schreibweise definieren Sie im ersten Schritt mit dem `tab`-Kommando, welche Spalten der nachfolgende `set`-Befehl verändert:

```
> tab Ifc Short-Guard-Interval
> set WLAN-1-3 No
```

Der `tab`-Befehl erlaubt dabei auch, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> tab Ifc Short-Guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```

Hinweis: Je nach Hardware-Modell enthalten die Tabellen nur einen Teil der Spalten. Der `tab`-Befehl ignoriert Spalten, die in der Tabelle des jeweiligen Geräts fehlen. So haben Sie die Möglichkeit, gemeinsame Scripte für unterschiedliche Hardware-Modelle zu entwickeln. Die `tab`-Anweisungen in den Scripten referenzieren dabei alle maximal erforderlichen Spalten. Je nach Modell führt das Script die `set`-Anweisungen allerdings nur für die tatsächlich vorhandenen Spalten aus.

Den `tab`-Befehl können Sie auch verkürzt über geschweifte Klammern darstellen. Mit dem folgenden Befehl setzen Sie in der Transmission-Tabelle das Short-Guard-Interval für das Interface WLAN-1-3 auf den Wert Nein:

```
> set WLAN-1-3 {short-guard} No
```

Die geschweiften Klammern ermöglichen ebenfalls, die Reihenfolge der gewünschten Spalten zu verändern. Das folgende Beispiel setzt für das Interface WLAN-1-3 den Wert für das Short-Guard-Interval auf `Nein` und den Wert für Use-LDPC auf `Ja`, obwohl die Tabelle die entsprechenden Spalten in einer anderen Reihenfolge anzeigt:

```
> set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

Funktionstasten für die Konsole

Mit den Funktionstasten (den F-Tasten) auf der Tastatur haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen.

Sie konfigurieren diese Funktion über das Setup-Menü unter **Config** > **Funktionstasten**. Wählen Sie dazu aus dem Auswahlmenü **Taste** eine der Funktionstasten F1 bis F12 aus und tragen Sie unter **Abbildung** die Befehlssequenz in der Form ein, wie Sie sie auch auf der Kommandozeile eingeben würden. Erlaubt sind alle an dem HiLCOS-Kommandozeilen-Interface möglichen Befehle bzw. Tastenkombinationen.

Besonderheiten beim Caret-Zeichen

Sofern Sie in Ihren Befehlen das Caret-Zeichen (^) verwenden, beachten Sie dabei, dass dieses auch dafür genutzt wird, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden:

- ^A steht für Strg-A (ASCII 1)
- ^Z steht für Strg-Z (ASCII 26)
- ^[steht für Escape (ASCII 27)
- ^^ Ein doppeltes Caret-Zeichen steht für das Caret-Zeichen selbst.

Hinweis: Wenn Sie ein Caret-Zeichen direkt gefolgt von einem anderen Zeichen in ein Dialogfeld oder in einem Editor eingeben, wird das Betriebssystem diese Sequenz möglicherweise als ein anderes Sonderzeichen deuten. Aus der Eingabe von `Caret-Zeichen + A` macht ein Windows-Betriebssystem z. B. ein Â. Um das Caret-Zeichen selbst aufzurufen, geben Sie vor dem folgenden Zeichen ein Leerzeichen ein: Aus `Caret-Zeichen + Leerzeichen + A` wird dann die Sequenz ^A.

2.2.4 SNMP Management-Programm

Das Simple Network Management Protocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netzwerk von einer zentralen Instanz aus. Seit der ersten Veröffentlichung im Jahr 1988 entwickelte es sich im Laufe der Zeit weiter, um einer immer komplexeren Netzwerk-Infrastruktur sowie gesteigerten Ansprüchen an Sicherheit, Flexibilität und Komfort gerecht zu werden.

HiLCOS unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

Neben den LCMS-Tools (LANCOM Mananagement System) gibt es noch weitere Konfigurations- und Management-Programme, um mit einem entsprechenden SNMP-Agent ausgestattete Netzwerkkomponenten wie Router, Switche, Drucker, Firewalls etc. über SNMP zu überwachen oder zu steuern. Hierzu zählen insbesondere kommerzielle Programme, allerdings existieren auch zahlreiche Anwendungen auf Open-Source-, Freeware- oder Shareware-Basis.

Die für die Verwendung in SNMP-Programmen benötigte Geräte-MIB-Datei (Management Information Base) lässt sich bequem über WEBconfig (vgl. *SNMP-Geräte-MIB abrufen* auf Seite 50) oder an der Konsole über den Befehl `readmib` erzeugen.

2.3 LANCOM Layer 2 Management Protokoll (LL2M)

2.3.1 Einleitung

Alle Wege zur Konfiguration eines Geräts setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem Gerät voraus. Egal ob LANconfig, WEBconfig oder Telnet – ohne IP-Verbindung können keine Befehle zur Konfiguration an das Gerät übertragen werden. Im Falle einer Fehlkonfiguration der TCP/IP-Einstellungen oder der VLAN-Parameter kann es vorkommen, dass diese benötigte IP-Verbindung nicht mehr hergestellt werden kann. In diesen Fällen hilft nur der Zugriff über die serielle Konfigurationsschnittstelle (nicht bei allen Geräten verfügbar) oder ein Reset des Gerätes auf den Auslieferungszustand. Beide Möglichkeiten setzen aber den physikalischen Zugriff auf das Gerät voraus, der z. B. bei der verdeckten Montage von Access Points nicht immer gegeben ist oder in größeren Szenarien erheblichen Aufwand darstellen kann.

Um auch ohne IP-Verbindung einen Konfigurationszugriff auf ein Gerät zu ermöglichen wird das **LANCOM Layer 2 Management Protokoll (LL2M)** verwendet. Dieses Protokoll benötigt nur eine Verbindung auf Layer 2, also auf dem direkt oder über Layer-2-Switches angebundenen Ethernet, um eine Konfigurationssitzung aufzubauen. LL2M-Verbindungen werden auf LAN- oder WLAN-Verbindungen unterstützt, nicht jedoch über das WAN. Die Verbindungen über LL2M sind passwortgeschützt und gegen Replay-Attacken resistent.

LL2M etabliert dazu eine Client-Server-Struktur: Der LL2M-Client schickt Anfragen oder Befehle an den LL2M-Server, der die Anfragen beantwortet oder die Befehle ausführt. Der LL2M-Client ist im HiLCOS integriert und wird über die Kommandozeile ausgeführt. Der LL2M-Server ist ebenfalls im HiLCOS integriert und wird üblicherweise nur für eine kurze Zeitspanne nach dem Einschalten des Gerätes aktiviert. In diesem Zeitfenster kann ein Administrator mit Hilfe des LL2M-Clients Änderungen an der Konfiguration des Gerätes mit dem LL2M-Server vornehmen.

2.3.2 Konfiguration des LL2M-Servers

Die Aktivierung und Konfiguration des LL2M-Servers erfolgt ausschließlich über das Setup-Menü eines Gerätes. Die nachfolgenden Handlungsschritte zeigen Ihnen, welche Einstellungen erforderlich sind:

1. Wechseln Sie WEBconfig oder ein Terminalprogramm in den Setup-Menü-Zweig **Config** > **LL2M**.
2. Setzen Sie den Parameter **In-Betrieb** auf **ja**.
3. Tragen für das **Zeit-Limit** eine eine Zeitspanne in Sekunden ein, in der ein LL2M-Client den LL2M-Server nach dem Booten/Einschalten des Gerätes ansprechen kann.
   Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert. Der Wert '0' deaktiviert das Zeit-Limit; in diesem Zustand bleibt der LL2M-Server dauerhaft aktiv.

Fertig!

2.3.3 Befehle für den LL2M-Client

Für jeden LL2M-Befehl wird ein verschlüsselter Tunnel aufgebaut, der die bei der Übertragung übermittelten Anmeldeinformationen schützt. Zur Nutzung des integrierten LL2M-Clients starten Sie eine Terminalsitzung auf einem Gerät, das lokalen Zugriff über das verfügbare physikalische Medium (LAN, WLAN) auf den LL2M-Server hat. In dieser Konsolensitzung können Sie den LL2M-Server über die folgenden Befehle ansprechen:

Hinweis: Zum Ausführen der Befehle für den LL2M-Client müssen Sie über Root-Rechte auf dem LL2M-Server verfügen.

`LL2Mdetect`

Mit diesem Befehl schickt der LL2M-Client eine SYSINFO-Anfrage an den LL2M-Server. Der Server sendet daraufhin seine Systeminformationen wie Hardware, Seriennummer etc. zur Anzeige an den Client zurück. Der LL2Mdetect-Befehl lässt sich mit folgenden Parametern einschränken:

`-a <MAC-Adresse>`

Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse geben Sie in der Form `00a057010203`, `00-a0-57-01-02-03` oder `00:a0:57:01:02:03` an.

Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder via `-b` alternativ als Broadcast) an alle LL2M-fähigen Geräte. Einzelne Stellen der MAC-Adresse können mit einem * oder x als Platzhalter besetzt werden, um Gruppen von MAC-Adressen anzusprechen, z. B. `00-a0-57-xx-xx-xx` für alle Geräte-MAC-Adressen.

Hinweis: In einer Befehlszeile mit mehreren Parametern **muss** `-a` der abschließende Parameter sein. Eine andere Reihenfolge ist nicht zulässig.

`-b`

Versendet die LL2Mdetect-Anfrage explizit als Broadcast und nicht als Multicast.

`-f <Version>`

Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein.

`-r <Hardware-Release>`

Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein.

`-s <Serialnumber>`

Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein.

`-t <Hardware-Type>`

Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein.

`-v <VLAN-ID>`

Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet.

Die Befehlszeile `ll2mdetect -r A` zum Beispiel versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release 'A'. Die Antwort des LL2M-Servers enthält dann die folgenden Angaben:

- Name des Gerätes
- Gerätetyp
- Seriennummer
- MAC-Adresse
- Hardware-Release
- Firmware-Version mit Datum

LL2Mexec

Mit diesem Befehl schickt der LL2M-Client ein einzeiliges Kommando zur Ausführung an den LL2M-Server. Mehrere Kommandos lassen sich durch Semikola getrennt in einem LL2M-Befehl kombinieren. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes zur Anzeige an den LL2M-Client übertragen. Der LL2Mexec-Befehl entspricht folgender Syntax:

```
ll2mexec <User>[:<Password>]@<MAC-Address>
```

Der LL2Mexec-Befehl lässt sich mit folgenden Parametern einschränken:

`-i <WLAN-Interface>`

Versendet den LL2Mexec-Befehl nur über das angegebene WLAN-Interface.

`-v <VLAN-ID>`

Versendet den LL2Mexec-Befehl nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID des ersten definierten IP-Netzwerks verwendet.

Die Befehlszeile `ll2mexec root@00a057010203 set /setup/name MyDevice` zum Beispiel meldet den LL2M-Client als 'root' auf dem LL2M-Server mit der MAC-Adresse '00a057010203' an. Da das Kennwort weggelassen wurde, sucht das Gerät zunächst nach dem entsprechenden Nutzernamen in der lokalen Datenbank und setzt automatisch das für diesen Nutzer gespeicherte Kennwort ein. Wird auch der Nutzername weggelassen, werden die Anmeldedaten des aktuell für die CLI-Sitzung registrierten Nutzers verwen-

det. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert 'MyDevice'.

2.4 Speichern und Laden von Gerätekonfiguration und Skriptdateien

Die Konfigurationsdatei eines Gerätes umfasst seine kompletten Einstellungen. Und mit Hilfe von Script-Dateien lassen sich die Einstellungen eines Gerätes automatisiert verwalten. Zum Schutz dieser Dateien vor unberechtigtem Zugriff oder Übertragungsfehlern ist es möglich, sie verschlüsselt und mit einer Prüfsumme versehen aus dem Gerät zu exportieren oder in das Gerät zu laden.

Es existieren somit grundsätzlich drei verschiedene Dateitypen:

- Keine Prüfsumme, keine Verschlüsselung: Eine Textdatei, deren Inhalt mit einem Texteditor lesbar ist.
- Prüfsumme: Die Textdatei enthält Informationen über die Prüfsumme sowie den Hash-Algorithmus zur Berechnung dieser Prüfsumme. Der Inhalt dieser Textdatei ist mit einem einfachen Texteditor lesbar.

  Hinweis: Ein LANconfig vor Version 9.10 erkennt auch Dateien mit Prüfsummen.

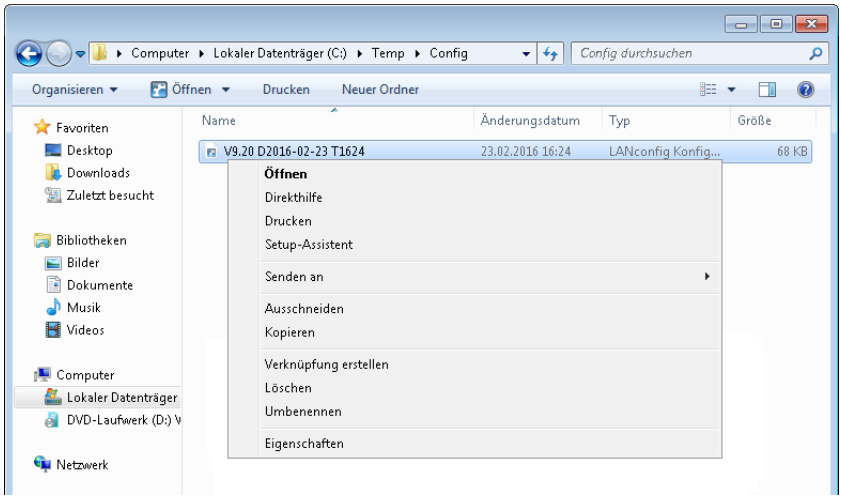
- Verschlüsselung: Vor dem Export verschlüsselt das Gerät die Datei mit einem vom Administrator gewählten Passwort. Die Textdatei enthält Informationen über den verwendeten Verschlüsselungsalgorithmus sowie eine Prüfsumme. Der Inhalt der Textdatei ist bis auf den Dateiheader mit einem Texteditor nicht mehr entzifferbar.

  Hinweis: Ein LANconfig vor Version 9.10 erkennt verschlüsselte Dateien nicht.

Hinweis: Die Dateiendungen dieser Dateien sind jeweils `.lcf` für Konfigurationsdateien oder `.lcs` für Skriptdateien. Die Erkennung, ob es sich um ver-

schlüsselte oder mit Prüfsummen versehene Dateien handelt, geschieht ausschließlich über den Dateiheader.

Über den Kontextdialog des Windows-Explorers können Sie die folgenden Funktionen ausführen:



Öffnen

Dieser Menüpunkt öffnet die Konfiguration der Datei über LANconfig.

Hinweis: Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

Direkthilfe

Dieser Menüpunkt öffnet einen Hilfetext, der Benutzerinformationen über den Umgang mit dieser Datei gibt.

Drucken

Mit diesem Menüpunkt drucken Sie die Datei aus.

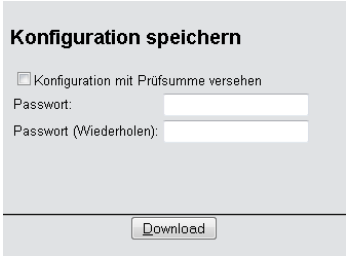
Setup-Assistent

Dieser Menüpunkt startet den LANconfig-Setup-Assistenten.

Hinweis: Dieser Punkt erscheint nur bei Konfigurations-Dateien mit der Endung `.lcf`.

2.4.1 Konfigurationsverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Konfigurationsdatei zu exportieren, wechseln Sie in die Ansicht **Dateimanagement** > **Konfiguration speichern**.



Folgende Optionen stehen zur Auswahl:

Keine Angaben

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei ohne Prüfsumme.

Konfiguration mit Prüfsumme versehen

Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei mit Prüfsumme.

Passwort

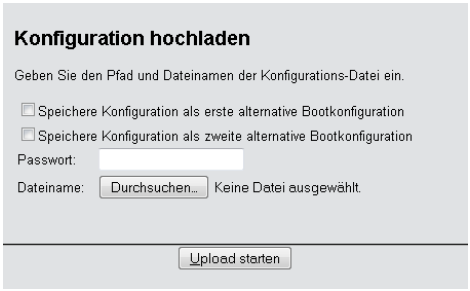
Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Um die Konfiguration über die Konsole zu sichern, verwenden Sie die folgenden Parameter:

- `readconfig`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.
- `readconfig -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.

- `readconfig -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.

Um über WEBconfig eine Konfigurationsdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Dateimanagement** > **Konfiguration hochladen**.

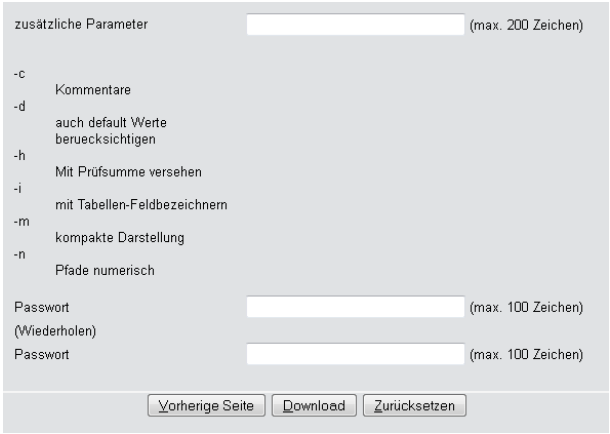


Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Konfigurationsdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

Hinweis: Weitere Informationen zu alternativen Boot-Konfigurationen finden Sie im Abschnitt *Alternative Boot-Config*.

2.4.2 Skriptverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Skriptdatei zu exportieren, wechseln Sie in die Ansicht **Dateimanagement** > **Konfigurations-Skript speichern**.



Folgende Optionen stehen zur Auswahl:

zusätzliche Parameter

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Skriptdatei ohne Prüfsumme.

Passwort

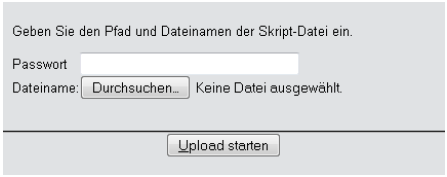
Geben Sie ein Passwort an, wenn Sie die Skriptdatei vor dem Download verschlüsseln möchten.

Um die Skriptdatei über die Konsole zu sichern, verwenden Sie z. B. die folgenden Parameter:

- `readscript`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.
- `readscript -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.
- `readscript -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.

Hinweis: Mehr Informationen zu den Parametern finden Sie im Abschnitt *Befehle für die Konsole* in der Zeile für `readscript`.

Um über WEBconfig eine Skriptdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Dateimanagement** > **Konfigurations-Skript anwenden**.

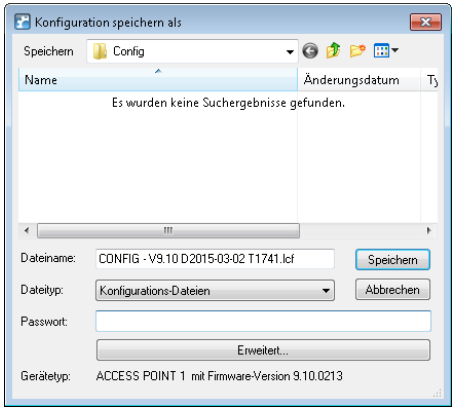


Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Skriptdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

2.4.3 Konfigurationsverwaltung über LANconfig

Um über LANconfig eine Konfigurationsdatei zu speichern, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, dessen Konfigura-

tion Sie speichern möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Als Datei sichern** den Speicherdialog.



Folgende Angaben stehen zur Auswahl:

Dateiname

LANconfig belegt den Dateinamen mit verschiedenen Angaben vor (u. a. Versionsnummer, Datum und Uhrzeit). Ändern Sie den Namen Ihren Anforderungen entsprechend.

Dateityp

Wählen Sie, ob es sich um eine Konfigurationsdatei oder etwas anderes handelt.

Passwort

Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Unter **Erweitert** bestimmen Sie weitere, optionale Parameter, die das Gerät beim automatischen Laden einer Konfigurations-Datei (Auto-Load) auswertet. Hiermit individualisieren Sie die Konfiguration.

Um über LANconfig eine Konfigurationsdatei in das Gerät zu laden, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, in das Sie eine Konfiguration laden möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Aus Datei wiederherstellen** den Uploaddialog.

Wählen Sie die gewünschte Konfigurationsdatei aus, geben Sie ggf. das benötigte Passwort an und klicken Sie auf **Öffnen**, um die Konfiguration in das Gerät zu laden.

2.5 Alternative Boot-Config

2.5.1 Einleitung

Das Verhalten der Geräte im Betrieb wird durch die Konfiguration bestimmt. Diese benutzerdefinierte Konfiguration wird in einem speziellen Bereich des Flash-Speichers abgelegt, der auch bei einem Neustart des Gerätes erhalten bleibt (Konfigurationsspeicher).

Im Auslieferungszustand ist der Konfigurationsspeicher leer, da das Gerät noch nicht über eine benutzerdefinierte Konfiguration verfügt. Im späteren Betrieb kann der Konfigurationsspeicher bei Bedarf durch einen Konfigurations-Reset wieder gelöscht werden. Wird ein Gerät mit leerem Konfigurationsspeicher gestartet oder gebootet, werden die Werte aus einer Boot-Konfiguration verwendet, welche die Standardwerte für das jeweilige Modell enthält.

Erst bei der Änderung von mindestens einem Konfigurationsparameter wird der Konfigurationsspeicher beschrieben. Dabei wird die komplette Konfiguration im Konfigurationsspeicher abgelegt. Auch wenn z. B. nur der Gerätename geändert wird, werden alle für das jeweilige Modell verfügbaren Parameter mit aktuellen Werten in der benutzerdefinierten Konfiguration gespeichert. Die Werte für die Parameter, die nicht geändert wurden, werden dabei aus einer Boot-Konfiguration übernommen.

Die Geräte können drei verschiedene Boot-Konfigurationen nutzen:

Werkseinstellungen

Diese enthält die Standardwerte für das jeweilige Modell im Auslieferungszustand. Die Standard-Boot-Konfiguration ist in der jeweiligen Firmware des Gerätes enthalten.

Kundenspezifische Standardeinstellungen

Diese enthält die kundenspezifischen Standardwerte für das jeweilige Modell für den Fall, dass der Konfigurationsspeicher leer ist, die Werkseinstellungen aber nicht verwendet werden sollen. Mit dieser

Funktion werden die Geräte persistent (über beliebig viele Boot-/Reset-Vorgänge hinweg) mit kundenspezifischen Vorgabewerten für den Neustart versehen. Die kundenspezifischen Standardeinstellungen werden bei einem Konfigurations-Reset **nicht** gelöscht. Die kundenspezifischen Standardeinstellungen werden auf dem ersten Boot-Speicherplatz abgelegt.

Rollout-Konfiguration

Diese Konfiguration wird in größeren Roll-Out-Szenarien verwendet, wenn für zahlreiche Geräte eine von den Werkseinstellungen abweichende Boot-Konfiguration verwendet werden soll. Die Rollout-Konfiguration muss durch eine entsprechende Bedienung des Reset-Tasters aktiviert werden. Die spezielle Rollout-Konfiguration wird auf dem zweiten Boot-Speicherplatz abgelegt.

2.5.2 Verwenden der Boot-Konfigurationen

Bei einem normalen Start nutzen die Geräte die möglichen Konfigurationen in einer definierten Reihenfolge:

1. Benutzerdefinierte Konfiguration (im Konfigurationsspeicher)
2. Kundenspezifische Standardeinstellungen (auf dem ersten Boot-Speicherplatz)
3. Werkseinstellungen (in der Firmware des Gerätes)

Die kundenspezifischen Standardeinstellungen werden also automatisch und vorrangig vor den Werkseinstellungen verwendet, wenn der Konfigurationsspeicher leer ist.

Besonderheiten der Rollout-Konfiguration

Die Verwendung der Rollout-Konfiguration wird über den Reset-Taster ausgelöst. Der Reset-Taster hat verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:

- **weniger als 5 Sekunden**:

  Booten (Neustart); dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal

kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.

- **mehr als 5 Sekunden** bis zum **ersten** Aufleuchten aller LEDs am Gerät:

  Konfigurations-Reset (Löschen des Konfigurationsspeichers) und anschließender Neustart. Damit werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn der erste Speicherplatz leer ist, werden die Werkseinstellungen geladen.

- **mehr als 15 Sekunden** bis zum **zweiten** Aufleuchten aller LEDs am Gerät:

  Aktivieren der Rollout-Konfiguration und Löschen der benutzerdefinierten Konfiguration. Nach dem Neustart wird die Rollout-Konfiguration (zweiter Speicherplatz) geladen. Das Laden der Rollout-Konfiguration wird angezeigt, indem alle LEDs des Geräts zweimal kurzzeitig rot aufleuchten. Wenn der zweite Speicherplatz leer ist, werden die Werkseinstellungen geladen.

Die Rollout-Konfiguration wird jeweils nur einmalig direkt nach dem Neustart verwendet, wenn der Reset-Taster für mehr als 15 Sekunden gedrückt wurde. Nach dem nächsten Neustart gilt automatisch wieder die normale Boot-Reihenfolge wie oben angegeben.

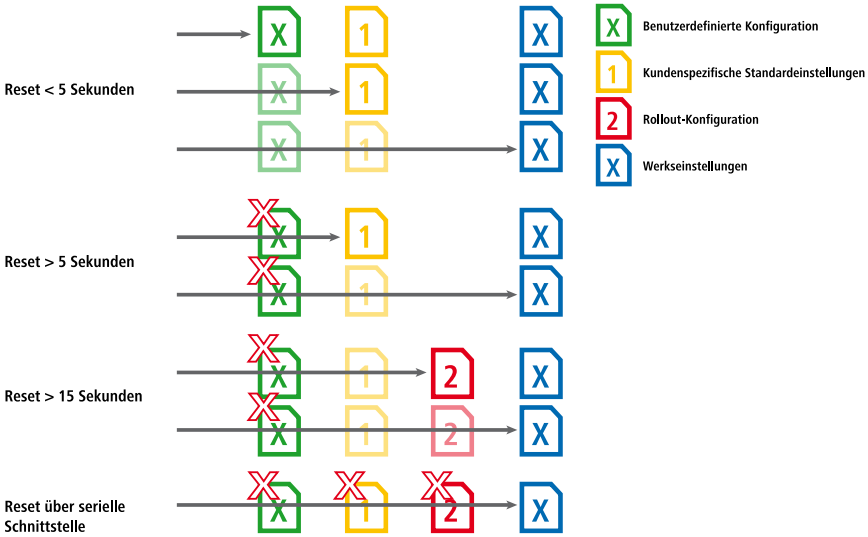
Hinweis: Wenn der Reset-Knopf in der Konfiguration deaktiviert ist (Einstellung **Ignorieren** oder **Nur-Booten**), wird das Laden der Rollout-Konfiguration unmöglich gemacht.

Beispiele

Die folgende Grafik zeigt, welche Konfiguration bei unterschiedlichen Reset-Vorgängen je nach Zustand des Gerätes geladen wird.

- Bei Drücken des Reset-Knopfs für **weniger als 5 Sekunden** wird die benutzerdefinierte Konfiguration geladen. Existiert keine benutzerdefinierte Konfiguration, greift das Gerät auf die kundenspezifischen Standardeinstellungen zurück. Sind diese ebenfalls nicht vorhanden, werden die Werkseinstellungen geladen.

- Bei Drücken des Reset-Knopfs für **mehr als 15 Sekunden** wird die benutzerdefinierte Konfiguration gelöscht und die Rollout-Konfiguration geladen. Wenn die Rollout-Konfiguration nicht vorhanden ist, werden die Werkseinstellungen geladen.



2.5.3 Speichern und Hochladen der Boot-Konfigurationen

Speichern

Die kundenspezifischen Standardeinstellungen als auch die Rollout-Konfiguration werden in einem komprimierten Format gespeichert. Über die Kommandozeile haben Sie die Möglichkeit, die aktuelle Konfiguration eines Gerätes wahlweise als kundenspezifische Standardeinstellung oder Rollout-Konfiguration abzulegen. Nutzen Sie dazu einen der folgenden Befehle:

```
bootconfig --savecurrent [1,2,all]
```

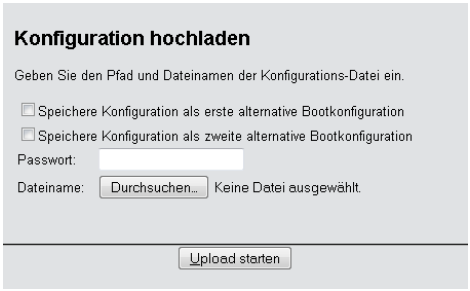
```
bootconfig -s [1,2,all]
```

Mit der entsprechenden Ziffer wird entweder der erste Boot-Speicherplatz für die kundenspezifischen Standardeinstellungen oder der zweite Boot-Speicherplatz für die Rollout-Konfiguration ausgewählt. Mit der Angabe des Parameters

`all` wird die aktuelle Konfiguration gleichzeitig in beide Speicherplätze geschrieben.

Hochladen

Die kundenspezifischen Standardeinstellungen oder die Rollout-Konfiguration können Sie in WEBconfig unter **Dateimanagement** > **Konfiguration hochladen** in das Gerät zu laden: Wählen Sie die zu verwendende Konfigurationsdatei aus und aktivieren Sie den Verwendungszweck als kundenspezifische Standardeinstellungen (erster Speicherplatz) und/oder Rollout-Konfiguration (zweiter Speicherplatz). Alternative Bootkonfigurationen müssen als *.lcf-Datei vorliegen.



Hinweis: Wenn beide Speicherplätze der Boot-Konfigurationen belegt (also kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration gespeichert) sind, lässt sich das Gerät nicht mehr über den Reset-Taster auf die Werkseinstellungen zurücksetzen. Gehen Sie für einen Geräte-Reset stattdessen so vor, wie unter *Firmware-Upload über Outband mit Rücksetzen der Konfiguration* auf Seite 108 beschrieben.

Hinweis: Für Geräte, die ausschließlich eine Boot-Konfigurationen erlauben, gilt die o. g. Einschränkung nicht. Sie lassen sich immer über den Reset-Taster auf die Werkseinstellungen zurücksetzen.

Hinweis: Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Konfigurationsdatei verschlüsselt ist.

2.5.4 Löschen der Boot-Konfigurationen

Die alternative und die spezielle Boot-Konfiguration können nicht über die normalen Datei-Funktionen gelöscht werden. Nutzen Sie stattdessen an der Kommandozeile einen der folgenden Befehle:

```
bootconfig --remove [1,2, all]
```

```
bootconfig -r [1,2, all]
```

Mit der entsprechenden Ziffer wird zu löschende Boot-Speicherplatz ausgewählt. Mit der Angabe des Parameters `all` werden gleichzeitig beide Speicherplätze gelöscht.

2.5.5 Verwendung von Zertifikaten

Für die Nutzung durch VPN und SSL/TLS nach einem Konfigurations-Reset kann ein **Standardzertifikat** als **PKCS#12-Container** im Gerät gespeichert werden. Dieses Standardzertifikat wird nur von den kundenspezifischen Standardeinstellungen und der Rollout-Konfiguration verwendet:

- Wenn die kundenspezifischen Standardeinstellungen geladen werden, wird das Standardzertifikat in den normalen Zertifikatsspeicher für VPN und SSL/TLS kopiert; somit steht es auch nach einem Reboot zur Verfügung.
- Wenn die Rollout-Konfiguration geladen wird, wird das Standardzertifikat für VPN verwendet, aber nicht kopiert; d. h. nach einem Neustart (auch ohne Konfigurations-Reset) kann das Gerät darauf nicht mehr zugreifen.

Das Standardzertifikat können Sie wahlweise über LANconfig oder WEBconfig in das Gerät laden.

Tipp: Das Hochladen von Zertifikaten ist u. a. im Kapitel *Zertifikate in das Gerät laden* auf Seite 860 erklärt.

2.6 FirmSafe

2.6.1 Einleitung

FirmSafe macht das Einspielen der neuen Software zur sicheren Sache: Die gerade verwendete Firmware wird dabei nicht einfach überschrieben, sondern es wird eine zweite Firmware zusätzlich im Gerät gespeichert (symmetrisches FirmSafe). Damit ist Ihr Gerät insbesondere auch gegen die Folgen eines Stromausfalls oder einer Verbindungsunterbrechung während des Firmware-Uploads geschützt.

Von den beiden im Gerät gespeicherten Firmware-Versionen kann immer nur eine aktiv sein. Beim Laden einer neuen Firmware wird die nicht aktive Firmware überschrieben. Sie können durch Auswahl des FirmSafe-Modus selbst entscheiden, welche Firmware nach dem Upload aktiviert werden soll.

2.6.2 Konfiguration

Den Modus für den Firmware-Upload stellen Sie im Setup-Menü unter **Firmware** > **Modus-Firmsafe** ein. Dabei stehen Ihnen drei verschiedene Modi zur Auswahl. In LANconfig haben Sie im Rahmen des Firmware-Uploads die Möglichkeit, entweder eine dem Modus 'unmittelbar' oder 'manuell' äquivalente Einstellung zu treffen (vgl. *Firmware-Upload über LANconfig* auf Seite 106).

- **unmittelbar**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nach dem Ende des Uploads sofort und endgültig. Folgende Szenarien sind daraufhin denkbar:
  - Der Start mit der neuen Firmware verläuft erfolgreich und das Gerät arbeitet anschließend wie gewünscht.
  - Das Gerät ist nach dem Ladevorgang der neuen Firmware nicht mehr ansprechbar. Sofern das Gerät nicht automatisch auf eine vorherige Firmware zurückfällt oder mit einer Minimal-Firmware startet, können Sie den Upload z. B. via LL2M wiederholen. Tritt schon während des Uploads ein Fehler auf, aktiviert das Gerät automatisch die bisherige Firmware und startet damit neu.
- **login**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nur temporär, um Probleme mit einem fehlerhaften Uploads vorzubeugen.

Nach der Aktivierung wartet das Gerät für die im Setup-Menü unter **Firmware** > **Timeout-Firmsafe** eingestellte Zeit (in Sekunden) auf einen erfolgreichen Login über ein Terminalprogramm oder WEBconfig. Nur wenn dieser Login erfolgt, wird die neue Firmware auch dauerhaft aktiviert.

Ist das Gerät nach dem Aktivieren der Firmware nicht mehr ansprechbar ist oder ein Login aus anderen Gründen unmöglich ist, aktiviert es nach Ablauf des Timeouts automatisch wieder die vorherige Firmware und startet neu.

- **manuell**: In diesem Modus aktiviert das Gerät eine hochgeladene Firmware nur temporär, um Probleme mit einem fehlerhaften Uploads vorzubeugen. Nach der Aktivierung wartet das Gerät für die im Setup-Menü unter **Firmware** > **Timeout-Firmsafe** eingestellte Zeit (in Sekunden) darauf, dass Sie die geladene Firmware von Hand endgültig aktivieren und damit dauerhaft wirksam machen.

  Unter LANconfig aktivieren Sie die neue Firmware über den Menüpunkt **Gerät** > **Firmware-Verwaltung** > **Im Test laufende Firmware freischalten**. Im Setup-Menü aktivieren Sie die Firmware unter **Firmware** > **Tabelle-Firmsafe**. Auf der Kommandozeile verwenden Sie dafür den Befehl `set # active`; '**#**' steht dabei für die Position der Firmware in der FirmSafe-Tabelle.

  Auch hier wechselt das Gerät nach Ablauf des Timeouts automatisch wieder auf die vorherige Firmware und startet neu.

Hinweis: Das Laden einer zweiten Firmware ist nur dann möglich, wenn das Gerät über ausreichenden Speicherplatz für zwei vollständige Firmwareversionen verfügt. Aktuelle Firmwareversionen (ggf. mit zusätzlichen Software-Optionen) können bei älteren Hardwaremodellen manchmal mehr als die Hälfte des verfügbaren Speicherplatzes beanspruchen. In diesem Fall wird das *asymmetrische FirmSafe* verwendet.

2.6.3 Asymmetrisches FirmSafe

Durch den großen und sich stetig erweiternden Funktionsumfang der Firmware ist es nicht bei allen Geräten möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Für solche Geräte existiert seit HiLCOS 7.60 stattdessen das asymmetrische FirmSafe.

Beim asymmetrischen FirmSafe enthält das Gerät immer eine "vollständige Firmware" sowie eine sogenannte "Minimal-Firmware". Die Minimal-Firmware wird normalerweise nicht gestartet – sie erlaubt jedoch nach einem fehlgeschlagenen Upload einer vollständigen Firmware (z. B. durch Stromausfall während des Uploads) den lokalen Zugriff auf das Gerät (über LAN, WLAN oder die Config-Schnittstelle), um eine funktionsfähige Firmware in das Gerät zu laden.

Die Minimal-Firmware ist **nicht** konfigurierbar! Änderungen in der Konfiguration über LANconfig, WEBconfig oder Telnet werden nicht in das Gerät gespeichert. Auch alle erweiterten Funktionalitäten – insbesondere die Remote-Administration über WAN oder ISDN – sind **nicht** verfügbar, solange die Minimal-Firmware aktiv ist! Allerdings ist auch in einer Minimal-Firmware der LL2M-Server aktiv und bietet so eine Zugriffsmöglichkeit auf das Gerät, sofern es über Layer 2 (Ethernet) von einem LL2M-Client erreichbar ist.

Umstellung auf asymmetrisches FirmSafe

Zur Umstellung der Geräte auf das asymmetrische FirmSafe laden Sie zunächst eine Konverter-Firmware in das Gerät. Dieser Konverter wandelt die vom Gerät aktuell **nicht aktive** Firmware in eine Minimal-Firmware um und schafft so Platz für eine neue, umfangreichere Firmware. Dieser Vorgang muss nur einmal vorgenommen werden.

Anschließend können Sie eine neue vollständige Firmware in das Gerät laden, die bei einem erfolgreichen Upload aktiviert wird. Die Minimal-Firmware verbleibt zur Sicherung der Erreichbarkeit im Gerät.

Firmware-Upgrade mit asymmetrischem FirmSafe

Bei jedem folgenden Firmware-Upload wird automatisch immer die **aktive** Firmware durch eine neue Firmware ersetzt.

2.7 Firmware über einen Client ins Gerät laden

Der Upload einer Firmware – also das Einspielen der Geräte-Software – kann auf verschiedenen Wegen erfolgen: beispielsweise über LANconfig, WEBconfig

oder ein Terminalprogramm. Dabei stehen Ihnen unterschiedliche Protokolle zur Auswahl.

Bei einem Upload bzw. Update der Firmware bleiben im Normalfall alle Einstellungen Ihres Gerätes erhalten (Ausnahme: *Upload mit Reset*). Trotzdem sollten Sie sicherheitshalber ein vollständiges Backup Ihrer Konfiguration anlegen. Außerdem sollten Sie ein Backup der bisherigen Firmware bereithalten für den Fall, dass der Update-Vorgang fehlschlägt und das Gerät z. B. auf eine Minimal-Firmware zurückfällt, welche keinen Internet-Zugang zulässt. Wenn Ihnen die entsprechende Firmware-Datei nicht mehr zur Verfügung steht, suchen Sie auf *www.hirschmann.de*.

Enthält die neu eingespielte Firmware Parameter, die in der aktuellen Firmware des Gerätes nicht vorhanden sind, werden die fehlenden Werte mit den Default-Einstellungen ergänzt.

2.7.1 Firmware-Upload über LANconfig

Dieser Abschnitt beschreibt, wie Sie über LANconfig eine andere Firmware in das Gerät laden.

1. Markieren Sie das gewünschte Gerät in der Auswahlliste und wählen Sie **Gerät** > **Firmware-Verwaltung** > **Neue Firmware hochladen**.
2. Wählen Sie im sich öffnenden Dialogfenster das Verzeichnis aus, in dem sich die neue Version befindet, und markieren die entsprechende *.upx-Datei.

   LANconfig informiert Sie dann in der Beschreibung über Art, Version und Release-Datum der Firmware.

3. Optional: Wählen Sie aus, ob das Gerät die Firmware nach dem Laden dauerhaft aktivieren oder zunächst in einem Test-Modus betreiben soll. Sofern Sie sich für den Test-Modus entscheiden, geben Sie eine Zeitraum an, nach der das Gerät wieder zur vorherigen Firmware wechselt, wenn Sie die Firmware über die ***Konfigurations-Verwaltung*** nicht aus diesem Modus heraus freischalten.

   Hinweis: Diese Auswahlmöglichkeit besteht nicht für Geräte, die mit *asymmetrischen FirmSafe* arbeiten.

4. Klicken Sie auf **Öffnen**, um die vorhandene Firmware durch die ausgewählte Version zu ersetzen.

LANconfig beginnt nun mit dem Firmware-Upload. Die können den Fortschritt über die Verlaufsspalte sowie Log-Informationsbereich verfolgen. Nach erfolgreichem Upload startet LANconfig das Gerät automatisch neu.

2.7.2 Firmware-Upload über WEBconfig

Innerhalb von WEBconfig laden Sie eine neue Firmware z. B. über das *Dateimanagement* hoch. Wählen Sie dafür eine geeignete Firmware-Datei aus und klicken Sie auf **Upload**. Überdies haben Sie genau wie unter LANconfig die Möglichkeit, die Firmware im Test-Modus hochzuladen (siehe *Firmware-Upload über LANconfig* auf Seite 106).

2.7.3 Firmware-Upload über Terminalprogramm

Dieser Abschnitt beschreibt, wie Sie mit Hilfe eines Terminalprogramms eine andere Firmware in das Gerät laden. Dabei stehen Ihnen prinzipiell zwei Möglichkeiten zur Auswahl:

- Upload über die serielle Konfigurationsschnittstelle
- Upload über TFTP oder SCP

Für den Upload über die serielle Verbindung benötigen Sie ein Programm, welches das XModem-Protokoll unterstützt, z. B. Windows HyperTerminal, Telix oder die freie Software Tera Term. Der Upload über TFTP oder SCP hingegen erfolgt über ein lokales oder externes Netzwerk.

Der nachfolgende Abschnitt beschreibt den Upload einer Firmware über die serielle Konfigurationsschnittstelle am Beispiel von HyperTerminal. Der Upload einer Firmware über TFTP oder SCP unterscheidet sich kaum vom allgemeinen Datei-Upload. Mehr Informationen hierzu finden Sie unter *Dateien über TFTP, HTTP(S) oder SCP direkt in das/aus dem Gerät laden* auf Seite 110.

1. Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.
2. Starten Sie auf diesem Rechner ein serielles Terminal-Programm, hier: Windows HyperTerminal.
3. Bauen Sie eine Verbindung mit folgenden Einstellungen auf und melden Sie sich mit Ihnen Login-Daten am Gerät an:

- Geschwindigkeit in bps: `115200`
- Datenbits: `8`
- Stopbits: `1`
- Parität: `keine`
- Flusssteuerung: `RTS/CTS` bzw. `RFR/CTS`

4. Wechseln Sie in das **Firmware**-Menü und legen Sie über den Befehl `set Modus-FirmSafe <Value>` den gewünschten FirmSafe-Modus fest, wobei `<Value>` für einen der möglichen Modi steht. Stellen Sie ggf. zusätzlich mit `set Timeout-FirmSafe <Time>` eine Zeit in Sekunden für den Firmware-Test ein.
   Eine Erläuterung zu den möglichen Modi sowie daran anknüpfende Konfigurationsschritte finden Sie im FirmSafe-Abschnitt *Konfiguration* auf Seite 103.
5. Versetzen Sie das Gerät mit dem Aktions-Befehl `do Firmware-Upload` in Empfangsbereitschaft.
6. Starten Sie den Upload-Vorgang von Ihrem Terminalprogramm aus.
   - Bei Telix klicken Sie auf die Schaltfläche **Upload**, stellen **XModem** für die Übertragung ein und wählen die gewünschte Firmware-Datei zum Upload aus.
   - Bei HyperTerminal klicken Sie auf **Übertragung** > **Datei senden**, wählen die Firmware-Datei aus, stellen **XModem** als Protokoll ein und starten mit **OK**.
   - Bei Tera Term klicken Sie auf **File** > **Transfer** > **XMODEM** > **Send** und wählen die gewünschte Firmware-Datei zum Upload aus.

Der Firmware-Upload wird nun durchgeführt. Nach dem erfolgreichen Firmware-Upload startet das Gerät schließlich neu.

2.7.4 Firmware-Upload über Outband mit Rücksetzen der Konfiguration

Wenn beide Speicherplätze der Boot-Konfigurationen belegt (also kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration gespeichert) sind, lässt sich das Gerät nicht mehr über den Reset-Taster auf die Werkseinstellungen zurücksetzen. Gleiches gilt, wenn die Funktion des Reset-Taster auf **Ignorieren** oder **Nur-Booten** beschränkt ist und das Konfigurationskennwort

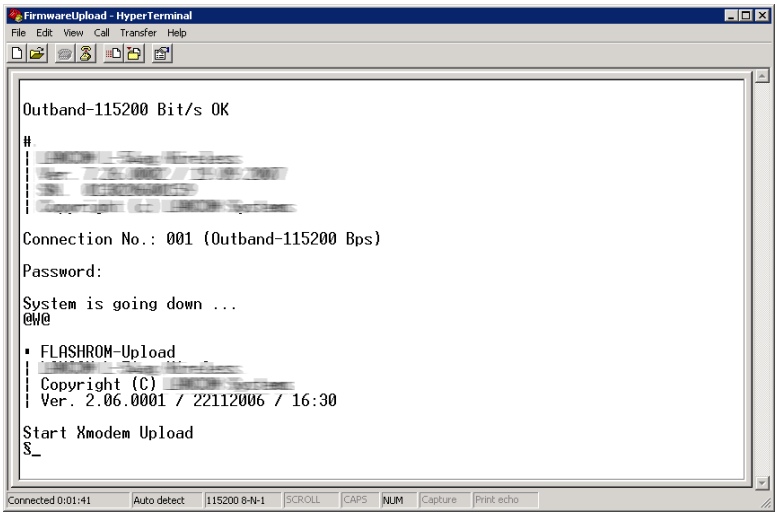
nicht mehr vorliegt. In diesem Fall können Sie einen Reset auf die Werkseinstellungen nur noch über den seriellen Zugang (Outband) durchführen.

Über die serielle Schnittstelle besteht die Möglichkeit, eine Firmware ins Gerät zu laden. Wenn Sie dabei statt des Konfigurations-Passwortes die Seriennummer des Gerätes verwenden, wird die Konfiguration wie bei einem Reset vollständig auf den Auslieferungszustand zurückgesetzt. Auf diese Weise können Sie sich stets Zugang zu einem Gerät verschaffen, wenn sich die Werkseinstellungen nicht auf einem anderen Weg wiederherstellen lassen.

Hinweis: Bei diesem Vorgang werden neben der Konfiguration auch die gespeicherten *Boot-Konfigurationen* vollständig gelöscht! Gleiches gilt für im Gerät abgelegten Dateien, z. B. vorhandene Rollout-Zertifikate. Nutzen Sie diese Möglichkeit daher nur, wenn Sie keinen anderen Zugang zum Gerät herstellen können. Die Konfiguration und die Boot-Konfigurationen werden auch dann gelöscht, wenn der Firmware-Upload abgebrochen wird.

Das nachfolgende Anwendungsbeispiel beschreibt den Firmware-Upload über die serielle Schnittstelle mit Rücksetzen der Konfiguration exemplarisch mittels HyperTerminal.

1. Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.
2. Starten Sie auf diesem Rechner ein serielles Terminal-Programm, hier: Windows HyperTerminal.
3. Bauen Sie eine Verbindung mit folgenden Einstellungen auf:
   - Geschwindigkeit in bps: `115200`
   - Datenbits: `8`
   - Stopbits: `1`
   - Parität: `keine`
   - Flusssteuerung: `RTS/CTS` bzw. `RFR/CTS`
4. Drücken Sie im Begrüßungsbildschirm des Terminal-Programms die Eingabe-Taste, bis die Aufforderung zur Eingabe des Passwortes erscheint.
5. Geben Sie als Passwort die Seriennummer ein, die unter der Firmware-Version angezeigt wird und drücken Sie erneut die Eingabe-Taste. Das System fährt daraufhin herunter und erwartet den Firmware-Upload.



6. Bei HyperTerminal klicken Sie auf **Übertragung** > **Datei senden**, wählen die Firmware-Datei aus, stellen **XModem** als Protokoll ein und starten mit **OK**.

Der Firmware-Upload wird nun durchgeführt. Nach dem erfolgreichen Firmware-Upload startet das Gerät schließlich neu.

2.8 Dateien über TFTP, HTTP(S) oder SCP direkt in das/aus dem Gerät laden

Verschiedene Anwendungen – wie z. B. das Laden von Konfigurationen, Firmware-Versionen sowie Skripten oder die Prüfung einer Server-Identität mit Zertifikaten – erfordern das Speichern der betreffenden Dateien im Gerät. Sie können diese Dateien mit LANconfig oder WEBconfig in das Gerät einspielen.

Alternativ haben Sie aber auch die Möglichkeit, über die Kommandozeile mittels TFTP, HTTP(S) oder SCP die entsprechenden Dateien direkt in das Gerät zu laden. Dieses Vorgehen erleichtert vor allem in größeren Installationen mit regelmäßigen Update-Intervallen von Firmware und/oder Konfiguration die Administration der Geräte. Dabei können Sie wählen, ob Sie eine Datei

von einer Maschine aus durch einen Client zum Gerät übertragen, oder das Gerät selbst auf der Kommandozeile die Datei von einem Server laden lassen.

2.8.1 Datei laden über einen TFTP-Client

TFTP (Trivial File Transfer Protocol) ist ein sehr einfaches Dateiübertragungsprotokoll zum Lesen oder Schreiben von Dateien. Es ermöglicht den einfachen Dateitransfer auf andere Geräte über das Netzwerk. Weitere Funktionen wie die des wesentlich mächtigerem FTPs (z. B. Rechtevergabe mittels chmod, Anzeige vorhandener Dateien, Benutzerauthentifizierung) sind allerdings nicht implementiert.

In LANconfig haben Sie die Möglichkeit, die Geräte-Kommunikation über TFTP abzuwickeln. Die Bedienung unterscheidet sich dabei aber nicht von der mit anderen Kommunikationsprotokollen. Daher richtet sich das hiesige Kapitel an alternative TFTP-Programme, welche Sie für die Geräte-Kommunikation nutzen können.

Unter vielen Windows-und Linux-Betriebssystemen z. B. ist standardmäßig ein kommandozeilenbasierter TFTP-Client enthalten. In Windows-Versionen 7 und neuer muss der TFTP-Client allerdings erst aktiviert werden. Alternativ können Sie auch einen anderen Client verwenden, wie z. B. die freie TFTP-Client-Server-Anwendung Tftpd32. Als Port geben Sie dann den Standardport `69` an. Die Blockgröße für Datenpakete entnehmen Sie dem Parameter **Bytes-pro-Hashmark** im Setup-Menü des Gerätes (normalerweise `8192`).

Syntax

Die Syntax des TFTP-Aufrufs ist abhängig vom verwendeten Betriebssystem bzw. Programm. Für den Windows-eigenen TFTP-Client lautet die Syntax beispielsweise:

```
tftp [-i] <Host> get|put <LocalFile|Command> <RemoteFile|Command>
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z. B. einer Firmware-Datei) muss daher meist die binäre Übertragung explizit gewählt werden. Unter Windows erreichen Sie dies durch den Parameter `-i`.

Sofern das Gerät mit einem Passwort geschützt ist, müssen Sie zudem Benutzername und Passwort in den TFTP-Befehl miteinbauen. Im TFTP wird

der Username und das Passwort im Quell- (TFTP-Read-Request) oder Ziel-Filename (TFTP-Write-Request) kodiert. Der Filename setzt sich dann entweder aus dem Root-Passwort und dem auszuführenden Kommando (für Supervisoren), oder aus der Kombination von Benutzername, Passwort und dem nachgestelltem Kommando (für lokale Administratoren) zusammen. Ein über TFTP abgesetzter Befehl sieht daher wie folgt aus:

- `<Root-Password> <Command>`
- `<Username>:<Password>@<Command>`

Als Kommandos ('<Command>') sind folgende Eingaben möglich:

- `readmib`: Kommando für das Einspielen einer Geräte-MIB-Datei (SNMP Management Information Base).
- `readconfig`: Kommando für das Auslesen einer Konfigurationsdatei.
- `writeconfig`: Kommando für das Einspielen einer Konfigurationsdatei.
- `writeflash`: Kommando für das Einspielen einer Firmware-Datei.

Hinweis: Die Rechte zur Nutzung von TFTP lassen sich für verschiedene Administrator-Typen einschränken, siehe *Rechteverwaltung für verschiedene Administratoren* auf Seite 135.

Anwendungsbeispiele

- Um z. B. eine Firmware in das Gerät zu laden, verwenden Sie das Kommando `writeflash`, wobei `10.0.0.1` für die IP-Adresse des Gerätes und `LC-L451-8.82.0083.upx` für die hochzuladende Datei stehen:

```
tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx writeflash
```

```
tftp -i 10.0.0.1 put LC-L451-8.82.0083.upx MyAdmin:MyPasswd@writeflash
```

- Um z. B. die Geräte-MIB auszulesen, verwenden Sie das Kommando `readmib`:

```
tftp 10.0.0.1 get readmib device.mib
```

- Um z. B. die Konfiguration unter Verwendung von Zugangsdaten aus dem Gerät auslesen, verwenden Sie das Kommando `readconfig`:

```
tftp 10.0.0.1 get root:MyPasswd@readconfig device.lcf
```

- Um z. B. Konfiguration unter Verwendung von Zugangsdaten in das Gerät schreiben, verwenden Sie das Kommando `writeconfig`:

```
tftp 10.0.0.1 put device.lcf root:MyPasswd@writeconfig
```

Hinweis: Die im Rahmen von *FirmSafe getätigten Einstellungen* gelten auch Firmware-Uploads via TFTP.

Fehlersuche

Sollten Sie keine Verbindung zum Gerät herstellen können, kann es sein, dass die Firewall Ihres Betriebssystems TFTP-Verbindungen blockiert. Sofern Sie die Firewall-Einstellungen des Gerätes verändert haben, prüfen Sie auch hier, ob diese Verbindungen über TFTP nachwievor erlaubt. Stellen Sie außerdem sicher, dass Sie im Gerät den Zugriff über das TFTP-Protokoll aus dem für den Upload verwendeten Netzwerk-Typ freigegeben haben (in LANconfig einstellbar unter **Management** > **Admin** > **Zugriffs-Rechte**).

2.8.2 Datei laden über einen SCP-Client

SCP (Secure Copy Protocol) ist ein Protokoll zur sicheren Übertragung von Daten zwischen zwei Rechnern in einem Netzwerk. Administratoren nutzen SCP häufig beim Datenaustausch zwischen Servern bzw. zwischen Server und Arbeitplatzrechner. Mit einem geeigneten Tool (unter Windows z. B. mit dem PuTTY-Zusatzprogramm PSCP oder unter Linux z. B. mit Konqueror oder Midnight Commander) lassen sich auch Daten zwischen einer Maschine und dem Gerät über das SCP-Protokoll austauschen.

Syntax

Die Syntax des SCP-Aufrufs ist abhängig vom verwendeten Programm. Für PSCP lautet die Syntax an der Windows-Kommandozeile:

- **Senden von Dateien**

```
pscp.exe -scp [-pw <Password>] <LocalFile> <User>@<IP-Address>:target
```

- **Empfangen von Dateien**

```
pscp.exe -scp [-pw <Password>] <User>@<IP-Address>:target <LocalFile>
```

Das Ziel (`target`) auf dem entfernten Gerät leiten Sie durch einen Doppelpunkt hinter der IP-Adresse ein. Als Ziel geben entweder den Namen eines Mountingpoints im internen Dateisystem des Gerätes an, `config` oder `firmware`. Das Ziel `firmware` ist ausschließlich für das Einspielen von Firmware-Updates reserviert; `config` benutzen Sie für das Ein- und Ausspielen von Konfigurationsdateien und -skripten.

Mountingpoints für die SCP-Dateiübertragung

Die folgende Tabelle zeigt, welche Dateien konkret Sie über die Einhängepunkte des Dateisystems (Mountingpoints) über SCP aus dem Gerät auslesen und/oder in das Gerät schreiben können.

Mountingpoint	*Lesen*	*Schreiben*	*Beschreibung*
ssl_cert	Ja	Ja	SSL - Zertifikat (*.pem, *.crt. *.cer [BASE64])
ssl_privkey	Nein	Ja	SSL - Privater-Schlüssel (*.key [BASE64 unverschlüsselt])
ssl_rootcert	Ja	Ja	SSL - Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
ssl_pkcs12	Nein	Ja	SSL - Container als PKCS#12-Datei (*.pfx, *.p12)
ssh_rsakey	Nein	Ja	SSH - RSA-Schlüssel (*.key [BASE64 unverschlüsselt])
ssh_dsakey	Nein	Ja	SSH - DSA-Schlüssel (*.key [BASE64 unverschlüsselt])
ssh_authkeys	Nein	Ja	SSH - akzeptierte öffentliche Schlüssel
vpn_rootcert	Ja	Ja	VPN - Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
vpn_devcert	Ja	Ja	VPN - Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])
vpn_devprivkey	Nein	Ja	VPN - Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])

Mountingpoint	*Lesen*	*Schreiben*	*Beschreibung*
vpn_pkcs12	Nein	Ja	VPN - Container (VPN1) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_2	Nein	Ja	VPN - Container (VPN2) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_3	Nein	Ja	VPN - Container (VPN3) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_4	Nein	Ja	VPN - Container (VPN4) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_5	Nein	Ja	VPN - Container (VPN5) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_6	Nein	Ja	VPN - Container (VPN6) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_7	Nein	Ja	VPN - Container (VPN7) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_8	Nein	Ja	VPN - Container (VPN8) als PKCS#12-Datei (*.pfx, *.p12)
vpn_pkcs12_9	Nein	Ja	VPN - Container (VPN9) als PKCS#12-Datei (*.pfx, *.p12)
vpn_add_cas	Nein	Ja	VPN - zusätzliche CA-Zertifikate hinzufügen (*.pfx, *.p12, *.pem, *.crt. *.cer [BASE64])
eaptls_rootcert	Ja	Ja	EAP/TLS - Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
eaptls_devcert	Ja	Ja	EAP/TLS - Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])
eaptls_privkey	Nein	Ja	EAP/TLS - Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])
eaptls_pkcs12	Nein	Ja	EAP/TLS - Container als PKCS#12-Datei (*.pfx, *.p12)
radsec_rootcert	Ja	Ja	RADSEC - Root-CA-Zertifikat (*.pem, *.crt. *.cer [BASE64])
radsec_devcert	Ja	Ja	RADSEC - Geräte-Zertifikat (*.pem, *.crt. *.cer [BASE64])
radsec_privkey	Nein	Ja	RADSEC - Privater-Geräte-Schlüssel (*.key [BASE64 unverschlüsselt])
radsec_pkcs12	Nein	Ja	RADSEC - Container als PKCS#12-Datei (*.pfx, *.p12)
radiuss_accnt_total	Ja	Ja	RADIUS-Server - Summarisches Accounting (*.csv)
scep_cert_list	Ja	Ja	SCEP-CA - Zertifikats-Liste

Mountingpoint	*Lesen*	*Schreiben*	*Beschreibung*
scep_cert_serial	Ja	Ja	SCEP-CA - Seriennummer
scep_ca_backup	Ja	Nein	Backup für SCEP-CA - PKCS12 Container
scep_ra_backup	Ja	Nein	Backup für SCEP-CA - PKCS12 Container
scep_ca_pkcs12	Nein	Ja	SCEP-CA - PKCS12 Container
scep_ra_pkcs12	Nein	Ja	SCEP-CA - PKCS12 Container
pbspot_template_welcome	Ja	Ja	Public Spot - Willkommensseite (*.html, *.htm)
pbspot_template_login	Ja	Ja	Public Spot - Login-Seite (*.html, *.htm)
pbspot_template_error	Ja	Ja	Public Spot - Fehlerseite (*.html, *.htm)
pbspot_template_start	Ja	Ja	Public Spot - Startseite (*.html, *.htm)
pbspot_template_status	Ja	Ja	Public Spot - Statusseite (*.html, *.htm)
pbspot_template_logoff	Ja	Ja	Public Spot - Logoff-Seite (*.html, *.htm)
pbspot_template_help	Ja	Ja	Public Spot - Hilfeseite (*.html, *.htm)
pbspot_template_noproxy	Ja	Ja	Public Spot - Kein-Proxy-Seite (*.html, *.htm)
pbspot_template_voucher	Ja	Ja	Public Spot - Voucher-Seite (*.html, *.htm)
pbspot_template_agb	Ja	Ja	Public Spot - AGB-Seite (*.html, *.htm)
pbspot_formhdrimg	Ja	Ja	Public Spot - Kopfbild Seiten (*.gif, *.png, *.jpeg)
WLC_Script_1.lcs	Ja	Ja	CAPWAP - WLC_Script_1.lcs
WLC_Script_2.lcs	Ja	Ja	CAPWAP - WLC_Script_2.lcs
WLC_Script_3.lcs	Ja	Ja	CAPWAP - WLC_Script_3.lcs
default_pkcs12	Nein	Ja	
rollout_wizard	Nein	Ja	
rollout_template	Nein	Ja	
rollout_logo	Nein	Ja	
hip_cert_0	Nein	Ja	

Mountingpoint	*Lesen*	*Schreiben*	*Beschreibung*
issue	Ja	Ja	Text zum Anzeigen beim Login auf der Kommandozeile (z. B: ASCII Logos)

Tabelle 12: Übersicht der Mountingpoints für die SCP-Dateiübertragung

Anwendungsbeispiele

- Um z. B. einen Datei von Ihrem Rechner auf das Gerät zu übertragen, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd c:\path\myfile.ext root@10.0.0.1:target
```

  Um z. B. eine Datei vom Gerät auf Ihren Rechner zu übertragen, wechseln Sie die Reihenfolge von Quelle und Ziel:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:target c:\path\myfile.ext
```

  Als `target` setzen Sie dabei die Bezeichnung eines Mountingpoints ein.

- Um z. B. die Konfiguration aus dem Gerät auf Ihren Rechner unter dem Namen `config.lcs` zu speichern, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd root@10.0.0.1:config c:\config.lcs
```

- Um z. B. eine neue Firmware von Ihren Rechner in das Gerät zu laden, nutzen Sie einen Befehl wie den folgenden:

```
C:\>pscp.exe -scp -pw MyPwd  c:\firmware.upx root@10.0.0.1:firmware
```

2.8.3 Datei-Download von einem TFTP- oder HTTP(S)-Server

Neben den Möglichkeiten, eine Firmware, eine Konfigurationsdatei oder ein Konfigurationsskript von einer Maschine aus an das Gerät zu übertragen, kann der Datei-Upload bzw. -Download auch durch das Gerät selbst von einem HTTP(S)- oder TFTP-Server im lokalen Netzwerk oder dem Internet erfolgen. Dazu werden die betreffenden Dateien auf einem HTTP(S)- bzw.

TFTP-Server abgelegt und nach Anmeldung am Gerät mit den weiter unten gelisteten HiLCOS-Befehlen aufgerufen.

Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Bei der Verwendung eines HTTPS-Servers können Sie im Gerät ein Zertifikat hinterlegen, mit dem sich später die Identität des Servers verifizieren lässt. In der Praxis ist es zumeist sehr viel leichter, einen HTTP(S)-Server zentral mit eindeutiger Adresse (URI) im Internet bereit zu stellen als einen TFTP-Server – ggf. lässt sich z. B. ein bestehender Webserver um diese Funktionalität erweitern.

Von einem solchen Server lassen sich die unterschiedlichen Dateitypen dann mit folgenden Befehlen abrufen:

- `LoadConfig`: Lädt eine Konfigurationsdatei (mit der Dateierweiterung *.lcf) in das Gerät.
- `LoadFirmware`: Lädt eine Firmware-Datei (mit der Dateierweiterung *.upx) in das Gerät.
- `LoadScript`: Lädt eine Skript-Datei (mit der Dateierweiterung *.lcs) – z. B. mit Teilkonfigurationen – in das Gerät.
- `LoadFile`: Lädt Dateien verschiedenen Typs in das Gerät.

  Hinweis: Der Befehl `LoadFile` unterstützt ausschließlich die Protokolle HTTP und HTTPS.

Syntax

Die genaue Syntax der Load-Befehle ist abhängig vom verwendeten Protokoll (HTTP[S] oder TFTP). Allgemein betrachtet setzt sich ein Aufruf aber immer aus dem entsprechenden Befehl, eventuellen Parametern und der URL zusammen, welche die zu ladende Datei referenziert. Diese URL können Sie auch im Setup-Menü unter **Automatisches-Laden** > **Netzwerk** > **…** > **URL** hinterlegen, sodass sich eine Firmware, Konfiguration oder Skriptdatei auch allein durch Eingabe des Kommandos allein ins Gerät laden lässt.

Verbindungen zu einem HTTP(S)-Server

Bei Nutzung von HTTP(S) kann der Befehl in der üblichen URL-Schreibweise angegeben werden. Als Protokoll tragen Sie entweder `http` oder `https` ein:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

Sofern Sie dabei auf einen kennwortgeschützten Bereich zugreifen wollen, authentisieren Sie sich mit der üblichen Benutzername/Kennwort-Schreibweise:

```
<Command> <Parameter>
<Protocol>://<Username>:<Password>@<Host>/<Directory>/<File>
```

Verbindungen zu einem TFTP-Server

Bei Nutzung von TFTP steht Ihnen ebenfalls die URL-Schreibweise zur Verfügung. Als Protokoll tragen Sie in diesem Fall `tftp` ein:

```
<Command> <Parameter> <Protocol>://<Host>/<Directory>/<File>
```

Alternativ können Sie stattdessen auch die URL durch die entsprechenden Parameter ersetzen:

```
<Command> <Parameter> -s <Host> -f <Directory>/<File>
```

Parameter

Die Befehle zur Verbindung mit einem HTTP(S)- oder TFTP-Server können durch Angabe zusätzlicher Parameter modifiziert werden. Dabei sind nicht alle Parameter für alle Protokolle verfügbar. Sofern über das Setup-Menü bestimmte Default-Werte konfigurierbar sind, verwendet das Gerät diese Werte, solange Sie die Werte nicht durch die dazugehörigen Parameter explizit überschreiben. Dies gilt z. B. für die Parameter der Versionsprüfung.

Parameter für die Verbindung

Über folgende Parameter können Sie die Art und Weise verändern, wie sich das Gerät mit dem Server verbindet.

-a <Address>

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: alle

Über diesen Parameter benennen Sie eine optionale Loopback-Adresse. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- `INT` für die Adresse des ersten Intranets
- `DMZ` für die Adresse der ersten DMZ
- `LB0` bis `LBF` für die 16 Loopback-Adressen
- Beliebige, gültige IP-Adresse

Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen.

-f <Directory>/<File>

Verfügbar für Protokoll: TFTP

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den Pfad und den Namen der Datei auf dem Server an. Der Parameter ersetzt zusammen mit `-s` die Angabe einer URL.

-s <Host>

Verfügbar für Protokoll: TFTP

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den DNS-Namen oder die IP-Adresse des Servers an. Der Parameter ersetzt zusammen mit `-f` die Angabe einer URL.

Parameter für die Versionsprüfung

In der Default-Einstellung sind die Bedingungen für Firmware, Konfiguration und Skript im Setup-Menü (unter **Automatisches-Laden** > **Netzwerk** > **…**) auf **unbedingt** eingestellt. Dadurch laden oder starten die Befehle LoadFirmware, LoadConfig oder LoadScript die entsprechende Firmware, Konfiguration oder Skriptdatei **ohne** dass eine Versionsprüfung stattfindet.

Durch Angabe des entsprechenden Parameters können Sie diese Einstellung jedoch für eine zu ladende Datei individuell übergehen.

-Cd

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware, LoadConfig, LoadScript

Dieser Parameter überprüft, ob die verwendete Datei **unterschiedlich** ist im Vergleich zur im Gerät vorhandenen Firmware oder Konfiguration bzw. neuer als das zuletzt ausgeführte Skript. Bei der Verwendung mit LoadScript aktualisiert dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes.

-Cn

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware

Dieser Parameter überprüft, ob die verwendete Datei **neuer** ist im Vergleich zur im Gerät vorhandene Firmware.

-m

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware

Dieser Parameter gibt die Minimalversion für eine Firmware an. Die für den Befehl verwendete Firmware muss mindestens dieser Version entsprechen, damit der Befehl ausgeführt wird.

-u

Verfügbar für Protokoll: HTTP, HTTPS, TFTP

Verfügbar für Befehl: LoadFirmware, LoadConfig, LoadScript

Dieser Parameter deaktiviert die Versionsprüfung. Die mit dem Befehl verwendete Datei wird auf jeden Fall geladen oder ausgeführt. Bei der Verwendung mit LoadScript belässt dieser Parameter die im Gerät gespeicherte Prüfsumme des zuletzt ausgeführten Skriptes unverändert.

Hinweis: Der Parameter -u hat immer Vorrang vor anderen mit dem Befehl übergebenen Parametern.

Parameter für die Zertifikatsprüfung

Bei der Übertragung von Dateien von einem HTTPS-Server zu einem Client-Gerät prüfen die beteiligten Netzwerkkomponenten die Identität der Gegenstelle mit Hilfe von Zertifikaten. Beim automatischen Laden von HTTPS-Servern stehen Ihnen zusätzliche Parameter für den Download der Zertifikate und deren anschließende Prüfung zur Verfügung. Das betreffende Zertifikat laden Sie z. B. über das Datenmanagement von LANconfig oder WEBconfig als **SSL - Root-CA-Zertifikat (*.pem, *.crt *.cer [BASE64])** in das Gerät.

-c <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: alle

Über diesen Parameter geben Sie den Namen des Zertifikats an, mit dem das Gerät die Identität des Servers prüft, bevor es die angeforderte Datei lädt.

-d <Passphrase>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Mit dieser Passphrase verschlüsselt das Gerät einen unverschlüsselten PKCS#12-Container.

-p <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter geben Sie beim Download einer Datei den Namen des PKCS#12-Containers an. Der PKCS#12-Container kann mehrere CA-Zertifikate enthalten und unterstützt so die Identitätsprüfung von HTTPS-Servern mit Zertifikatsketten. Außerdem kann ein PKCS#12-Container ein Gerätezertifikat und den zugehörigen privaten Schlüssel enthalten und so die Identität des Geräts gegenüber dem HTTPS-Server bestätigen, wenn der HTTPS-Server die Authentifizierung mit einem Zertifikat erfordert.

-n

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter deaktivieren Sie die Prüfung des Server-Namens beim Laden einer Datei. Wenn Sie den Server in der betreffenden URL als DNS-Name angeben (und nicht als IP-Adresse), dann überprüft das Gerät das Zertifikat auf den zugehörigen Server-Namen. Wenn es sich bei dem HTTPS-Server um einen virtuellen Server handelt, kann dieser Server mit den passenden Zertifikaten für den übermittelten DNS-Namen antworten. Ohne Angabe dieses Parameters prüft das Gerät, ob der DNS-Name in der betreffenden URL mit dem 'common name' der übermittelten Zertifikate übereinstimmt. Das Gerät lädt die Datei nur dann, wenn diese Prüfung erfolgreich verläuft.

-o <MainDir>/<File>

Verfügbar für Protokoll: HTTPS

Verfügbar für Befehl: LoadFile

Über diesen Parameter geben Sie das Ziel für den Download einer Datei an. Verwenden Sie diese Option, um z. B. ein Zertifikat für die spätere Identitätsprüfung bei Zugriff auf einen HTTPS-Server in Ihrem Gerät zu speichern.

Verwenden Sie dabei als `<MainDir>` eines der beiden folgenden Hauptverzeichnisse:

- Sofern das Ziel eine Datei im internen Dateisystem des Geräts darstellt, verwenden Sie das Hauptverzeichnis `/minifs/`. In Kombination mit einem Parameter lautet eine mögliche Eingabe z. B. `-c /minifs/sslroot.crt`. Die möglichen Einhängepunkte (Mountpoints) finden Sie im Status-Menü unter **Dateisystem** > **Inhalt**. Alternativ finden Sie eine allgemeine Übersicht auch im Abschnittt *Mountingpoints für die SCP-Dateiübertragung* auf Seite 114.
- Sofern das Ziel eine Datei auf einem externen USB-Datenträger darstellt, verwenden Sie das Hauptverzeichnis `/mountpoint/`. In Kombination mit einem Parameter lautet eine mögliche Eingabe z. B. `-o /mountpoint/Device-9.00.0244.upx`.

Wichtig: Sofern der angegebene Speicherpfad Unterverzeichnisse enthält, müssen diese bereits existieren. Das Gerät legt keine neuen Verzeichnisse an.

Darüber hinaus können Sie in nicht bereits vom Gerät vorgegebenen Dateinamen und -pfaden Variablen verwenden, um z. B. dynamische Verzeichnisstrukturen zu realisieren (siehe *Variablen* auf Seite 124.

Variablen

Sie haben die Möglichkeit, in den Load-Befehlen dynamische Pfadangaben zu verwenden, wann immer Sie innerhalb eines Parameters oder einer URL auf eine Datei referenzieren. Die Inhalte der einzelnen Variablen werden dabei vom Gerät vorgegeben und lassen sich nicht manuell verändern.

Folgende Variablen sind in Ihren Verzeichnis- und Dateinamen erlaubt:

%m
MAC-Adresse des Gerätes in hexadezimaler Schreibweise, mit Kleinbuchstaben und ohne Trennzeichen

%s
Seriennummer des Gerätes

%n
Gerätename

%l
Standort des Gerätes, wie in der Konfiguration angegeben

%d
Gerätetyp

Neben diesen allgemeinen Variablen können Sie auch die folgenden *Umgebungsvariablen* der Geräte nutzen, um die Ausführung der Load-Befehle flexibler zu gestalten.

Anwendungsbeispiele

Mit dem folgenden Befehl laden Sie – nachdem Sie sich auf der Kommandozeile am Gerät angemeldet haben – …

- eine Firmware-Datei mit dem Namen 'Device-8.80.0103.upx' aus dem Verzeichnis 'HiLCOS/880' vom TFTP-Server mit der IP-Adresse '192.168.2.200' in das Gerät:

```
LoadFirmware -s 192.168.2.200 -f HiLCOS/880/Device-8.80.0103.upx
```

- ein zur MAC-Adresse passendes Script (mit z. B. dem Namen '00a0571735da.lcs') vom TFTP-Server mit der IP-Adresse '192.168.2.200' in das Gerät:

```
LoadScript -s 192.168.2.200 -f %m.lcs
```

- eine Firmware-Datei mit dem Namen 'Device-8.80.0103.upx' aus dem Verzeichnis 'download' vom HTTPS-Server mit der Adresse 'www.myserver.com' in das Gerät. Dabei wird die Identität des Servers mit dem Zertifikat 'sslroot.crt' geprüft, das im internen Dateisystem des Gerätes gespeichert ist:

```
LoadFirmware -c /minifs/sslroot.crt
https://www.myserver.com/download/Device-8.80.0103.upx
```

- ein zur Seriennummer und zur aktuellen Firmware-Version passendes Script in das Gerät. Das Gerät entnimmt die Werte für Seriennummer und Firmware aus den entsprechenden Umgebungsvariablen:

```
LoadScript $__SERIALNO-$__FWVERSION.lcs
```

  Hinweis: Dieser Befehl funktioniert ohne Angabe einer URL, wenn diese unter **Setup** > **Autoload** > **Netzwerk** > **Skript** im Parameter **URL** angegeben ist. Fehlt dieser Eintrag, ist die Angabe einer URL im Befehl erforderlich:

```
LoadScript -s 192.168.2.200 $__SERIALNO-$__FWVERSION.lcs
```

Firmware und/oder Konfiguration regelmäßig updaten

Dieses Szenario beschreibt, wie Sie an der Kommandozeile das Gerät so konfigurieren, dass zu einer festgelegten Uhrzeit ein regelmäßiges Update der Firmware und/oder der Konfiguration erfolgt. Der Download von Firmware

und Konfiguration erfolgt dabei von einem externen Server (siehe *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 117) über die Befehle 'LoadFirmware' und 'LoadConfig' unter Verwendung fixer Dateinamen. Die Zeitplanung realisieren Sie mittels Cron-Jobs.

1. Geben Sie die URL an, von dem der Befehl 'LoadFirmware' die Firmware lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Firmware von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/firmware/LCOS.upx
```

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Konfiguration von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

```
set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL
http://www.mycompany.de/configuration/LCOS.lcf
```

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:

```
set /Setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung
wenn-unterschiedlich
```

5. Erstellen Sie einen Cron-Job, der regelmäßig um 23:55 Uhr das Kommando 'LoadFirmware' ausführt:

```
cd /Setup/Config/Cron-Tabelle
set 1 * * * 55 23 * * * LoadFirmware
```

6. Erstellen Sie einen Cron-Job, der regelmäßig um 23:59 Uhr das Kommando 'LoadConfig' ausführt:

```
set 2 * * * 59 23 * * * LoadConfig
```

Fertig! Damit haben Sie das automatische Update von Firmware und Konfiguration eingerichtet.

Hinweis: Die Reihenfolge (erst Firmware, anschließend Konfiguration) stellt sicher, dass die Konfiguration auch Menüpunkte beinhalten kann, die erst in der neuen Firmware vorhanden sind.

Konfiguration erst im Anschluss an die Firmware updaten

Dieses Szenario beschreibt, wie Sie an der Kommandozeile das Gerät so konfigurieren, dass es in einem festgelegten Intervall Firmware und Konfiguration aktualisiert. Das Update der Firmware erfolgt dabei **vor** dem Update der Konfiguration. Der Download von Firmware und Konfiguration geschieht von einem externen Server (siehe *Datei-Download von einem TFTP- oder HTTP(S)-Server* auf Seite 117) über die Befehle 'LoadFirmware' und 'LoadConfig' unter Verwendung dynamischer Dateinamen. Die Zeitplanung realisieren Sie mittels Cron-Jobs.

1. Geben Sie die URL an, von dem der Befehl 'LoadFirmware' die Firmware lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Firmware von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL
   http://www.mycompany.de/firmware/
   ```

   Der Dateiname wird später durch den Cron-Job definiert.

2. Stellen Sie die Bedingung für das Laden der Firmware so ein, dass nur eine neuere als die im Gerät vorhandene Firmware geladen wird:

   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/Bedingung wenn-neuer
   ```

3. Geben Sie den Pfad an, von dem der Befehl 'LoadConfig' eine Konfiguration lädt, wenn keine anderen Parameter vorliegen. Für das Laden der Konfiguration von einem HTTP-Server z. B. verwenden Sie einen Befehl ähnlich dem folgenden:

   ```
   set /Setup/Automatisches-Laden/Netzwerk/Firmware/URL
   http://www.mycompany.de/configuration
   ```

Der Dateiname wird später durch den Cron-Job definiert.

4. Stellen Sie die Bedingung für das Laden der Konfiguration so ein, dass nur eine andere als die im Gerät vorhandene Konfiguration geladen wird:

```
set /Setup/Automatisches-Laden/Netzwerk/Konfiguration/Bedingung
wenn-unterschiedlich
```

5. Erstellen Sie einen Cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadFirmware' ausführt:

```
cd /Setup/Config/Cron-Tabelle
set 1 * * * 10 * * * * LoadFirmware\ $__SERIALNO-Device.upx
```

Im obigen Beispiel muss die Firmware auf dem HTTP-Server also in der Form `<SerialNumber>-Device.upx` vorliegen, z. B. `000018100060-Device.upx`.

Hinweis: Im cron-Befehl `LoadFirmware\ $__SERIALNO-Device.upx` ist das Leerzeichen zwischen dem Load-Kommando und der Umgebungsvariablen mit einem Backslash geschützt. Eine denkbare alternative Schreibweise, bei welcher der komplette Befehl mit Anführungszeichen eingeschlossen wird, führt zu einem Fehler. LCOS behandelt Umgebungsvariablen in Anführungszeichen wie normaler Text; die Umsetzung in den Inhalt der Variablen entfällt.

6. Erstellen Sie einen Cron-Job, der regelmäßig alle 10 Minuten das Kommando 'LoadConfig' ausführt:

```
set 2 * * * 10 * * * * LoadScript\ $__SERIALNO-$__FWVERSION.lcs
```

Im obigen Beispiel muss das Konfigurationsskript auf dem HTTP-Server also in der Form `<SerialNumber>-<FirmwareVersion>.lcs` vorliegen, z. B. `000018100060-8.84.lcf`.

Fertig! Bei dieser Konfiguration lädt das Gerät in jedem Fall zuerst die aktuelle Firmware.

Wenn das Gerät – nach dem Hochladen der aktuellen Firmware und des aktuellen Konfigurationsskriptes (z. B. für Version 8.84) auf den HTTP-Server – zuerst den Befehl 'LoadScript' ausführt, enthält die Umgebungsvariable

'__FWVERSION' zu diesem Zeitpunkt den Wert der vorangegangenen Firmware (z. B. '8.80'). Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet zu diesem Zeitpunkt also kein passendes Konfigurationsskript. Anschließend führt das Gerät den Befehl `LoadFirmware 000018100060-Device.upx` aus; nach dem Neustart enthält die Umgebungsvariable '__FWVERSION' den Wert '8.84'. Der Befehl `LoadScript\ $__SERIALNO-$__FWVERSION.lcs` findet dann ein passendes Skript zum Updaten der Konfiguration.

2.9 Automatisches Laden von Firmware oder Konfiguration über USB

Geräte mit USB-Anschluss können Sie mit Hilfe eines externen Datenträgers sehr komfortabel in Betrieb nehmen. Loader und Firmware-Dateien lassen sich ebenso wie vollständige Konfigurationen oder Skripte automatisch von einem USB-Medium in das Gerät laden.

2.9.1 Automatisches Laden von Loader- und/oder Firmware-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Loader- und/oder Firmware-Dateien im Verzeichnis 'Firmware'. In diesem Verzeichnis werden alle Dateien mit der Dateiendung '*.upx' für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu liest das Gerät den Header der Dateien aus und verwendet die Dateien anschließend nach folgenden Regeln:

- Wurde mindestens eine upx-Datei mit Loader gefunden, wird der Loader mit der höchsten Versionsnummer geladen, sofern im Gerät nicht schon ein Loader mit höherer Versionsnummer vorhanden ist.
- Wurde mindestens eine Firmware-Datei gefunden, wird die Firmware mit der höchsten Versionsnummer geladen, wenn die Version ungleich der im Gerät aktiven oder inaktiven Firmwareversionen ist.

Während des automatischen Ladevorgangs blinken die Power- und die Online-LED am Gerät abwechselnd. Wird zunächst ein Loader geladen, erfolgt nach dem Ladevorgang ein Neustart des Geräts und anschließend evtl. ein zweiter

automatischer Ladevorgang für eine Firmware. Auch bei dem zweiten Ladevorgang blinken die Power- und die Online-LED am Gerät abwechselnd.

An den automatischen Ladevorgang von Loader- und/oder Firmware-Dateien können sich evtl. noch weitere Ladevorgänge für Konfigurations- und/oder Skript-Dateien anschließen, siehe *Automatisches Laden von Konfigurations- und/oder Skript-Dateien* auf Seite 130.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Sie können das USB-Medium dann entfernen.

2.9.2 Automatisches Laden von Konfigurations- und/oder Skript-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Loader- und/oder Firmware-Dateien im Verzeichnis 'Config'. In diesem Verzeichnis werden alle Dateien mit der Dateiendung '*.lcf' (Konfigurationen) sowie '*.lcs' (Skripte) für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu liest das Gerät den Header der Dateien aus und verwendet die Dateien anschließend nach folgenden Regeln:

- Eine Voll-Konfiguration wird immer vor einem Skript geladen. Es werden nur Voll-Konfigurationen geladen, deren Gerätetyp-Eintrag gleich dem Typ des ladenden Geräts ist und deren Firmware-Versions-Eintrag im Header gleich der im ladenden Gerät aktiven Firmware ist. Liegen mehrere passende Voll-Konfigurationen vor, erfolgt die Auswahl nach den folgenden Kriterien in dieser Reihenfolge:
  - Der Konfigurationsheader enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
  - Der Konfigurationsheader enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
  - Sollten danach mehrere Konfigurationsdateien ohne die zuvor genannten Kriterien verbleiben, verwendet das Gerät die Konfiguration mit dem aktuellsten Datum.
- Sollte keine Voll-Konfiguration vorliegen, wählt das Gerät eine eventuell vorhandene Skript-Datei. Liegen mehrere passende Skripte vor, erfolgt die Auswahl nach den folgenden Kriterien in dieser Reihenfolge:

- Der Skript-Header enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
- Der Skript-Header enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
- Der Skript-Header enthält eine Firmware-Version und diese stimmt mit der Firmware-Version des ladenden Gerätes überein.

Sollten danach mehrere Skripte ohne die zuvor genannten Kriterien verbleiben, verwendet das Skript mit der aktuellsten Versionsnummer bzw. dem Datum.

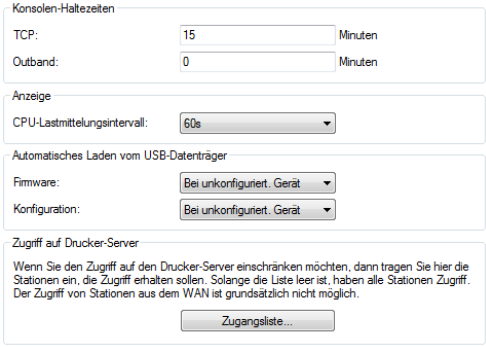
Hinweis: Die Meta-Daten zur verwendeten Firmwareversion und zum Erstellungsdatum werden automatisch beim Speichern einer Konfigurations- bzw. Skript-Datei generiert. Die Speicherung einer MAC-Adresse und/oder Geräte-Seriennummer ist optional. Mehr dazu erfahren Sie unter *Erweiterte Meta-Daten für Konfigurationsdateien* auf Seite 238.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Sie können das USB-Medium dann entfernen.

2.9.3 Konfiguration des automatischen Ladens via USB

Die nachfolgenden Schritte zeigen Ihnen, wie Sie das automatische Laden von einem USB-Datenträger konfigurieren.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Management** > **Erweitert**.



3. (De-)Aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien über die Auswahlliste **Firmware**. Dazu wählen Sie die entsprechende Rahmenbedingung aus.

   - **Aus**: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.
   - **Bei unkonfiguriert. Gerät**: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Nach erfolgreicher Erstkonfiguration durch den Assistenten für Sicherheitseinstellungen bzw. Grundeinstellungen setzt dieser die Einstellung auf **Aus**.
   - **Ein**: Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und/oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

4. (De-)Aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien über die Auswahlliste **Konfiguration**. Dazu wählen Sie die entsprechende Rahmenbedingung aus.

   - **Aus**: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.
   - **Bei unkonfiguriert. Gerät**: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Nach erfolgreicher Erstkonfiguration durch den Assistenten für Sicherheitseinstellungen bzw. Grundeinstellungen setzt dieser die Einstellung auf **Aus**.

- **Ein**: Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist aktiviert. Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und/oder Skript-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

Fertig! Damit haben Sie die Konfiguration des automatischen Ladens von einem USB-Datenträger abgeschlossen.

Hinweis: Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

2.10 Geräte-Reset durchführen

Wenn Sie unabhängig von den evtl. vorhandenen Einstellungen das Gerät neu konfigurieren müssen oder selbst nach einem Neustart keine Verbindung zur Gerätekonfiguration zustande kommt, besteht die Möglichkeit, mit einem Reset das Gerät in den Auslieferungszustand zurückzusetzen. Dazu betätigen Sie den Reset-Knopf **bis zum ersten Aufleuchten** sämtlicher LEDs des Gerätes (ca. 5 Sekunden).

Wichtig: Das Gerät startet nach dem Reset neu im unkonfigurierten Zustand, **alle** Einstellungen gehen dabei verloren. Sichern Sie daher **vor** dem Reset nach Möglichkeit die aktuelle Konfiguration des Gerätes!

Wichtig: Ein Access Point befindet sich nach dem Reset im Managed-Modus. In diesem Modus ist kein WLAN-Zugriff auf die Konfiguration möglich.

Wichtig: Bei einem Reset werden die im Gerät definierten WLAN-Verschlüsselungseinstellungen auf den Standard-WPA-Schlüssel zurückgesetzt. Der Standard-WPA-Schlüssel besteht aus der MAC-Adresse der physikalischen WLAN-Schnittstelle mit vorangestelltem "L". Die drahtlose Konfiguration mit

dem WLAN-Gerät gelingt nach einem Reset lediglich dann, wenn Sie den Standard-WPA-Schlüssel unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** eingetragen haben.

Hinweis: Bei Outdoor Access Points ist der Geräte-Reset von der Bauform abhängig. Die genaue Vorgehensweise für ein spezifisches Gerät finden Sie in der entsprechenden Hardware-Schnellübersicht.

2.10.1 Konfiguration des Reset-Knopfes

Der Reset-Knopf hat mit Booten (Neustart) und Reset (Rücksetzen auf Werkseinstellung) grundsätzlich zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Knopfes ausgelöst werden.

Manche Geräte können jedoch nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Knopf zu lange gedrückt hält. Mit einer entsprechenden Einstellung lässt sich das Verhalten des Reset-Knopfes gezielt steuern.

1. Wechsel Sie im Setup-Menü in den Zweig **Config**.
2. Legen Sie über den Parameter **Reset-Knopf** das Verhalten des Gerätes beim Betätigen des Reset-Knopfes fest. Mögliche Einstellungen sind:
   - **ignorieren**: Der Druck auf den Knopf löst keine Aktion aus.
   - **nur-booten**: Der Druck auf den Knopf löst einen Neustart aus, unabhängig von der gedrückten Dauer.
   - **reset-oder-booten**: In dieser Einstellung hat der Reset-Knopf verschiedene Funktionen, die Sie durch unterschiedlich lange Betätigungszeiten des Knopfes auslösen. Mehr zu den unterschiedlichen Betätigungszeiten finden Sie im Abschnitt *Besonderheiten der Rollout-Konfiguration* auf Seite 98.

   Gefahr: Mit der Einstellung **ignorieren** oder **nur-booten** wird das Rücksetzen der Konfiguration in den Auslieferungszustand sowie das Laden der Rollout-Konfiguration durch einen Reset unmöglich gemacht. Falls für ein Gerät in diesem Zustand das Konfigurationskennwort nicht mehr vorliegt, gibt es keine Möglichkeit mehr, auf das Gerät zuzugreifen! In diesem

Fall kann über die serielle Konfigurationsschnittstelle eine neue Firmware in das Gerät geladen werden; dabei wird das Gerät in den Auslieferungszustand zurückgesetzt und die bisherige Konfiguration gelöscht.

3. Klicken Sie **Setzen**, um die Konfiguration zurück in das Gerät zu schreiben.

2.11 Rechteverwaltung für verschiedene Administratoren

Sie haben die Möglichkeit, in der Konfiguration Ihres Gerätes mehrere Administratoren anzulegen, die über unterschiedliche Zugriffs- und Funktionsrechte verfügen.

Neben den in der Konfiguration angelegten Administratoren gibt es auch noch den Root-Administrator mit dem Haupt-Geräte-Passwort. Dieser Administrator hat immer die vollen Rechte und kann auch nicht gelöscht, eingeschränkt oder umbenannt werden. Um sich als Root-Administrator anzumelden, benutzen Sie beim Login via LANconfig, WEBconfig oder Terminalprogramm den Bentzternamen `root` oder lassen das betreffende Eingabefeld leer.

Sobald in der Geräte-Konfiguration ein Haupt-Geräte-Passwort gesetzt ist, erscheint beim HTTP(S)-Zugriff auf das Gerät mit einem Webbrowser die Anmeldemaske von WEBconfig. Sofern neben dem Root-Administrator noch andere Administratoren eingerichtet sind, umfasst die Maske die Eingabefelder **Login** und **Passwort**; andernfalls nur **Passwort**. Nach der Eingabe der korrekten Zugangsdaten gelangt ein Benutzer weiter zum Hauptmenü. In diesem Menü sind nur die Punkte vorhanden, für die ein Administrator auch die entsprechenden Zugriffs- bzw. Funktionsberechtigungen hat.

2.11.1 Die Rechte für die Administratoren

Die Rechte für Administratoren unterteilen sich in zwei Bereiche:

- *Zugrifftsrechte*: Jeder Administrator gehört zu einer bestimmten Gruppe, der global definierte Zugriffsrechte zugewiesen sind.
- *Funktionsrechte*: Jeder Administrator verfügt außerdem über sogenannte Funktionsrechte, die den persönlichen Zugriff auf bestimmte Funktionen – wie z. B. die Setup-Assistenten – regeln.

Zugriffsrechte

Die nachfolgende Tabelle zeigt Ihnen eine Übersicht aller Berechtigungslevel, die Sie an Administratoren vergeben können. Folgende Zugriffsrechte bzw. Gruppen von Administrator-Konten sind konfigurierbar:

Bezeichnung unter LANconfig	*Bezeichnung im Setup-Menü*	*Rechtebeschreibung*
Alle	Supervisor	Supervisor. Ist Mitglied in allen Gruppen und hat vollen Zugriff auf die Konfiguration.
Eingeschr. und Tracen	Admin-RW	Lokaler Administrator mit Lese- und Schreibzugriff. Hat vollen Zugriff auf die Konfiguration, jedoch sind folgende Möglichkeiten gesperrt: ▶ Firmware in das Gerät hochladen ▶ Konfiguration in das Gerät einspielen ▶ Konfiguration über LANconfig
Eingeschränkt	Admin-RW-Limit	Lokaler Administrator mit Lese- und Schreibzugriff, aber ohne Trace-Rechte. Hat vollen Zugriff auf die Konfiguration, jedoch sind folgende Möglichkeiten gesperrt: ▶ Firmware in das Gerät hochladen ▶ Konfiguration in das Gerät einspielen ▶ Konfiguration über LANconfig ▶ Trace-Ausgaben über die Kommandozeile oder LANmonitor
Lesen und tracen	Admin-RO	Lokaler Administrator mit Lesezugriff, aber ohne Schreibzugriff. Kann die Konfiguration über die Kommandozeile auslesen, aber keine Werte verändern.
Nur lesen	Admin-RO-Limit	Lokaler Administrator mit Lesezugriff, aber ohne Schreibzugriff und ohne Trace-Rechte. Kann die Konfiguration über die Kommandozeile auslesen, aber keine Werte verändern und Trace-Ausgaben anfordern.
Keine	Kein	Hat keinen Zugriff auf die Konfiguration.

Tabelle 13: Übersicht der Zugriffsrechte

Wichtig: Lokale Administratoren können auch die Admintabelle bearbeiten. Dabei kann ein lokaler Administrator jedoch nur solche Einträge bearbeiten oder anlegen, die die gleichen oder weniger Rechte haben wie er selbst. Ein lokaler Administrator kann also keinen Supervisor anlegen und sich selbst auch nicht diese Rechte einräumen.

Funktionsrechte

Die nachfolgende Tabelle zeigt Ihnen eine Übersicht aller Funktionsrechte, die insgesamt für Administrator-Konten konfigurierbar sind. Die Verfürbarkeit einzelner der Funktionsrechte kann dabei – je nach Funktionsumfang des Gerätes – variieren. Sofern die Funktionsrechte auf der Konsole oder in einem Skript setzen möchten, haben Sie die Möglichkeit, alternativ zur Klartext-Bezeichnung des jeweiligen Rechtes die Hexschreibweise zu verwenden. Mehr dazu erfahren Sie im Abschnitt *Hexadezimale Kombination von Funktionsrechten auf der Konsole* auf Seite 139.

Bezeichnung: [1]LANconfig, [2]Setup-Menü	***Hexschreibweise an der Konsole***	***Rechtebeschreibung***
1. AP-Assignment-Assistent **2.** WTP-Zuordnungs-Assistent	0x00000400	Assistent für die Zuweisung von WLAN-Profilen
1. Content-Filter-Assistent **2.** CF-Profil-Assistent	0x00040000	Assistent für die Einrichtung des Content-Filters
1. Dynamic-DNS-Assistent **2.** Dynamic-DNS-Assistent	0x00004000	Assistent für die Konfiguration von Dynamic DNS
1. Einstellen von Datum und Uhrzeit **2.** Zeit-Setzen	0x00000040	Setzen von Uhrzeit und das Datum (gilt auch für Telnet und TFTP)
1. Grundeinst.-Assistent **2.** Grundkonfigurations-Assistent	0x00000001	Assistent für die Grundeinstellungen
1. Internet-Assistent **2.** Internet-Assistent	0x00000004	Assistent für die Einrichtung des Internetzugangs
1. LAN-LAN-Assistent **2.** LANLAN-Assistent	0x00000020	Assistent für die Verbindung zweier lokaler Netze (VPN)
1. Public-Spot-Assistent (Benutzer anlegen) **2.** Public-Spot-Assistent	0x00000800	Assistent für die Einrichtung von Public Spot-Benutzern*
1. Public-Spot-Assistent (Benutzer verwalten) **2.** Public-Spot-Benutzerverwaltungs-Assistent	0x00100000	Assistent für die Verwaltung von Public Spot-Benutzern*
1. – **2.** Public-Spot-Konfigurations-Assistent	0x00200000	Assistent für die Einrichtung eines Public Spots

Bezeichnung: [1]LANconfig, [2]Setup-Menü	*Hexschreibweise an der Konsole*	*Rechtebeschreibung*
1. Public-Spot-XML-Interface **2.** Public-Spot-Xml-Schnittstelle	0x00080000	Zugriff auf die XML-Schnittstelle des Public Spot-Moduls **Hinweis:** Ein 'normaler' Public Spot-Administrator benötigt dieses Recht nicht. Das Recht dient vielmehr dazu, einem externen Gateway – z. B. einer Maschine oder einem Programm (Webserver, Skript etc.) – die Kommunikation mit dem Modul zu ermöglichen, um komplexe Anmeldeszenarien zu realisieren. Näheres dazu siehe *LANCOM Public Spot XML-Interface*.
1. RAS-Assistent **2.** RAS-Assistent	0x00000010	Assistent für die Einrichtung eines Einwahlzugangs (RAS, VPN)
1. Rollout-Assistent **2.** Rollout-Assistent	0x00002000	Assistent für den Rollout*
1. Sicherheits-Assistent **2.** Sicherheits-Assistent	0x00000002	Assistent für die Kontrolle der Sicherheitseinstellungen
1. SSH-Client **2.** SSH-Kommando	0x00020000	Herstellen einer SSH-/Telnet-Verbindung von Ihrem Gerät zu anderen HiLCOS-Geräten oder SSH-/Telnet-Servern
1. Suche weiterer Geräte im LAN **2.** Geraetesuche	0x00000080	Suche nach weiteren Geräten in lokalen und entfernten Netzen*
1. WLAN-Assistent **2.** WLAN-Assistent	0x00001000	Assistent für die Konfiguration der WLAN-Schnittstelle
1. WLAN-Linktest **2.** WLAN-Linktest	0x00000100	Ausführen des WLAN Link-Tests* (gilt auch für Telnet)
1. WLC-Profil-Assistent **2.** WLC-Profil-Assistent	0x00010000	Assistent für die Einrichtung eines WLC-Profils
1. CA-Web-Schnittstellen-Assistent **2.** CA-Web-Schnittstelle	0x1000000	Erstellen für Profile der CA-Web-Schnittstelle

Tabelle 14: Übersicht der Funktionsrechte

*) Die Berechtigung bzw. das Ausführen dieses Assisteten oder dieser Funktion bezieht sich – sofern nicht anders erwähnt – ausschließlich auf WEBconfig. Entweder ist der betreffende Assistent oder die betreffende Funktion nur dort

verfügbar (z. B. Einrichten und Verwalten von Public Spot-Benutzern) oder nur dort beschränkbar (z. B. Suche nach Geräten).

Hexadezimale Kombination von Funktionsrechten auf der Konsole

Da die Konfiguration mehrerer Funktionsrechte über die Klartext-Bezeichnung beim Skripten einen hohen Schreibaufwand verursacht, haben Sie alternativ auch die Möglichkeit, an Stelle der Bezeichnungen deren Hexwerte zu verwenden und diese Einzelwerte als kombinierte Summe in Ihr Skript-Kommando einzubauen.

Die Summe mehrerer Hex-Werte ergibt sich aus der hexadezimalen Addition der ersten, zweiten, dritten … n-ten Stelle von rechts. Soll der Benutzer z. B. die Funktionen **Sicherheits-Assistent**, **Provider-Auswahl**, **RAS-Assistent**, **Zeit-Setzen** und **WLAN-Linktest** ausführen dürfen, berechnet sich die Summe der einzlnen Hexwerte wie folgt:

- 1. Stelle rechts: `2` (Sicherheits-Assistent) + `8` (Provider-Auswahl) = a
- 2. Stelle rechts: `1` (RAS-Assistent) + `4` (Zeit-Setzen) = `5`
- 3. Stelle rechts: `1` (WLAN-Linktest) = `1`

Für dieses Beispiel tragen die Funktionsrechte somit den Wert `0x0000015a`. Anders ausgedrückt handelt es sich hierbei um eine ODER-Verknüpfung der Hexadezimal-Werte:

Bezeichnung auf der Konsole	Wert
Sicherheits-Assistent	`0x00000002`
Provider-Auswahl	`0x00000008`
RAS-Assistent	`0x00000010`
Zeit-Setzen	`0x00000040`
WLAN-Linktest	`0x00000100`
ODER-verknüpft	`0x0000015a`

Tipp: Alternativ zur Schreibweise `0x0000015a` stehen Ihnen auch die verkürzten Kurzschreibweisen `0000015a`, `0x15a` und `15a` zur Option.

Konfigurationsbeispiel auf der Konsole

Mit dem folgenden Befehl legen Sie in der Kurzschreibweise einen neuen Benutzer in der Admintabelle (im Setup-Menü unter **Config** > **Admins**) an, der als lokaler Administrator `NetAdmin` mit dem Passwort `BW46zG29` den Internetprovider auswählen darf. Der Benutzer wird dabei sofort aktiviert:

```
set NetAdmin BW46zG29 ja Admin-RW 8
```

Mit dem folgenden Befehl erweitern Sie die Funktionsrechte dahingehend, das Benutzer `NetAdmin` auch den WLAN-Link-Test ausführen darf. Die Sternchen im Kommando stehen dabei für die nicht zu verändernden Werte:

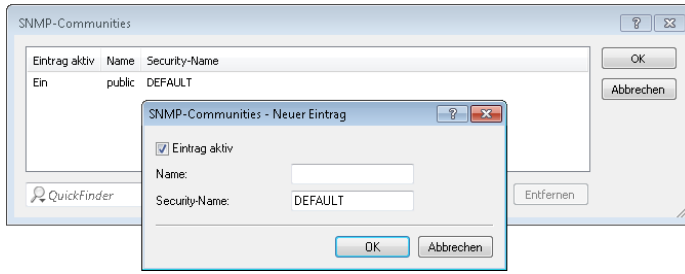
```
set NetAdmin * * * 108
```

2.11.2 Konfigurieren des SNMP-Lesezugriffs

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten “Community”, welche die Bedeutung eines Passworts bzw. Zugangsschlüssel inne hat. Die Authentifizierung kann hierbei wahlweise

- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff), oder
- eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen. Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig unter **Management** > **Admin** mit einem Klick auf **SNMP-Einstellungen** und **SNMP-Communities** eigene Communities zu definieren.



Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community. Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Hinweis: Der SNMP-Schreibzugriff bleibt ausschließlich Administratoren mit entsprechenden Berechtigungen vorbehalten.

Hinweis: Mehr Informationen zu SNMP finden Sie im Kapitel *Simple Network Management Protocol (SNMP)*

2.12 Geräteinterne SSH-/SSL-Schlüssel

Sämtliche Geräte, die mit einer HiLCOS-Version vor 8.90 ausgeliefert werden, sind ab Werk mit einem Satz vordefinierter Kryptographie-Schlüssel mit 1024 Bit Länge ausgestattet, die folgende Fingerprints abbilden:

```
SSH
    ssh-dss 27:c5:1d:9f:be:27:3d:50:d7:bf:c1:68:0b:18:97:d7
    ssh-rsa 03:56:e6:52:ee:d2:da:f0:73:b5:df:3d:09:08:54:b7
SSL
    SHA-1: f9:14:7f:7c:e0:15:20:b6:71:94:46:3f:0e:00:93:9c:ad:ff:d9:fb
    MD5:   ac:5b:45:2d:f9:20:3e:0b:b0:45:35:44:b8:3a:de:c6
```

Das Gerät übermittelt diese Fingerprints beim Aufbau gesicherter Verbindungen (z. B. via SSH oder SSL) an die anfragende Gegenstelle. Die Gegenstelle kann anhand des Fingerprints 1.) das Gerät eindeutig identifizieren und 2.) für sich verifizieren, den Verbindungsaufbau mit dem korrekten als vertrauenswürdig eingestuften Gerät durchgeführt zu haben.

Wenn Sie also z. B. in LANconfig als Kommunikationsprotokoll SSH auswählen und darüber erstmalig eine Verbindung zum betreffenden Gerät aufbauen, hinterfragt LANconfig in einer Sicherheitsabfrage, ob Ihnen der zugehörige ssh-rsa-Schlüssel vertraut ist und LANconfig das Gerät darüber zukünftig als 'bekannt' registrieren soll.

Wichtig: Da diese Schlüssel für alle Geräte gleich sind, sollten Sie diese Schlüssel für den Produktivbetrieb unbedingt durch eigene individuelle Schlüssel ersetzen (vgl. *Automatische Erzeugung gerätespezifischer SSH-/SSL-Schlüssel* auf Seite 142). Modelle mit bestimmten Firmware-Versionen und hinreichender Entropie versuchen teils auch automatisch, gerätespezifische Schlüssel zu erzeugen (vgl. *Automatische Erzeugung gerätespezifischer SSH-/SSL-Schlüssel* auf Seite 142).

2.12.1 Automatische Erzeugung gerätespezifischer SSH-/SSL-Schlüssel

Sofern Sie ein Gerät mit HiLCOS 8.90 oder höher einsetzen und keinen individuellen Schlüssel ins Gerät geladen haben, versucht der interne SSH-Server

nach einem Konfigurations-Reset direkt beim Systemstart, eigene gerätespezifische SSH-Schlüssel zu kompilieren. Dazu gehören

- ein SSH-2-RSA-Schlüssel mit 2048 Bit Länge;
- ein SSH-2-DSS-Schlüssel mit 1024 Bit Länge (Definition nach FIPS 186-2);
- ein SSH-2-ECDSA-Schlüssel mit 256, 384 oder 521 Bit Länge;
- ein SSL-RSA-Schlüssel mit 2048 Bit Länge;

welche das Gerät als `ssh_rsakey`, `ssh_dsakey`, `ssl_privkey` oder `ssh_ecdsakey` in seinem internen Dateisystem ablegt.

Im Falle einer erfolgreichen Schlüsselerzeugung erfolgt der Eintrag `SSH: … host key generated` als “Hinweis” ins SYSLOG; bei fehlgeschlagener Erzeugung der Eintrag `SSH: host key generation failed, try later again with '…'` als “Alarm”. Bei fehlgeschlagener Erzeugung (z. B. mangelnder Entropie) erfolgt ein Rückfall auf den werksseitig implementierten Kryptographie-Schlüssel.

Wichtig: Wenn Sie von einer älteren HiLCOS-Version ein Update auf 8.90 oder höher ohne anschließenden Konfigurations-Reset durchführen, generiert das Gerät keinen gerätespezifischen SSH-/SSL-Schlüssel, um die Kompatibilität zu Bestandsinstallationen zu wahren. Sie haben jedoch die Möglichkeit, die Schlüsselerzeugung manuell zu initiieren. Geben Sie dazu an der Konsole die folgenden Befehle ein:

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
```

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
sshkeygen -t rsa -b 2048 -f  ssl_privkey
```

2.12.2 Individuelle SSH-Schlüssel manuell erzeugen

Sie haben die Möglichkeit, die werksseitig installierten sowie die automatisch generierten SSH-/SSL-Schlüssel durch eigene RSA- und DSA- oder DSS-

Schlüssel zu ersetzen, um z. B. eine höhere Verschlüsselungsstärke zu realisieren. Dafür stehen Ihnen mehrere Wege zur Auswahl:

- Sie lassen den individuellen Schlüssel auf der Konsole direkt durch HiLCOS erzeugen.
- Sie erzeugen mit einem externen Programm einen OpenSSH-Private-Key und laden diesen Schlüssel anschließend als `SSH - DSA-Schlüssel […]` oder `SSH - RSA-Schlüssel (*.key [BASE64 unverschlüsselt])` in das Gerät.

Der Weg über ein externes Programm bietet sich z. B. dann an, wenn Ihr Gerät über keine hinreichende Entropie verfügt und dadurch die Schlüsselerzeugung unter LCOS fehlschlägt.

SSH-Schlüsselerzeugung unter HiLCOS

Die Erzeugung eines Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – starten Sie an der Konsole des Gerätes mit folgendem Befehl:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-?, -h
Zeigt eine kurze Hilfe der möglichen Parameter.

-t (dsa|rsa|ecdsa)
Dieser Parameter bestimmt den Typ des erzeugten Schlüssels. Insgesamt unterstützt SSH folgende Typen von Schlüsseln:

- RSA-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis zu 16384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 1024 bis 2048 Bit.
- DSA-Schlüssel folgen dem Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST) und werden z. B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. DSA- oder DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.
- ECDSA-Schlüssel sind eine Variante von DSA-Schlüsseln, bei der das Gerät für die Schlüsselerzeugung elliptische Kurven verwendet (Elliptic Curve Cryptography, ECC). Die ECC ist eine Alternative zu

den klassischen Signatur- und Schlüsselaustauschverfahren wie RSA und Diffie-Hellman. Der Hauptvorteil von elliptischen Kurven liegt darin, dass Sie durch deren mathematische Eigenschaften die gleiche Schlüsselstärke wie bei RSA oder Diffie-Hellman mit einer deutlich kürzeren Schlüssellänge erreichen. Dies erlaubt eine bessere Leistung bei äquivalenter Hardware. ECC und deren Integration in SSL und TLS sind in den RFCs 5656 und 4492 beschrieben.

Wenn Sie keinen Typ angeben, erzeugt das Kommando immer einen RSA-Schlüssel.

-b <Bits>

Dieser Parameter bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel. Wenn Sie keine Länge angeben, erzeugt das Kommando immer einen Schlüssel mit einer Länge von 1024 Bit.

-f <OutputFile>

Über diesen Parameter geben Sie den Mountingpoint der erzeugten Schlüsseldatei im Dateisystem des Gerätes an. Die Wahl des Mountingpoints hängt davon ab, was für einen Schlüssel sie von welchem Typ erzeugen. Zur Auswahl stehen Ihnen in diesem Fall:

- `ssh_rsakey` für RSA-Schlüssel
- `ssh_dsakey` für DSA-Schlüssel
- `ssh_ecdsakey` für ECDSA-Schlüssel
- `ssl_privkey` für SSL-RSA-Schlüssel

-q

Dieser Parameter aktiviert den 'Quiet'-Modus für die Schlüsselerzeugung. Wenn Sie diesen Parameter setzen, überschreibt LCOS bereits existierende RSA- oder DSA-Schlüssel ungefragt; Ausgaben über den Fortschritt der Operation entfallen. Nutzen Sie diesen Parameter z. B. in einem Skript, um die Bestätigung von Sicherheitsabfragen durch den Benutzer zu unterdrücken.

SSH-Schlüsselerzeugung unter Linux-Systemen

Zahlreiche Linux-Distributionen haben das OpenSSH-Paket bereits installiert. Hier genügt ein einfacher Befehl an der Shell, um die gewünschte Schlüssel-

datei zu erzeugen. Die verwendete Syntax entspricht dabei der des HiLCOS-Befehls `sshkeygen`:

```
ssh-keygen [-t (dsa|rsa)] [-b <Bits>] [-f <OutputFile>]
```

Mit einem Befehl `ssh-keygen -t rsa -b 4096 -f hostkey` erzeugen Sie also einen RSA-Schlüssel mit 4096 Bit Länge, welcher sich aus dem privaten Bestandteil 'hostkey' und dem öffentlichen Bestandteil 'hostkey.pub' zusammensetzt.

SSH-Schlüsselerzeugung unter Windows-Systemen

Windows-Systeme sind von Haus aus nicht dazu in der Lage, SSH-Schlüssel zu kompilieren. Nutzen Sie stattdessen entsprechende Hilfsprogramme wie die freie Software PuTTYgen.

Eine Anleitung, wie Sie mit PuTTYgen einen individuellen Schlüssel erstellen, finden Sie im Abschnitt *SSH-Schlüsselpaar erzeugen mit PuTTY* auf Seite 147. Befolgen Sie darin die einzelnen Schritte; speichern Sie den Schlüssel nach seiner Erzeugung jedoch **nicht** über die Schaltflächen **Save public key** und **Save private key**, sondern wählen Sie **Conversions** > **Export OpenSSH key**. Der so erstellte OpenSSH-Private-Key lässt sich anschließend ohne weitere Bearbeitung ins Gerät laden.

2.13 SSH-Authentifizierung mit Hilfe eines Public-Keys

Das SSH-Protokoll und der HiLCOS-eigene SSH-Server unterstützen zwei verschiedene Authentifizierungs-Mechanismen:

1. interaktiv durch Eingeben eines Benutzernamens und Passworts über die Tastatur;
2. automatisiert durch Übermitteln eines öffentlichen Schlüssels (Public-Key)

Beim Public-Key-Verfahren wird ein Schlüsselpaar aus privatem und öffentlichem Schlüssel verwendet – ein digitales Zertifikat. Der private Teil des Schlüsselpaares wird beim Client bzw. Nutzer gespeichert (häufig mit einem Kennwort – auch Passphrase genannt – geschützt); der öffentliche Teil wird in das Gerät geladen. Da die Schlüssel individuell und anwenderbezogen sein

müssen, existieren keine vordefinierten Standardschlüssel. Im Auslieferungszustand unterstützt Ihr Gerät daher nur die interaktive Authentifizierung über Zugangsdaten.

Die nachfolgenden Abschnitte beschreiben, wie Sie einen eigenen SSH-Schlüssel generieren und die Authentifizierung mit Hilfe eines öffentlichen Schlüssels realisieren. Als Anwendungen dienen exemplatisch LANconfig sowie der freie SSH-Client PuTTY, über dessen Hilfsprogramm PuTTYgen auch die Erzeugung des benötigten Schlüsselpaares erfolgen kann. PuTTY selbst ist sowohl für Windows- als auch Linux-Betriebssysteme erhältlich; die nachfolgenden Abschnitte beschränken sich jedoch – analog zu LANconfig – vorwiegend auf die Windows-Variante.

Tipp: Ihr Gerät unterstützt sowohl RSA als auch DSA- bzw. DSS-Schlüssel. RSA-Schlüssel sind etwas kleiner und erlauben so einen etwas schnelleren Betrieb. Weitere Informationen zu diesen Schlüsseln finden Sie auch im VPN-Kapitel des Referenzhandbuchs im Abschnitt *Einsatz von digitalen Zertifikaten* auf Seite 837.

2.13.1 Ablauf der Zertifikatsprüfung beim SSH-Zugang

Beim Aufbau der SSH-Verbindung erkundigt sich der Client zunächst beim Gerät, welche Authentifizierungs-Methoden für diesen Zugang zugelassen sind. Sofern das Public-Key-Verfahren erlaubt ist, sucht der Client nach installierten privaten Schlüsseln und übergibt diese mit der Angabe des Benutzernamens zur Prüfung an das Gerät.

Findet das Gerät in der Liste seiner öffentlichen SSH-Schlüssel einen passenden Eintrag, in dem der Benutzername enthalten ist, wird der Zugang über SSH erlaubt. Hat der Client keinen passenden privaten Schlüssel installiert oder auf Seiten des Gerätes gibt es keine Übereinstimmung mit Benutzernamen oder öffentlichem Schlüssel, fordert das Gerät die Authentifizierung mit Benutzername/Kennwort an (sofern diese Authentifizierungs-Methode erlaubt ist) oder bricht den Authentifizierungsprozess ab.

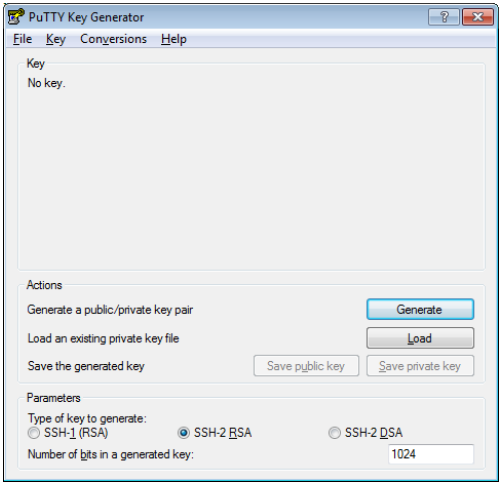
2.13.2 SSH-Schlüsselpaar erzeugen mit PuTTY

Für die SSH-Authentifizierung mit Hilfe eines Public-Keys benötigten Sie zu allererst ein persönliches Schlüsselpaar. Dieses Tutorial beschreibt, wie Sie

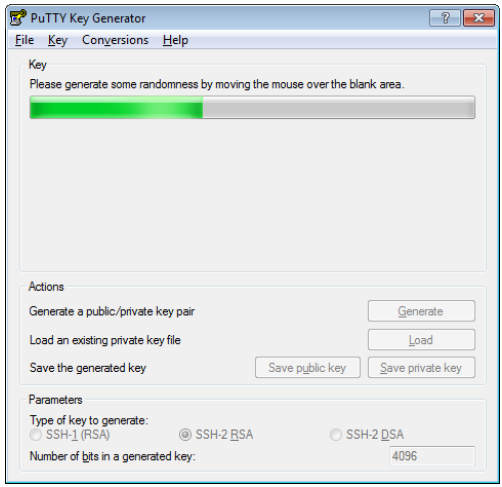
mit PuTTYgen ein RSA-Schlüsselpaar – bestehend aus Public Key und Private Key – erzeugen.

Unter Linux-Betriebssystemen erstellt der Befehl `ssh-keygen` an der Shell ein RSA-Schlüsselpaar aus dem öffentlichen Teil 'id_rsa.pub' und dem privaten Teil 'id_rsa'.

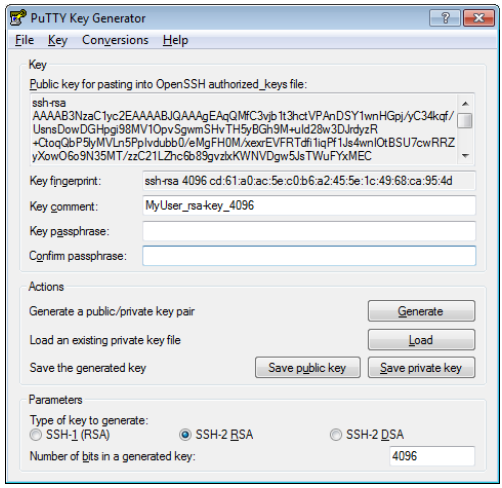
1. Starten Sie das PuTTY-Hilfsprogramm **PuTTYgen**. Es öffnet sich das Hauptfenster des **PuTTY Key Generator**s.



2. Wählen Sie die Art des zu erzeugenden Schlüssels (hier: **SSH-2-RSA**) und dessen Bit-Stärke (z. B. `4096`). Klicken Sie dann auf **Generate**, um mit der Schlüsselerzeugung zu beginnen.
3. Bewegen Sie die Maus daher solange willkürlich im Programmfenster, bis der Forschrittsbalken das Ende erreicht hat. PuTTYgen generiert die für die Schlüsselerzeugung notwendigen Zufallszahlen aus den Bewegungen des Mauszeigers, die Sie innerhalb des Programmfensters vollziehen. Nach Abschluss der Erzeugung zeigt Ihnen das Programm die erzeugten Schlüsseldaten im Hauptfenster an.



4. PuTTYgen generiert die für die Schlüsselerzeugung notwendigen Zufallszahlen aus den Bewegungen des Mauszeigers, die Sie innerhalb des Programmfensters vollziehen. Bewegen Sie die Maus daher solange willkürlich im Programmfenster, bis der Forschrittsbalken das Ende erreicht hat.



5. Optional: Sofern Sie Ihren Private-Key mit einer zusätzlichen Passphrase absichern möchten, tragen Sie diese im Feld **Key passphrase** ein und bestätigen die Eingabe im Feld darunter.

Bitte beachten Sie, dass einige SSH-Clients das Speichern einer Passphrase nicht oder nur für die aktuelle Sitzung erlauben (PuTTY z. B. nur über Pageant). Es kann daher sinnvoll sein, auf die Eingabe einer Passphrase zu verzichten, sofern Sie diese beim Verbindungsaufbau nicht manuell eingeben wollen. LANconfig selbst unterstützt das persistente Speichern einer Passphrase.

6. Klicken Sie auf die Schaltflächen **Save public key** und **Save private key**, um Ihren öffentlichen und Ihren privaten Schlüssel zu speichern.
   Den so erstellten öffentlichen Schlüssel hinterlegen Sie nach anschließender Bearbeitung im Gerät; den privaten Schlüssel verwenden Sie in Kombination mit PutTTY für die Authentisierung.
7. Wählen Sie außerdem **Conversions** > **Export OpenSSH key**, um den Schlüssel gleichzeitig als OpenSSH Private-Key abzuspeichern.
   Den so erstellten privaten Schlüssel verwenden Sie in Kombination mit LANconfig für die Authentisierung.
8. Beenden Sie PuTTYgen. Gehen Sie anschließend zum nächsten Einrichtungskapitel über.

2.13.3 Syntax und Benutzer öffentlicher Schlüssel anpassen

Nachdem Sie ein Schlüsselpaar erzeugt haben, müssen Sie den dazugehörigen Public Key in eine vom Gerät akzeptierte und lesbare Form bringen. Ein HiLCOS-Gerät erwartet die öffentlichen Schlüssel in der folgenden Syntax:

```
<EncryptionAlgorithm> <PublicKey> <Admin1> [<Admin2> … <AdminN>]
```

Sie können somit einem einzigen öffentlichen Schlüssel mehrere Benutzerkonten zuweisen. Ebenso ist es möglich, mehrere Schlüssel für unterschiedliche Benutzer das Gerät zu laden. Die nachfolgenden Schritte beschreiben anhand einer mit PuTTYgen erzeugten Public-Key-Datei, wie Sie einen öffentlichen Schlüssel korrekt anpassen.

1. Öffnen Sie die Public-Key-Datei in einem Texteditor. Es zeigt sich Ihnen folgender oder ähnlicher Inhalt:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key_myuser"
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1wnHGpj/yC34kq
f/UsnsDowDGHpgi98MV1OpvSgwmSHvTH5yBGh9M+uId28w3DJrdyzR+CtoqQbP5l
```

```
…
0N8V3ydp+qbx+8FNbBQCVhxxiKZwXxmMh70pTWHxixOFte4HBxGHxcRaiSoMyNdv
wCkWlx8=
---- END SSH2 PUBLIC KEY ----
```

2. Löschen Sie die Kopf- und Fußzeile sowie die Kommentarzeile, sodass nur noch der eigentliche Schlüssel in der Datei verbleibt. Entfernen Sie anschließend sämtliche Zeilenumbrüche, sodass der öffentliche Schlüssel in einer einzigen Zeile steht.

```
AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8=
```

3. Ergänzen Sie den Anfang des Schlüssels um das Verschlüsselungsalgorhytmus `ssh-rsa` und das Ende um den Namen des Benutzerkontos, für den dieser Key Gültigkeit hat (z. B. `root`); getrennt mit je einem Leerzeichen.
   Sie haben die Möglichkeit, einem Schlüssel mehrere Benutzer zuzuweisen oder mehrere Schlüssel in einer einzigen Public-Key-Datei unterbringen.
   Beispiele:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1j…wCkWlx8= root
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAgEAqQMfC3vjb1t3hctVPAnDSY1…wCkWlx8= root
 admin user
ssh-rsa VLn5PpIvdubb0/eMgFH0M/xexrEVFRTdfi1iqPf1Js4wnIOtBSU…xKWNVDg/ backup
```

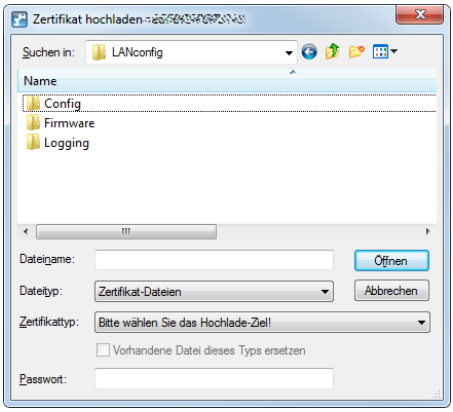
   Hinweis: Achten Sie dabei lediglich darauf, dass jeder Schlüssel (inklusive Verschlüsselungsalgorhytmus und Benutzer[n]) für sich in einer separaten Zeile steht. Zeilenumbrüche machen die Datei ungültig und führen zu einem Fehler bei der späteren Authentifizierung!

4. Speichern Sie die Datei und schließen Sie den Texteditor. Gehen Sie anschließend zum nächsten Einrichtungskapitel über.

2.13.4 Gerät für die Public-Key-Authentifizierung einrichten

Dieses Tutorial beschreibt, wie Sie die Schlüsseldatei ins Gerät laden und das Gerät für die SSH-Authentifizierung vorbereiten.

1. Starten Sie LANconfig und markieren Sie das Gerät, für das Sie die SSH-Authentifizierung einrichten wollen.
2. Wählen Sie **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** und ändern Sie im sich öffnenden Fenster die Auswahllisten **Dateityp** auf **Alle Dateien** sowie **Zertifikattyp** auf **SSH - akzeptierte öffentliche Schlüssel**.

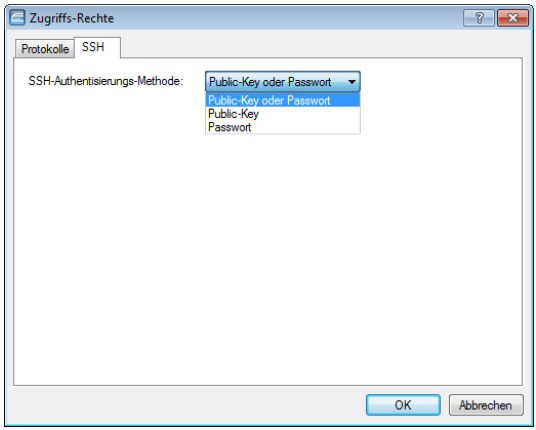


3. Wählen Sie die zuvor erstellte Public-Key-Datei aus und klicken Sie **Öffnen**. LANconfig beginnt daraufhin mit dem Upload des öffentlichen Schlüssels in das Gerät.

   Hinweis: Die hochgeladene Datei ersetzt die Liste der bisher ggf. im Gerät vorhandenen akzeptierten Schlüssel. Alternativ können Sie in WEBconfig die Schlüssel auch direkt editieren und einzelne Schlüssel an die bestehende Liste anhängen (siehe *Erlaubte öffentliche SSH Schlüssel* auf Seite 50).

4. Öffnen Sie den Konfigurationsdialog des Gerätes und wechseln Sie in den Dialog **Management** > **Admin**.
5. Konfigurieren Sie im Abschnitt **Konfigurations-Zugriffs-Wege** unter **Zugriffsrechte** > **…** > **SSH** für jedes Netz die **SSH-Authentisierungs-Methode**.
   Die zulässigen Authentifizierungs-Methoden für den SSH-Zugang können für LAN, WAN und WLAN getrennt eingestellt werden. Folgende Möglichkeiten zur Auswahl:

- **Public-Key oder Passwort**: Hier wird zuerst die Authentisierungs-Methode Public-Key versucht. Sollte dieses scheitern wird die Passwort-Abfrage gewählt.
- **Public-Key**: Hier wird nur die Authentisierungs-Methode Public-Key versucht.
- **Passwort**: Die Authentisierungs-Methode Public-Key wird abgeschaltet und es erfolgt die Passwort-Abfrage.

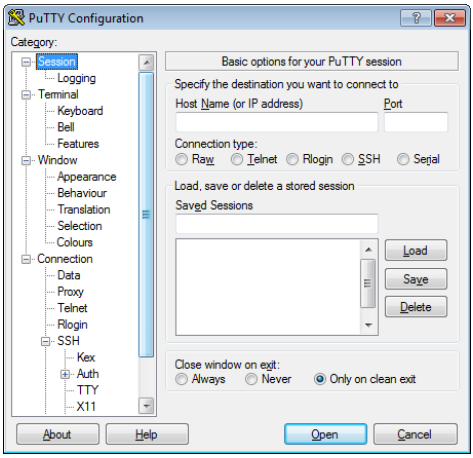


6. Schließen Sie den Konfigurationsdialog und schreiben Sie die Konfiguration auf das Gerät zurück. Gehen Sie anschließend zum nächsten Einrichtungskapitel über.

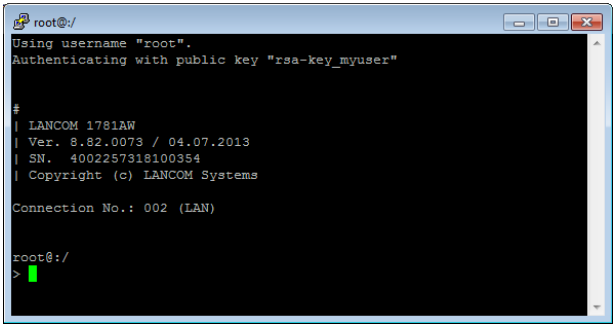
2.13.5 Public-Key-Authentifizierung mit PuTTY

Dieses Tutorial beschreibt, wie Sie in PuTTY die SSH-Authentifizierung mit Hilfe eines Public-Keys konfigurieren und sich anschließend am konfigurierten Gerät anmelden.

1. Starten Sie PuTTY.
2. Geben Sie im sich öffnenden Fenster den Host-Namen oder die IP-Adresse des Gerätes an, und wählen Sie als **Connection type** die Option **SSH**. Der Standardport für SSH-Verbindungen ist 22.



3. Wechseln Sie in den Dialog **Connection** > **Data** und tragen Sie in das Eingabefeld **Auto-login username** den Benutzernamen ein, auf den Sie den Public-Key zuvor ausgestellt haben (z. B. `root`).
4. Wechseln Sie in den Dialog **Connection** > **SSH** > **Auth** und geben Sie im Eingabefeld **Private key file for authentication** den Pfad sowie den Dateinamen der Private-Key-Datei an, die Sie speziell für PuTTY erstellt haben.
5. Klicken Sie abschließend auf **Open**. PuTTY beginnt daraufhin mit dem Verbindungsaufbau unter Verwendung der SSH-Authentifizierung mit Hilfe eines Public-Keys.



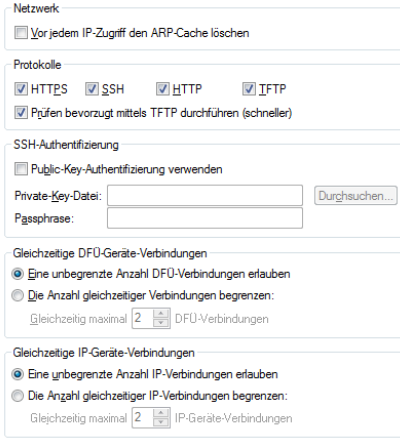
Hinweis: Sofern Sie Ihre Private-Key-Datei mit einer optionalen Passphrase gesichert haben, fragt PuTTY diese im Rahmen des Anmeldevorgangs bei Ihnen ab.

Fertig!

2.13.6 Public-Key-Authentifizierung mit LANconfig

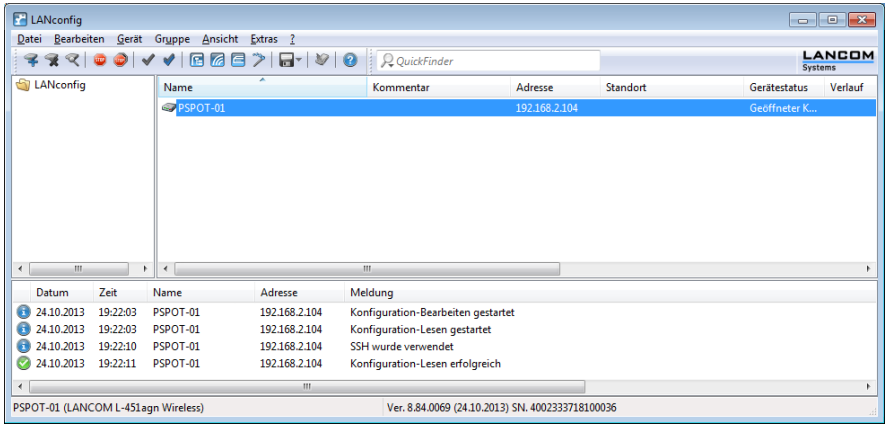
Dieses Tutorial beschreibt, wie Sie in LANconfig die SSH-Authentifizierung mit Hilfe eines Public-Keys konfigurieren.

1. Starten Sie LANconfig.
2. Öffnen Sie über die Menüleiste den Dialog **Extras** > **Optionen** > **Kommunikation**.



3. Deaktivieren Sie im Bereich **Protokoll** mit Ausnahme von **SSH** und **Prüfen bevorzugt mittels TFTP durchführen** alle anderen Auswahlkästchen bzw. Protokolle.
   Dadurch verhindern Sie, dass LANconfig ein anderes Protokoll bei der Gerätekommunikation bevorzugt (z. B. HTTPS) oder bei Fehlschlagen der Authentifizierung auf ein anderes, womöglich unverschlüsseltes Protokoll (z. B. HTTP) ausweicht.
4. Aktivieren Sie die Option **Public-Key-Authentifizierung verwenden**.
5. Geben Sie passend dazu den Pfad und den Dateinamen der OpenSSH Private-Key-Datei an, und benennen Sie ggf. die Passphrase, mit der Ihr Schlüssel gesichert ist.
6. Schließen Sie den Dialog mit Klick auf **OK**, um den Einstellungsdialog zu schließen.

Fertig! Wenn Sie nun für ein Gerät den Konfigurationsdialog oder den Setup-Assistenten öffnen, wählt LANconfig die Kommunikation über das SSH-Protokoll und versucht, sich mit dem angegebenen Private-Key zu authentisieren.



2.14 SSH- und Telnet-Client im HiLCOS

2.14.1 Einleitung

Neben einem SSH-Server, der Ihnen eine sichere und authentifizierte Einwahl in das Gerät ermöglicht (siehe *SSH-Authentifizierung mit Hilfe eines Public-Keys* auf Seite 146), verfügt das Betriebssystem Ihres Gerätes auch über einen SSH-Client. Über diesen SSH-Client haben Sie die Möglichkeitet, von Ihrem Gerät aus SSH-Verbindungen zu einem entfernten Server – z. B. einem weiteren Gerät oder einem Linux-Server – aufbauen. Diese Funktion ist auch dann nützlich, wenn eine direkte Verbindung einem entfernten System nicht möglich ist, aber eine indirekte Verbindung über ein anderes Gerät existiert, welches aus beiden Subnetzen erreichbar ist.

Sie starten den LCOS-eigenen SSH-Client über einfache Befehle an der Konsole, ähnlich dem OpenSSH-Client auf einem Linux- oder Unix-System.

2.14.2 Syntax des SSH-Clients

Die SSH-Verbindung zu einem entfernten System über den HiLCOS-eigenen SSH-Client starten Sie an der Konsole mit folgendem Befehl:

```
ssh [-(?|h)] [-(b|a) <Loopback-Address>] [-p <Port>] [-C] [-j <Interval>]
[<User>@]<Host> <Command>
```

Die einzelnen Parameter haben dabei die folgende Bedeutung:

-?, -h
Zeigt eine kurze Hilfe der möglichen Parameter.

-b, -a <Loopback-Address>
Ermöglicht die Angabe einer Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig: Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät das entfernte System anspricht. Dies kann z. B. dann sinnvoll sein, wenn das System über verschiedene Wege erreichbar ist und dieses einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

-p <Port>
Gibt den zu verwendenen Port an. Wenn Sie keinen Port angegeben, verwendet das Gerät den für SSH standardisierten TCP-Port 22.

-C
Wenn Sie diesen Parameter setzen, versucht der SSH-Client, eine Datenkompression über den zlib-Algorithmus mit dem entfernten System auszuhandeln. Wenn das entfernte System diese Kompression nicht unterstützt, werden die Daten ohne Kompression übertragen.

Der Einsatz der Kompression ist in den meisten Fällen nur auf langsamen Verbindungen sinnvoll. Auf schnellen Verbindungen ist der zusätzliche Overhead der Kompression meistens größer als der Gewinn durch die Datenreduzierung.

-j <Interval>
Wenn die Verbindung zu dem entfernten System über einen NAT-Router oder eine Firewall geführt wird, ist es möglicherweise sinnvoll, die Verbindung dauerhaft aufrecht zu erhalten. Bei einer interaktiven SSH-Sitzung werden jedoch phasenweise keine Daten übertragen, was

zu einer Unterbrechung der Verbindung im Gateway aufgrund von Timeouts führen kann. In diesen Fällen kann der SSH-Client regelmäßig Keep-Alive-Pakete senden, die das entfernte System als Leerlaufprozess interpretiert, dem Gateway aber das Fortbestehen der Verbindung signalisieren.

Über diesen Parameter geben Sie das Interval in Sekunden an, in dem Ihr Gerät die Keep-Alive-Pakete verschickt. Die Keep-Alive-Pakete werden dabei nur versendet, wenn der SSH-Client für die Dauer des Intervalls keine anderen Daten an das entfernte System schicken muss.

<User>
Benutzername für die Anmeldung am entfernten System. Wenn Sie keinen expliziten Benutzername angeben, verwendet HiLCOS Ihren aktuellen den Benutzernamen (der, mit dem Sie sich an der Konsole angemeldet haben).

<Host>
DNS-Name oder IP-Adresse des entfernten Systems.

<Command>
Der HiLCOS-eigene SSH-Client kann entweder eine interaktive Shell auf dem entfernten System starten oder nur einen einzelnen Befehl ausführen. Wenn Sie keinen Befehl angeben, wird eine interaktive Shell gestartet.

2.14.3 Syntax des Telnet-Clients

Als Alternative zu SSH können Sie auch mit dem HiLCOS-eigenen Telnet-Client eine Verbindung zu einem entfernten System aufbauen. Den Telnet-Client starten Sie an der Konsole mit folgendem Befehl:

```
telnet [-(?|h)] [-b <Loopback-Address>] <Host> [<Port>]
```

-?, -h
Zeigt eine kurze Hilfe der möglichen Parameter.

-b <Loopback-Address>
Ermöglicht die Angabe einer Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig: Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät das entfernte System anspricht. Dies kann z. B. dann sinnvoll sein, wenn das System über verschiedene Wege erreichbar

ist und dieses einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

<Host>

DNS-Name oder IP-Adresse des entfernten Systems.

<Port>

Gibt den zu verwendenen Port an. Wenn Sie keinen Port angegeben, verwendet das Gerät den für Telnet standardisierten TCP-Port 23.

2.14.4 Öffentliche Schlüssel für die Authentifizierung

SSH nutzt für die Authentifizierung öffentliche Schlüssel, die vom entfernten System übermittelt werden. Wenn ein SSH-Client eine Verbindung zu einem SSH-Server aufbauen will, übermittelt der Server den öffentlichen Schlüssel an den Client, der diesen Schlüssel dann in seinen Dateien sucht. Die folgenden Situationen können dabei auftreten:

- Der SSH-Client findet den Schlüssel in seiner Liste der bekannten Server-Schlüssel, und der Schlüssel ist dem entsprechenden Hostnamen bzw. der IP-Adresse zugeordnet. Die SSH-Verbindung kann dann ohne weitere Benutzeraktivität aufgebaut werden.
- Der SSH-Client findet den Schlüssel **nicht** in seiner Liste der bekannten Server-Schlüssel, und auch keinen anderen Schlüssel vom gleichen Typ (RSA bzw. DSA/DSS) für den entsprechenden Hostnamen bzw. die IP-Adresse. Der SSH-Client geht davon aus, dass es die erste Verbindung zu diesem Server ist und zeigt den öffentlichen Schlüssel und den zugehörigen Fingerabdruck (Fingerprint) an. Der Anwender kann den Schlüssel mit einer auf anderem Wege übermittelten Version verifizieren und entscheiden, ob der Server in der Liste der bekannten SSH-Server gespeichert werden darf. Wenn der Anwender diese Verifizierung ablehnt, wird die SSH-Verbindung sofort beendet.
- Der SSH-Client findet einen Schlüssel für den entsprechenden Hostnamen bzw. die IP-Adresse, dieser weicht aber von dem aktuell verwendeten Schlüssel ab. Beide Schlüssel werden angezeigt, dann wird die SSH-Verbindung beendet, weil der SSH-Client eine Man-in-the-middle-Attacke vermutet. Sofern das entfernte System den öffentlichen Schlüssel kürzlich geändert hat, muss der Administrator den veralteten Eintrag aus der Liste der bekannten Server löschen (siehe *Bekannte SSH-Serverschlüssel manuell entfernen* auf Seite 161.

Nach der erfolgreichen Verifikation des Server-Schlüssels kann der Administrator das Passwort zur Anmeldung am entfernten System eingeben. Das Passwort kann nicht direkt über den Kommandozeilenbefehl eingegeben werden.

SSH-Verbindungen werden üblicherweise durch den Server beendet, z. B. durch Eingabe von `exit` in der Shell. In manchen Fällen ist es nötig, die SSH-Verbindung durch den Client zu beenden, z. B. wenn die Anwendung auf der Server-Seite gestört ist. Der SSH-Client im HiLCOS verwendet die gleiche Zeichenfolge wie OpenSSH zum Beenden einer Verbindung, also die Folge 'Tilde – Punkt'.

Hinweis: Wenn die HiLCOS-Konsolensitzung selbst durch einen OpenSSH-Client geöffnet wurde, wird die Folge 'Tilde – Tilde – Punkt'verwendet, da ansonsten die falsche Verbindung beendet werden würde.

Liste der bekannten SSH-Server

Der SSH-Client im HiLCOS speichert alle ihm bekannten SSH-Schlüssel entfernter Systeme automatisch in einer eigenen Schlüsseldatei. Diese Schlüsseldatei trägt im internen Dateisystem die Bezeichnung **ssh_known_hosts**. Der Inhalt dieser Datei ändert sich jedes Mal, wenn Sie eine Verbindung zu einem Ihrem Gerät unbekannten SSH-Server aufbauen und den Ihnen als Sicherheitsabfrage angezeigten Schlüssel des entfernten Systems akzeptieren.

Jeder Schlüssel ist in dieser Datei in einer Zeile gespeichert und enthält drei Felder:

- Der Name oder die IP-Adresse des entfernten Systems, so wie es beim Aufbau der Verbindung im SSH-Befehl eingegeben wird.
- Der Typ des Schlüssels, also ssh-rsa oder ssh-dss.
- Die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.

Wichtig: Sobald ein Administrator den öffentlichen Schlüssel eines SSH-Servers akzeptiert hat, gilt dieser Eintrag auch für alle übrigen Administratoren; es findet keine benutzerbezogene Unterscheidung statt.

Wichtig: Die in diesem Kapitel benannte(n) Datei(en) sind auf dem Gerät ausschließlich für den Root-Administrator über SCP (siehe *Datei laden über einen SCP-Client* auf Seite 113) zugänglich. Das Hoch- und Herunterladen über LANconfig oder WEBconfig ist nicht möglich.

Bekannte SSH-Serverschlüssel manuell entfernen

Sie haben die Möglichkeit, Ihrem Gerät bekannte SSH-Schlüssel externer Systeme gezielt zu entfernen. Dies ist z. B. dann notwendig, wenn sich der SSH-Schlüssel des externen Servers geändert hat und Ihr Gerät die Verbindung zu diesem System aufgrund eines ihm bereits vorliegenden SSH-Schlüssels verweigert. Dazu verwenden Sie den `sshkeygen`-Befehl im Zusammenhang mit dem Parameter `-R`:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] -R <Host>
```

-?, -h
Zeigt eine kurze Hilfe der möglichen Parameter.

-t (dsa|rsa|ecdsa)
Dieser optionale Parameter bestimmt den Typ des Schlüssels, den das Gerät löscht. Wenn Sie keinen Typ angegeben, löscht das Kommando alle SSH-Schlüssel des angegebenen Hosts.

-R <Host>
Über diesen Parameter benennen Sie die IP-Adresse oder den DNS-Namen des externen Systems, dessen SSH-Schlüssel Sie gezielt von Ihrem Gerät löschen wollen.

Tipp: Um die komplette Liste aller bekannten SSH-Serverschlüssel auf einmal zu löschen, entfernen Sie die Datei **ssh_known_hosts** aus dem Dateisystem Ihres Gerätes.

2.14.5 Schlüssel für den SSH-Client im HiLCOS erzeugen

Die Erzeugung eines Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – starten Sie an der Konsole des Gerätes, dessen HiLCOS-internen SSH-Client Sie nutzen wollen, mit folgendem Befehl:

```
sshkeygen [-(?|h)] [-t (dsa|rsa|ecdsa)] [-b <Bits>]
```

Eine detaillierte Beschreibung der Parameter im `sshkeygen`-Befehl finden Sie im Abschnitt *SSH-Schlüsselerzeugung unter HiLCOS* auf Seite 144. Das Gerät legt die Schlüssel im PEM-Format automatisch unter dem Dateinamen **ssh_rsakey** (für RSA-Schlüssel), **ssh_dsakey** (für DSA- bzw. DSS-Schlüssel) oder **ssh_ecdsakey** (für ECDSA-Schlüssel) in seinem internen Dateisystem ab. Die ID-Dateien entsprechenden dem folgenden Aufbau, der die Nutzung eines Schlüssels für einen bestimmten HiLCOS-Administrator definiert:

```
*** User <MyAdmin>
<SSH-Key>
*** End
```

Öffentlichen Schlüssel abrufen

Nachdem das Gerät das Schlüsselpaar erzeugt hat, müssen Sie den öffentlichen Teil auf das entfernte System übertragen. Den öffentlichen Teil des Schlüssels rufen Sie mit dem folgenden Befehl ab:

```
show ssh idkeys
```

Diese Befehl erzeugt eine Ausgabe ähnlich der folgenden:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAAAQEA28BtnFFInAi8I5B1aOwq5g2Y…0nkuNQ== root@
```

- Der erste Teil zeigt den Typ des Schlüssels (ssh-rsa oder ssh-dss).
- Der zweite Teil ist die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.
- Der dritte Teil enthält den Hostnamen, der mehr als Kommentar gedacht ist.

Öffentlichen Schlüssel auf ein entferntes System übertragen

Sofern es sich bei dem entfernten System um ein Gerät mit HiLCOS handelt, laden Sie den betreffenden DSA- oder RSA-Schlüssel entweder über das Dateimanagement ins Gerät oder ergänzen die Liste der öffentlichen Schlüssel in WEBconfig über den Menüpunkt **Extras** > **Liste erlaubter öffentlicher SSH-Schlüssel bearbeiten** direkt. Kopieren Sie dazu den ersten und zweiten Teil und ersetzen Sie den dritten Teil mit einer Liste von Anwendern, um die Nutzung dieses Schlüssels auf einen Teil der HiLCOS-Administratoren einzugrenzen.

Weitere Informationen zur geforderten Syntax eines öffentlichen Schlüssels, dem Einsatz unterschiedlicher Schlüssel und deren Verknüpfung mit unterschiedlichen Administratoren finden Sie im Abschnitt *Syntax und Benutzer öffentlicher Schlüssel anpassen* auf Seite 150.

2.14.6 Prioritäten für die SSH-Authentifizierung

Die Reihenfolge der SSH-Authentifizierung an einem entfernten System folgt einer festen Prioritätenfolge:

1. Als erste Methode versucht Ihr Gerät immer die Authentifizierung über einen öffentliche Schlüssel; es sei denn, das entfernte System unterstützt diese Methode nicht oder der sich anmeldende Administrator besitzt keinen öffentlichen Schlüssel.
2. Als zweite Methode verwendet Ihr Gerät die interaktive Authentifizierung über die Tastatur, wenn die Authentifizierung über öffentliche Schlüssel prinzipiell nicht verwendet werden kann oder wenn das entfernte System alle öffentlichen Schlüssel des sich anmeldende Administrators abgelehnt hat. Die interaktive Authentifizierung kann je nach Anwendung aus dem Austausch mehrerer Nachrichten zwischen SSH-Client und SSH-Server bestehen; im einfachsten Fall z. B. reicht die Eingabe eines gültigen Zugangspassworts aus.

2.14.7 Berechtigung zur Nutzung des SSH-/Telnet-Clients

Sie haben die Möglichkeit, das Recht zur Nutzung des SSH-/Telnet-Clients für jeden einzelnen Administrator explizit zu vergeben. Dazu setzen Sie beim Hinzufügen oder Bearbeiten von Administratorkonten (in LANconfig unter **Management** > **Admin** > **Weitere Administratoren**) das Funktionsrecht

SSH-Client. Ohne dieses Funktionsrecht kann sich ein Administrator nicht zu einem anderen SSH-/Telnet-Gerät weiterverbinden.

2.15 Basic HTTP Fileserver für externe Speichermedien

2.15.1 Einleitung

Der eingebaute HTTP-Server in HiLCOS bietet Ihnen die Möglichkeit, Dateien von einem USB-Speichermedium über das HTTP-Protokoll bereitzustellen und arbeitet so als einfacher Dateiserver.

Hinweis: Diese Funktion wird ausschließlich von Geräten mit USB-Anschluss unterstützt.

2.15.2 Vorbereitung des USB-Speichermediums

Bevor Sie von Ihrem Gerät auf ein externes Speichermedium zugreifen können, müssen Sie einige Vorbereitungen treffen. Der nachfolgende Abschnitt beschreibt, wie Sie ein USB-Medium für den Einsatz am Gerät einrichten.

1. Formatieren Sie das USB-Medium mit einem FAT16- oder FAT32-Dateisystem.
2. Erstellen Sie auf dem USB-Medium das Verzeichnis `public_html`.
   Der HTTP-Server von LCOS greift nur auf Dateien in diesem Verzeichnis und den evtl. vorhandenen Unterverzeichnissen zu. Alle anderen Dateien auf dem USB-Medium werden ignoriert.

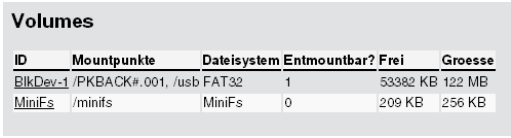
   Tipp: Sie können den Namen des Verzeichnisses im Setup-Menü auch ändern unter **HTTP** > **Datei-Server** > **Oeffentliches-Unterverzeichnis**.

Die Vorbereitung des USB-Mediums ist damit abgeschlossen.

2.15.3 Einhängepunkt des USB-Mediums im HiLCOS ermitteln

Beim Anschließen eines USB-Mediums erzeugt Ihr Gerät automatisch einen Einhängepunkt (Mounting-Point), der von HiLCOS zur internen Verwaltung des Mediums verwendet wird. Dieser Einhängepunkt bleibt für ein bestimmtes USB-Medium immer gleich, auch nach einem Reboot oder Neustart. Verschiedenen Medien wird jeweils ein eigener, eindeutiger Einhängepunkt zugewiesen.

Um auf die Daten des USB-Mediums zugreifen zu können, muss der zugehörige Einhängepunkt bekannt sein. Den Einhängepunkt der USB-Medien ermitteln Sie über das Status-Menü unter **Dateisystem** > **Volumes**.



Volumes

ID	Mountpunkte	Dateisystem	Entmountbar?	Frei	Groesse
BlkDev-1	/PKBACK#.001, /usb	FAT32	1	53382 KB	122 MB
MiniFs	/minifs	MiniFs	0	209 KB	256 KB

Die Status-Tabelle zeigt alle Datenträger (Volumes), die dem Gerät bekannt sind:

- `MiniFs` ist das eingebaute Flash-Dateisystem, das es auf fast allen Geräten gibt.
- `BlkDev-n` bezeichnen die bekannten USB-Medien. Wenn nur ein USB-Massenspeichergerät angeschlossen ist, wird es `BlkDev-1` genannt und unter `/usb` eingehangen.

2.15.4 Zugriff auf die Dateien eines USB-Mediums

Um auf die Dateien auf dem USB-Medium über den HTTP-Server im LCOS zuzugreifen, verwenden Sie die folgende URL:

```
http://<Device-IP-Adress>/filesrv/<Mounting-Point>/<File>
```

Wenn z. B. eine Datei `coupon.jpeg` benannt ist und auf dem einzigen USB-Medium im Basisverzeichnis unter `\public_html` gespeichert ist, dann können Sie mit folgendem Link darauf zugreifen:

```
http://<Device-IP-Adress>/filesrv/usb/coupon.jpeg
```

Tipp: Der Zugriff kann auch über HTTPS anstatt HTTP erfolgen.

2.15.5 Regeln für den Verzeichniszugriff

Das Verzeichnis `\public_html` darf Unterverzeichnisse beinhalten. Sie haben die Möglichkeit, auf diese Verzeichnisse zugreifen, ohne eine darin enthaltene Datei anzugeben. Wenn in einem Verzeichnis eine Datei mit dem Namen `index.html` oder `index.htm` existiert, dann wird diese zum HTTP-Client übertragen. Andernfalls gibt der Fileserver eine Liste aller Dateien und Verzeichnisse aus, die im aufgerufenen Verzeichnis existieren.

2.15.6 Unterstützte Inhaltstypen

Der HTTP-Server im LCOS nutzt die Dateierweiterung, um den MIME-Inhaltstyp zu bestimmen, der für die korrekte Darstellung der Inhalte im Browser benötigt wird. Momentan sind die folgenden Erweiterungen bekannt und werden in einen korrekten MIME-Inhaltstyp übersetzt:

- .htm und .html für HTML-Dateien
- .gif, .jpg, .jpeg, .png, .bmp, .pcx für entsprechende Formate der Bilddateien
- .ico für Icon-Dateien
- .pdf für Adobe Acrobat PDF-Dateien
- .css für Cascading-Style-Sheet-Dateien

2.16 Rollout-Assistent

In größeren Projekten zur Vernetzung richten die Administratoren eines Unternehmens oft zahlreiche Geräte vom gleichen oder ähnlichen Typ an unterschiedlichen Standorten ein. Um die persönliche Anwesenheit an den jeweiligen Standorten zu reduzieren oder ganz zu vermeiden, führen Administratoren oft einen sogenannten Rollout durch. Ein "Rollout" bezeichnet im Netzwerkumfeld einen (weitgehend automatisiert) ablaufenden Vorgang, der dazu dient, ein Gerät auf eine standardisierte Weise für den geplanten Einsatzzweck vorzukonfigurieren. Dabei stehen den Administratoren zwei grundlegende Möglichkeiten zur Verfügung:

1. Die Administratoren bereiten die Geräte in ihrer Zentrale lokal für den Rollout vor. Am Einsatzort führt ein Mitarbeiter oder ein Kunde dann einen speziell angepassten (benutzerdefinierten) Rollout-Assistenten aus, über

den er die standortbezogenen Teile der Konfiguration ergänzt und das Gerät in den gewünschten Betriebszustand bringt.

2. Die Administratoren setzen in ihrer Zentrale *Large Scale Rollout & Management (LSR)* ein. Sämtliche Konfigurationseinstellungen für ein bestimmtes Gerät werden über das Management-System vorgenommen und verwaltet. Am Einsatzort führt ein Mitarbeiter oder ein Kunde dann den standardmäßig im Gerät vorhandenen (Default-)Rollout-Assistenten aus und lädt die Konfiguration vom LSR-Server, um das Gerät in den gewünschten Betriebszustand zu bringen.

Im Unterschied zum benutzerdefinierten Rollout-Assistenten ist es bei Verwendung des Default-Rollout-Wizards zusammen mit LSR also nicht erforderlich, die Konfiguration eines Gerätes in mehreren Etappen durchzuführen; das Einspielen einer aktuellen Komplettkonfigurationen kann nach dem Anschluss des Gerätes unmittelbar durch das LSR erfolgen.

Sofern LSR jedoch nicht zum Einsatz kommen kann oder soll, haben Sie als Administrator mit dem benutzerdefinierten Rollout-Assistenten auch weiterhin die Möglichkeit, einen eigenen Assisten mit beliebig komplexen Umfang für spezielle Aufgaben in das Gerät zu implementieren.

Wichtig: Ein Parallelbetrieb beider Assistenten ist ausgeschlossen. Die Einrichtung benutzerdefinierten Rollout-Assistenten ersetzt den Default-Rollout-Wizard; die Fernkonfiguration durch ein LSR-System ist dann nicht mehr möglich. Um wieder zum Default-Rollout-Wizard zurückzukehren, müssen Sie den benutzerdefinierten Rollout-Assistenten aus dem Dateisystem des Gerätes löschen.

2.16.1 Default-Rollout-Assistent

Ihr Gerät beinhaltet standardmäßig einen vorkonfigurierten Rollout-Assistenten, welcher es Ihnen ermöglicht, mit wenigen Klicks von einem *Large Scale Rollout & Management (LSR)*-Server eine Konfigurationen zu beziehen. Dieser **Default-Rollout-Assistent** erscheint immer dann, wenn Sie den Rollout-Assistenten im HiLCOS aktiviert und keinen benutzerdefinierten Rollout-Assistenten eingerichtet haben.

Beim Aufruf des Default-Rollout-Assistenten fragt der Assistent alle Informationen ab, die er für einen erfolgreichen Verbindungsaufbau zum LSR benötigt. Hierzu gehören:

- das für den Verbindungsaufbau verwendete Protokoll (HTTP oder HTTPS);
- die IP-Adresse oder den DNS-Namen des LSR-Servers;
- den Benutzernamen und das Passwort für die Authentisierung am LSR;
- der Name oder die Nummer des Rollout-Projektes;
- die Geräte-ID (optional); sowie
- die zum Gerät gehörende Rollout-TAN.

Tipp: Dieser Prozess lässt sich auch teilweise bis vollständig automatisieren, indem Sie die betreffenden Angaben dauerhaft im Gerät hinterlegen. Die dazugehörige Tabelle finden Sie im Setup-Menü unter **HTTP** > **Rollout-Wizard** > **Vorbelegungen**. Standardmäßige Vorbelegungen sind der vom Assistenten verwendete Port sowie die Loopback-Adresse.

Tipp: Sofern Ihr Gerät über einen USB-Anschluss verfügt, lässt sich dessen automatische Ladefunktion auch dafür nutzen, um ein beliebiges unkonfiguriertes Gerät per USB-Stick mit den relevanten Basisinformationen für den Rollout-Wizard zu versorgen. Mehr Informationen zu der Funktion erhalten Sie unter *Automatisches Laden von Firmware oder Konfiguration über USB* auf Seite 129.

Bevor das Gerät mit dem Rollout-Vorgang beginnt, zeigt Ihnen der Assistent die verwendeten Verbindungsdaten in einer Zusammenfassung noch einmal an. Außerdem überprüft das Gerät mit einem ICMP Echo Request (Ping), ob der angegebene Server erreichbar ist. Schlägt diese Prüfung fehl, haben Sie die Möglichkeit, den Assistenten neu zu konfigurieren oder den Rollout-Vorgang trotzdem fortzusetzen. Ist der angegebene Host erreichbar, beginnt das Gerät im weiteren Verlauf damit, seine Zielkonfiguration beim LSR abzufragen.

Wichtig: Sofern der LSR-Server über das Internet erreichbar ist, Sie den Rollout-Wizard aber auf einem Gerät ausführen, auf dem noch keine Internet-Verbindung eingerichtet ist, müssen Sie zunächst den Einrichtungsassistenten für das Internet durchlaufen.

2.16.2 Benutzerdefinierter Rollout-Assistent

Der benutzerdefinierte Rollout-Assistent ist ein individuell programmierbarer Setup-Assistent in WEBconfig, der es Ihnen als ausrollender Administrator

erlaubt, einen auf Ihre Kunden oder andere (z. B. beschränkte) Administratoren abgestimmten Konfigurationsassistenten zu implementieren. Dazu bedienen Sie sich einer speziellen Beschreibungssprache, mit der sich auch sehr komplexe Assistenten definieren lassen.

Ein solcher benutzerdefinierter Assistent unterstützt folgende Funktionen:

- Definition von beliebigen internen Variablen
- Bedingte Verzweigungen
- Bedingte Sprunganweisungen zu beliebigen URL
- Bedingte Anzeige von Hinweisen
- Ausführen von allen (nicht interaktiven) Aktionen, die in der HiLCOS-Kommandozeile zur Verfügung stehen
- Auslesen von aktuellen Werten aus der Konfiguration des Gerätes
- Schreiben von neuen Werten in die Konfiguration des Gerätes
- Statusprüfungen, wie z. B. Prüfen der Uhrzeit im Gerät
- Verbindungsprüfungen, wie z. B. die erfolgreiche VPN-Verbindung zu einer bestimmten Gegenstelle

Sie erstellen den neuen Assistenten nach den Regeln der Beschreibungssprache in Form einer Text-Datei, die Sie anschließend in das Gerät laden. Der Anwender am Einsatzort kann den benutzerdefinierten Assistenten dann unter WEBconfig über den gewählten Namen ausführen.

Tipp: Sie können bestimmte Administrator-Accounts gezielt auf die Ausführung des Rollout-Assistenten beschränken und so auch ungeübten Anwendern die Konfiguration bestimmter Funktionen ermöglichen, ohne einen kompletten Konfigurationszugriff zu erlauben.

Struktur des benutzerdefinierten Assistenten

Die Beschreibung eines benutzerdefinierten Assistenten besteht aus den folgenden Abschnitten:

- String-Tabellen mit den benötigten Texten in Deutsch und Englisch.
- Eine Definition des Assistenten.
- Beliebig viele Sektionen zur Beschreibung der einzelnen HTML-Seiten, die der Assistent anzeigen kann.

- Ein Initialisierungs-Bereich, der die Aktionen beim Starten des Assistenten definiert.
- Ein abschließender Bereich, der die Aktionen beim Beenden des Assistenten definiert.

Beachten Sie für die Beschreibung des Assistenten die folgenden Konventionen:

- Die Elemente der Beschreibung folgen genau der oben genannten Struktur.
- Die Textdatei mit der Beschreibung ist nach ISO 8859-1 kodiert.
- Kommentare beginnen mit einem Semikolon und dienen nur der Lesbarkeit der Beschreibung.
- Interne Variablen beginnen mit dem Schlüsselwort `wizard.` (inklusive des Punktes) und speichern Informationen für die interne Vearbeitung des Assistenten.
- Konfigurationsvariablen beginnen mit dem Schlüsselwort `config.` (inklusive des Punktes) und lesen Informationen aus der aktuellen Gerätekonfiguration aus oder schreiben Werte in die aktuelle Konfiguration hinein. Geben Sie die Konfigurationsvariablen in einer der folgenden Schreibweisen an:
  - Dedizierte Parameter der Konfiguration referenzieren Sie über `config.1.<SNMP-ID>`, also z. B. `config.1.2.1` für den Zugriff auf den Namen des Gerätes (auf der Konsole unter **Setup** > **Name**).

    Tipp: Die SNMP-ID zu einem Parameter der Konfiguration ermitteln Sie z. B. mit dem Befehl `ls -a` an der Kommandozeile in dem entsprechenden Untermenü.

  - Die Werte in einer Tabelle referenzieren Sie über:

    ```
    config.1.<SNMP-ID>.<Zeile>.ID:<Spalte>
    ```

    Beispiel für den Wert in der ersten Zeile und der Spalte mit der ID '2' in der Routing-Tabelle '1.2.8.2':

    ```
    config.1.2.8.2.1.ID:2
    ```

– Wenn Ihnen die ID der Spalte nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle alternativ über:

```
config.1.<SNMP-ID>.<Zeile>.<Spalte>
```

Beispiel für den Wert in der ersten Zeile und der zweiten Spalte:

```
config.1.2.8.2.1.2
```

– Wenn Ihnen die benötigte Zeile der Tabelle nicht bekannt ist, referenzieren Sie die Werte in einer Tabelle über einen bekannten Wert in der ersten Spalte mit:

```
config.<SNMP-ID>."<Bekannter-Wert>".ID:<Spalte>
```

Beispiel für den Wert der Spalte mit der ID '2' von genau der Zeile, die in der ersten Spalte den Wert der Default-Route enthält:

```
config.1.2.8.2."255.255.255.0".ID:2
```

Enthält die Tabelle mehrere Zeilen mit dem gleichen Wert in der ersten Spalte, referenziert die Konfigurationsvariable die erste dieser Zeilen.

– Wenn die benötigte Zeile der Tabelle erst bei der Ausführung des Assistenten durch eine Benutzereingabe definiert wird, referenzieren Sie die Wert in der Tabelle über die Verwendung einer Variablen mit:

```
config.<SNMP-ID>.\"<Interne-Variable>\".ID:<Spalte>
```

Beispiel für die Zeile, deren Wert in der ersten Spalte mit dem aktuellen Wert der internen Variablen wizard.target_network übereinstimmt:

```
config.1.2.8.2."\wizard.target_network"\.ID:2
```

▶ Geräte-Variablen für Geräteeigenschaften beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes) und lesen bestimmte Geräteeigenschaften aus dem Gerät aus. Weitere Informationen über die Geräte-Variablen finden Sie im Abschnitt *Geräte-Variablen für Geräteeigenschaften* auf Seite 182.

String-Tabellen

Die Beschreibung des benutzerdefinierten Assistenten basiert auf der Definition der zur Anzeige benötigten Texte in deutscher und englischer Sprache.

Die Zeile `stringtable "English"` leitet die englischen Texte ein, die Zeile `stringtable "Deutsch"` die deutschen Texte. Jede String-Definition besteht aus dem Schlüsselwort `string`, gefolgt vom Namen des Strings und dem in doppelte Hochkommata gesetzen Wert.

Das folgende Beispiel zeigt die String-Tabellen mit nur einem Eintrag:

```
; -String tables start-----------------------------------------------
   stringtable "English"
   string title_test, "Test wizard"
   stringtable "Deutsch"
   string title_test, "Test-Assistent"
; -String tables end-------------------------------------------------
```

Wichtig: Der Interpreter für die Beschreibung des benutzerdefinierten Assistenten im HiLCOS erwartet alle Texte zwingend mit einer deutschen und einer englischen Definition. HiLCOS führt den Assistenten nicht aus, wenn zu einem Eintrag in der englischen String-Tabelle kein gleichnamiger Eintrag in der deutschen String-Tabelle gefunden wird (oder umgekehrt).

Definition des Assistenten

Die Definition legt den Namen des Assistenten fest. Nach dem Schlüsselwort `wizard` folgt der interne Name in doppelten Hochkommata, gefolgt von der Referenz auf einen Eintrag der String-Tabelle (*String-Tabellen*). Der Assistent zeigt den mit diesem String definierten externen Namen bei der Ausführung in der HTML-Seite an:

```
; -Assistenenten-Definition Start---------------------------
   wizard "Mein_Test-Assistent", title_test
; -Assistenenten-Definition Ende----------------------------
```

Sektionen

Die Sektionen stellen die eigentlichen HTML-Seiten dar, die der Anwender während der Ausführung des Assistenten im Browser angezeigt bekommt.

Jede Sektion beginnt mit dem Schlüsselwort `section` und endet mit dem Beginn der nächsten Sektion. Die letzte Sektion endet mit dem Beginn des Bereiches `on-init`; die Sektionen enden also ohne ein explizites Schlüsselwort für das Ende.

Die Sektionen beinhalten die folgenden Elemente in beliebieger Reihenfolge und Menge:

- Bedingungen
- Optional: Eigene Bezeichnung für die Sektion, beginnend mit dem Schlüsselwort `label`, gefolgt von einer Zeichenkette aus Groß- und Kleinbuchstaben und dem Unterstrich ('_'):

```
Label Mein_RolloutAssistent
```

  Tipp: Die Beschreibung des Assistenten kann die eigene Bezeichnung (das Label) als Sprungziel nutzen.

- Statischer Text, beginnend mit dem Schlüsselwort `static_text`, gefolgt von einer Referenz auf einen Eintrag der *String-Tabelle*:

```
static_text str.conf_general
```

- Felder für verschiedene Datentypen wie Text oder IP-Adresse: Eingabefelder, Kontrollkästchen, Optionsfelder, Auswahllisten etc.

  Hinweis: Hinweise zu den verfügbaren Feldern finden Sie im Abschnitt *Felder und Attribute* auf Seite 176.

- Aktionen, die der Assistent je nach Schlüsselwort zu Beginn des Blocks in unterschiedlichen Situationen ausführt:
  - `on_show`: Der Assistent führt die Aktionen in diesem Block aus, bevor eine Sektion (HTML-Seite) angezeigt wird.

- `on_skip:` Der Assistent führt die Aktionen in diesem Block aus, wenn eine Sektion (HTML-Seite) aufgrund der darin enthaltenen Bedingungen nicht angezeigt wird.
- `on_next`: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche **Weiter** in der Sektion (HTML-Seite) klickt.
- `on_back`: Der Assistent führt die Aktionen in diesem Block aus, wenn der Benutzer die Schaltfläche **Zurück** in der Sektion (HTML-Seite) klickt.

Hinweis: Hinweise zum Aufbau der Blöcke mit den Aktionen und den darin verfügbaren Elementen finden Sie im Abschnitt *Aktionen* auf Seite 184.

Bedingungen

Die Beschreibung des Assistenten kann alle Elemente einer Sektion mit Bedingungen versehen. Über eine Bedingung lässt sich die ausgegebene HTML-Seite kontextabhängig verändern, indem bestimmte Konfigurationsmöglichkeiten in Abhängigkeit der zuvor getätigten Einstellungen ein- oder ausgeblendet werden.

Die Bedingungen beziehen sich dabei immer auf das vorhergehende Element und bestehen aus der Angabe einer Klasse und einem oder mehreren Bedingungsmustern. Ein Muster wiederum besteht aus zwei Operanden und einem Operator. Hierbei gilt:

- Wenn eine Bedingung mehrere Bedingungsmuster in einer Zeile enthält, wertet der Assistent diesen Ausdruck als ODER-Verknüpfung.
- Wenn die Beschreibung mehrere Bedingungen in separaten Zeilen zu einem übergeordneten Element enthält, wertet der Assistent diesen Ausdruck als UND-Verknüpfung.

Eine Klasse darf beliebig viele Bedingungsmuster und ein Element beliebig viele Bedingungen enthalten. Die folgenden Bedingungen z. B. zeigen die Sektion nur dann an, wenn die interne Variable `wizard.test_select1`

gleich `1`, und `wizard.test_select4` oder `wizard.test_select5` gleich `0` sind:

```
section
only_if wizard.test_select1, "1", equal
only_if wizard.test_select4, "0", equal, wizard.test_select5, "0", equal
```

Klassen

Die Beschreibung kann die folgenden Klassen enthalten:

- `only-if`: Das vorhergehende Element wird nur ausgeführt oder angezeigt, wenn mindestens eines der folgenden Bedingungsmuster erfüllt ist.
- `skip-if`: Das vorhergehende Element wird nicht ausgeführt oder angezeigt, wenn alle der folgenden Bedingungsmuster erfüllt sind.

Operanden

Das Bedingungsmuster kann folgende Operanden enthalten:

- Statische Texte
- Interne Variablen des Assistenten
- Variablen zur Referenzierung von Werten aus der aktuellen Konfiguration des Gerätes (Konfigurations-Variablen)
- Das Zeichen '*' als Platzhalter (Wildcard)

Operatoren

Das Bedingungsmuster kann folgende Operatoren enthalten:

- `equal`: Prüft, ob die beiden Operanden gleich sind.
- `exists`: Prüft, ob die angegebene Konfigurations-Variable gesetzt ist, also der Wert des Parameters in der Konfiguration nicht leer ist.
- `empty`: Prüft, ob der erste Operand leer ist. Der zweite Operand wird als Platzhalter (Wildcard) '*' angegeben.
- `contains`: Prüft, ob der erste Operand den zweiten Operanden enthält.
- `!`: Verneint die Bedingung.

Beispiele

Die folgende Bedingung zeigt die Sektion nur dann an, wenn die interne Variable 'wizard.test_select' gleich '0' ist.

```
section
only_if wizard.test_select, "0", equal
```

Die folgende Bedingung setzt die interne Variable 'wizard.intranet_name' auf den Wert 'INTRANET', wenn diese Variable bisher leer ist.

```
set wizard.intranet_name, "INTRANET"
only_if wizard.intranet_name, *, empty
```

Die folgende Bedingung setzt die interne Variable 'wizard.target_1' auf den Wert 'ZIEL_1', wenn die interne Variable 'wizard.select_target' entweder den Wert '1' oder den Wert '5' hat.

```
set wizard.target_1,"ZIEL_1"
only_if wizard.select_target,"1",equal,wizard.select_target,"5",equal
```

Felder und Attribute

Der Assistent verwendet Felder, um dem Benutzer Informationen anzuzeigen und ihm die Möglichkeit zur Eingabe von Informationen zu geben. Jedes Feld entspricht einer internen Variablen.

Der Assistent definiert ein Feld durch die Angabe des entsprechenden Schlüsselwortes, gefolgt von einer internen Variablen in der gleichen Zeile. In weiteren Zeilen folgen optional die Attribute für das Feld.

Ein Beispiel für eine Felddefinition im Assistenten:

```
selection_buttons select_inet
 description   str.inet_Selection
 button_text   str.inet_PPPoE, str.inet_IPoE
```

Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Der Assistent setzt den in der String-Tabelle definierten Text `str.inet_Selection` als Beschreibung neben das Feld. Für die Optionsschaltflächen selbst zeigt der Assistent die Texte `str.inet_PPPoE` und `str.inet_IPoE` an. Nach der Auswahl einer Option

durch den Benutzer schreibt der Assistent den gewählten Wert in die interne Variable `wizard.select_inet`.

Folgende Felder können Sie im Assistenten verwenden:

`check_local_ip`

Dieses Feld prüft, ob der Assistent zuvor die IP-Adresse des Gerätes verändert hat und leitet den Benutzer auf die entsprechende HTML-Seite weiter. Mögliche Attribute:

- `destination`: Ziel für die Weiterleitung als FQDN oder IPv4-Adresse.
- `timeout`: Wartezeit vor der Weiterleitung.

`check_time`

Dieses Feld prüft, ob das Gerät über eine gültige Zeitinformation verfügt. Mögliche Attribute:

- `success_jump`: Label der Seite, die der Assistent bei erfolgreicher Prüfung öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreicher Prüfung öffnet.
- `limit`: Maximale Anzahl der Prüfungen, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Prüfungen ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Prüfungen.

`entryfield_hex`

Dieses Feld dient zur Eingabe von hexadezimalen Werten, z. B. MAC-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_ipaddress`

Dieses Feld dient zur Eingabe von IPv4-Adressen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `never_zero`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches nicht den Wert '0' enthalten darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numbers`

Dieses Feld dient zur Eingabe von Telefonnummern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

`entryfield_numeric`

Dieses Feld dient zur Eingabe von Zahlen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `range_min`: Minimaler Wert, den der Benutzer in dieses Feld eintragen kann
- `range_max`: Maximaler Wert, den der Benutzer in dieses Feld eintragen kann
- `signed_value`: Ermöglicht die Angabe eines numerischen Wertes mit Vorzeichen
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `default_value`: Standardwert

- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

`entryfield_text`

Dieses Feld dient zur Eingabe von Texten. Mit dem Attribut `hidden` dient das Feld zur Eingabe von Passwörtern. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `hidden`: Kennzeichnet ein Feld, in welches der Benutzer Kennwörter einträgt.
- `add_to_charset`: Fügt zusätzliche Zeichen zum standardmäßig verwendeten Eingabezeichensatz hinzu.
- `convert_to_upper`: Wandelt die Eingabe des Benutzers in Großbuchstaben um
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `min_len`: Minimale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `never_empty`: Der Wert '1' für dieses Attribut kennzeichnet ein Feld, welches der Benutzer nicht freilassen darf.
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld anzeigt.

`entryfield_textwithlist`

Dieses Feld dient zur Eingabe von Texten. Außerdem kann der Benutzer aus einer Reihe von vordefinierten Werten auswählen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `default_value`: Standardwert
- `max_len`: Maximale Anzahl der Zeichen, die der Benutzer in dieses Feld eintragen kann
- `item_value`: Liste mit vordefinierten Werten, die der Benutzer für dieses Feld auswählen kann

`onoff_switch`

Dieses Feld erzeugt ein einfaches Kontrollkästchen. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung

- `value_list`: Liste der beiden Werte, welche das Kontrollkästchen annehmen kann
- `default_selection`: Standardwert

`page_switch`

Dieses Feld erzeugt einen Link, über den der Benutzer zu einer von mehreren anderen HTML-Seiten des Assistenten wechseln kann. Mögliche Attribute:

- `page_description`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der möglichen Link-Ziele.
- `page_label`: Komma separierte Liste mit Seiten-Labels der möglichen Link-Ziele.
- `description`: Beschreibung des Feldes in der HTML-Darstellung

`ping_barrier`

Dieses Feld verzögert die weitere Ausführung des Assistenten, bis ein Ping zu dem verwendeten Ziel erfolgreich beantwortet wurde. Mögliche Attribute:

- `destination`: Zieladresse für den Ping.
- `loopback`: Loopback-Adresse, die der Ping anstelle der standardmäßigen Antwortadresse verwendet
- `success_jump`: Label der Seite, die der Assistent bei erfolgreichem Ping öffnet.
- `fail_jump`: Label der Seite, die der Assistent bei nicht erfolgreichem Ping öffnet.
- `limit`: Maximale Anzahl der Pings, bevor der Assistent die Prüfung als erfolglos ansieht. Setzen Sie das Limit auf den Wert '0', um die Pings ohne Limit fortzusetzen.
- `timeout`: Wartezeit zwischen zwei Pings.

`popup`

Dieses Feld öffnet die angegebene Zieladresse in einem Popup-Fenster.

Tipp: Die Zieladresse kann Variablen enthalten (siehe *Variablen* auf Seite 181).

readonly_text

Dieses Feld erzeugt ein Feld ohne Eingabemöglichkeit. Der Assistent kann diese Felder nutzen, um Text anzuzeigen. Mit dem Attribut `hidden` kann der Assistent interne Variablen definieren. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `unit`: Die Einheit des Wertes, welchen der Assistent in der HTML-Darstellung nach dem Eingabefeld
- `hidden`: Kennzeichnet ein verstecktes Feld.

selection_buttons

Dieses Feld erzeugt eine Gruppe von Optionsschaltflächen, von denen der Benutzer nur eine aktivieren kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `button_text`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Optionsschaltflächen.
- `button_value`: Komma separierte Liste mit Texte-Strings mit den Werten der einzelnen Optionsschaltflächen.

selection_list

Dieses Feld erzeugt eine Auswahlliste (Drop-Down-Liste), aus welcher der Benutzer einen Wert auswählen kann. Mögliche Attribute:

- `description`: Beschreibung des Feldes in der HTML-Darstellung
- `item_text`: Komma separierte Liste mit Texte-Strings oder Referenzen auf Strings zur Beschreibung der einzelnen Listeneinträge.
- `item_value`: Komma separierte Liste mit Texte-Strings mit den Werten der einzelnen Listeneinträge.
- `default_selection`: Standardwert

static_text

Dieses Feld erzeugt einen statischen Text auf der HTML-Seite, der als Referenz auf einen Text-String dem Feldnamen folgt.

Variablen

In einigen Attributen der Felder sind Variablen einsetzbar, um den Wert des Attributs durch eine andere Zeichenkette zu ersetzen oder mit einer zusätzli-

chen Zeichenkette zu ergänzen. Dabei haben Sie die Wahl zwischen den internen Variablen des benutzerdefinierten Assistenten und den vordefinierten Umgebungsvariablen der Konsole, welche Sie über besondere Platzhalter einfügen.

Einfügen von Assistenten-Variablen

Um eine interne Variable in den Wert eines Attributs einzusetzen, verwenden Sie die Syntax `$(VariablenName)`. Um den Benutzernamen aus der internen Variablen `wizard.username` in eine URL einzusetzen, fügen Sie z. B. das folgende Attribut ein: `http://host/directory?param=$(username)`.

Einfügen von Umgebungsvariablen

Um eine Umgebungsvariable in den Wert eines Attributs einzusetzen, verwenden Sie die Syntax `%VariablenName`. Folgende Umgebungsvariablen lassen sich in den Attributen verwenden:

- `%` fügt ein Prozentzeichen ein.
- `f` fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- `r` fügt die Hardware-Release des Gerätes ein.
- `v` fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- `m` fügt die MAC-Adresse des Gerätes ein.
- `s` fügt die Seriennummer des Gerätes ein.
- `n` fügt den Namen des Gerätes ein.
- `l` fügt den Standort des Gerätes ein.
- `d` fügt den Typ des Gerätes ein.

Geräte-Variablen für Geräteeigenschaften

In manchen Situationen soll ein Assistent Entscheidungen aufgrund der Geräteeigenschaften treffen. So soll der Assistent z. B. bestimmte Werte nur dann in die Konfiguration schreiben, wenn das jeweilige Gerät über eine bestimmte Art von WAN-Schnittstelle verfügt. Als Basis für diese Entscheidungen kann der Assistent mit bestimmten Variablen auf die Geräteeigenschaften zugreifen. Diese Variablen beginnen mit dem Schlüsselwort `device.` (inklusive des Punktes), gefolgt von dem Bezeichner der jeweiligen Eigenschaft. Der Assistent kann folgende Variablen für den lesenden Zugriff auf Geräteeigenschaften nutzen:

`device.flags.dhcp_addr`

Diese Variable gibt an, ob ein DHCP-Server dem Gerät eine IP-Adresse zugewiesen hat (in diesem Fall hat die Variable den Wert '128') oder nicht ('0').

`device.hasADSL`

Diese Variable gibt an, ob das Gerät über eine ADSL-Schnittstelle verfügt ('1') oder nicht ('0').

`device.hasISDN`

Diese Variable gibt an, ob das Gerät über eine ISDN-Schnittstelle verfügt ('1') oder nicht ('0').

`device.FirmwareVersion`

Diese Variable gibt die aktuelle Firmware-Version des Gerätes an.

`device.HardwareRelease`

Diese Variable gibt die Hardware-Release des Gerätes an.

`device.LoaderVersion`

Diese Variable gibt die aktuelle Loader-Version des Gerätes an.

`device.MacAddress`

Diese Variable gibt die MAC-Adresse des Gerätes in hexadezimaler Schreibweise ohne Trennzeichen an.

`device.SerialNumber`

Diese Variable gibt die Seriennummer des Gerätes an.

`device.Location`

Diese Variable gibt den Standort des Gerätes an, wie er im Setup-Menü unter **SNMP** > **Standort** eingetragen ist.

`device.DeviceString`

Diese Variable gibt den Typ des Gerätes an.

`device.Name`

Diese Variable gibt den Namen des Gerätes an, wie er im Setup-Menü unter **Name** eingetragen ist.

Aktionen

Der Assistent verwendet die Aktionen, um Werte in der Konfiguration der Geräte zu verändern. Für jede Aktion können Sie eine oder mehrere Bedingungen definieren, bei deren Eintreffen der Assistent die Aktion ausführt.

set

Diese Aktion ersetzt den Inhalt der Ziel-Variable durch die angegebene Quelle. Die Quelle enthält in Form einer Komma separierten Liste entweder Variablen oder Text-Strings.

```
set $target, $sourcelist
```

Wenn es sich bei der Ziel-Variablen um einen einzelnen Konfigurationsparameter handelt, geben Sie als Quelle nur einen Wert an, weitere Werte werden ansonsten ignoriert.

Wenn es sich bei der Ziel-Variablen um eine Tabelle handelt, geben Sie in der Quelle zuerst den Wert aus der Zeile an, die der Assistent ändern soll. Der Assistent durchsucht die erste Indexspalte nach diesem Wert und ändert die erste Zeile, in der er diesen Wert findet. Findet der Assistent keine passende Zeile mit diesem Wert, fügt er eine neue Zeile in die Tabelle ein.

Wenn es sich bei der Ziel-Variablen um einen numerischen Wert handelt, können Sie mit Hilfe der `add`- oder `sub`-Aktion den als `$number` definierten Betrag addieren oder subtrahieren.

```
set $target, $number, add
```

```
set $target, $number, sub
```

Beispiele

Die folgende Aktion setzt die Default-Route auf die gewünschten Werte:

```
set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0", "on",
 "Yes", ""
```

Die folgende Aktion erhöht den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", add
```

Die folgende Aktion reduziert den Wert der ARP-Aging-Minuten um '5':

```
set config.1.2.7.11, "5", sub
```

del

Diese Aktion löscht den Inhalt der Ziel-Variable. Wenn es sich bei dieser Variablen um eine Tabelle handelt, geben Sie den Wert der ersten Indexspalte aus der zu löschenden Zeile an.

Beispiel

Die folgende Aktion löscht die Default-Route aus der Routing-Tabelle:

```
del config.1.2.8.2, "255.255.255.0"
```

cat

Diese Aktion hängt den Inhalt der Quell-Variablen an die Ziel-Variable an.

Beispiel

Die folgende Aktion fügt den Inhalt der Variablen `wizard.user` und die Variable `wizard.name` an:

```
cat wizard.name, wizard.user
```

cut

Diese Aktion löscht eine bestimmte Anzahl von Zeichen aus der Ziel-Variablen. Geben Sie die Position der zu löschenden Stelle von links gesehen sowie optional die Anzahl der zu löschenden Zeichen als Parameter an.

Beispiele

Die folgende Aktion löscht in der Variablen `wizard.name` alle Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2
```

Die folgende Aktion löscht in der Variablen `wizard.name` genau 4 Zeichen nach dem 2. Zeichen.

```
cut wizard.name, 2, 4
```

trigger_config_change

Änderungen der Konfiguration durch den Wizard sind je nach Teil der Firmware nicht sofort wirksam, da einige Module interne Strukturen für die Konfiguration verwenden.

Die Aktion `trigger_config_change` löst eine Aktualisierung dieser internen Strukturen aus. Setzen Sie diese Aktion in einer Sektion ein, wenn Sie beim Wechsel einer Seite im Rollout-Assistenten sichergehen möchten, dass die Konfiguration aktualisiert wurde.

Hinweis: Beim Beenden führt der Assistent diese Aktion automatisch aus.

exec

Der auf diesen Aktionsbefehl folgende String führt das Gerät als Befehl auf der Konsole aus. Dabei ist auch die Nutzung von Variablen im String möglich, z. B. um ein `LoadScript` zu starten.

Trace für Rollout-Assistenten (Debugging)

Die HTML-Seiten des Assistenten zeigen nur das jeweilige Ergebnis einer internen Verarbeitung an. Während der Entwicklung eines Assistenten kann der Trace zum Assistenten dem Administrator zusätzliche Informationen z. B. über die Auswertung der einzelnen Bedingungen liefern, die er für die weitere Optimierung nutzt.

Den Trace des Rollout-Assistenten starten Sie an der Konsole mit dem Befehl `trace + Rollout-Wizard`.

Benutzerdefiniertes HTML-Template nutzen

Zur Anpassung des Assistenten an die Gestaltungsrichtlinien Ihres Unternehmens haben Sie optional die Möglichkeit, ein benutzerdefiniertes HTML-Template in das Gerät zu laden. In diesem Template legen Sie den grundlegenden Aufbau der HTML-Seiten und die Gestaltung von Farben, Schriften etc. über CSS-Regeln fest.

Der Assistent verwendet im HTML-Template folgende Platzhalter, um die Inhalte des Assistenten in die jeweiligen HTML-Seiten einzufügen:

- `<WIZARD_LOGO>`: An dieser Stelle setzt der Assistent das Logo ein, welches Sie im Format GIF, JPEG oder PNG in das Gerät geladen haben.
- `<WIZARD_CONTENT>`: An dieser Stelle setzt der Assistent den Inhalt der Sektionen in Form einer zweispaltigen Tabelle mit den zugehörigen Schaltflächen ein.

Ein sehr einfaches Beispiel für ein HTML-Template sieht folgendermaßen aus:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
    <head>
        <title>Titel des Assistenten</title>
        <meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1">
    </head>
    <body>
        <div>
            <WIZARD_LOGO>
        </div>
        <WIZARD_CONTENT>
    </body>
</html>
```

Der Assistent verwendet einige vordefinierte CSS-Klassen, die Sie durch die Angabe von entsprechenden Werte in Ihrem HTML-Template einfach anpassen können, u. a.:

- `class="header"`: Die CSS-Klasse für den Kopfbereich mit dem Logo.
- `class="wizardName"`: Die CSS-Klasse Absatz mit dem Namen des Assistenten im Kopfbereich.
- `class="headerLogo"`: Die CSS-Klasse für den Bereich des Logos im Kopfbereich.
- `class="wizardTable"`: Die CSS-Klasse für Tabelle mit den angezeigten Feldern.
- `class="footer"`: Die CSS-Klasse für den Fußbereich mit den Schaltflächen.

Dateien für den Assistenten hochladen

Um den Assistenen verfügbar zu machen, laden Sie z. B. über LANconfig oder WEBconfig die folgenden Dateien in das Gerät:

- **Rollout-Assistent (einfacher Text)**: Die Beschreibung des Assistenten (erforderlich). Diese ISO-8859-1-kodierte Text-Datei ist für den Betrieb des Assistenten notwendig und in der Größe nicht beschränkt.
- **Rollout-Assistent - Template (*.html, *.htm)**: Ein HTML-Template für den Assistenten (optional). Mit diesem Template steuern Sie die Darstellung der Sektionen in den HTML-Seiten des Assistenten im Browser des Anwenders. In diesem Template können Sie u. a. eigene CSS-Informationen zur Definition des Layouts verwenden. Wenn Sie kein eigenes HTML-Template in das Gerät laden, verwendet der Assistent ein vordefiniertes Template.
- **Rollout-Assistent - Logo (*.gif, *.png, *.jpeg)**: Das Logo Ihres Unternehmens (optional). Der Assistent setzt diese Bilddatei an der Stelle des Markers <WIZARD_LOGO> im HTML-Template ein.Wenn Sie kein eigenes Logo in das Gerät laden, verwendet der Assistent ein vordefiniertes Logo.

Dateien des Assistenten aus dem Gerät entfernen

Um die Dateien des Assistenen aus dem Gerät zu entfernen, haben Sie mehrere Möglichkeiten: Entweder Sie löschen die betreffenden Dateien gezielt aus dem Dateisystem Ihres Gerätes oder Sie verwenden dazu an der Konsole den Befehl `rollout` mit den entsprechenden Parametern.

Löschen über den rollout-Befehl

Die Löschfunktion des `rollout`-Befehls besitzt die folgende Syntax:

```
rollout (-r|-remove) <RelatedFile>
```

Mögliche Dateien sind:

- `wizard`: Löscht den Assistenten
- `template`: Löscht das Template
- `logo`: Löscht das Logo
- `alle`: Löscht den Assistenten, das Template und das Logo

Löschen über das Dateisystem

Im Dateisystem löschen Sie die Dateien des Assistenten über die analog lautenden Mountingpoints:

- **rollout_wizard**
- **rollout_template**
- **rollout_logo**

Beispiel für einen benutzerdefinierten Rollout-Assistenten

Dieses Kapitel stellt ein Programmierungsbeispiel für einen benutzerdefinierten Rollout-Assistenten vor. Der Assistent ermöglicht die Einrichtung eines Internet-Zugangs.

Im ersten Abschnitt definiert der Assistent die Texte, die das Gerät auf den verschiedenen HTML-Seiten anzeigt.

```
stringtable "Deutsch"
 string title_MyCompany,   "MyCompany Rollout"
 string txt_Welcome,       "Willkommen beim MyCompany Rollout Assistenten"
 string dev_serial_number, "Seriennummer"
 string dev_type,          "Gerätetyp"
 ;---Seite: Auswahl der Internetverbindung
 string inet_Selection,    "Typ der Internetverbindung"
 string inet_PPPoE,        "PPPoE"
 string inet_IPoE,         "IPoE"
 ;---Seite: IPoE
```

```
 string inet_ipoe,         "Bitte geben Sie die Details für die Verbindung
ein."
 string con_ipaddress,     "IP-Adresse"
 string con_subnet,        "Netzmaske"
 string con_gateway,       "Gateway"
 string con_dns,           "DNS"
 ;---Seite: PPPoE
 string inet_pppoe,        "Bitte geben sie Benutzername und Kennwort ein."

 string con_username,      "Benutzername"
 string con_password,      "Passwort"
 ;---Seite: Ende
 string ende,              "Die Konfiguration wird nun abgeschlossen."
```

Die erste Zeile des nächsten Abschnitts leitet den Assistenten mit dem Namen 'MyCompany Rollout' ein. Das Gerät zeigt den Text-String `str.title_MyCompany` als Titel in den HTML-Seiten an.

Danach definiert der Assistent die Sektionen, also die benötigten HTML-Seiten.

Die Sektion 'Start' zeigt zunächst einen statischen Text zur Begrüßung an. Darunter zeigt der Assistent in zwei Read-Only-Feldern den Gerätetyp und die Seriennummer an. Der Assistent liest diese beiden Werte beim Öffnen der Seite über den Bereich `on_show` aus dem Gerät aus. In einer Optionsliste bietet der Assistent dem Benutzer die Auswahl für einen Internetzugang über 'PPPoE' oder 'IPoE' an. Da keine Werte für die Optionsfelder definiert sind, setzt der Assistent die Variable `select_inet` je nach Auswahl des Benutzers für PPPoE auf '0' und für IPoE auf '1'.

```
wizard "MyCompany Rollout", str.title_MyCompany

section ;---Start---
 static_text    str.txt_Welcome

 readonly_text device_string
  description   str.dev_type
 readonly_text device_serial_number
  description   str.dev_serial_number

 selection_buttons select_inet
  description   str.inet_Selection
  button_text   str.inet_PPPoE, str.inet_IPoE

 on_show
```

```
  set wizard.device_string, device.DeviceString
  set wizard.device_serial_number, device.SerialNumber

 on_next
```

Der Assistent zeigt die Sektion IPoE nur dann an, wenn die Variable select_inet den Wert '1' hat.

Auf dieser Seite fragt der Assistent vom Benutzer die Werte für die IP-Adresse, die Netzmaske, das Gateway und den DNS-Server ab. Alle Felder sind für die Ausführung des Assistenten notwendig.

```
section ;---IPoE---
 only_if wizard.select_inet, "1", equal

 static_text   str.inet_ipoe

 entryfield_ipaddress inet_ipaddress
  description  str.con_ipaddress
  never_empty  1
 entryfield_ipaddress inet_subnet
  description  str.con_subnet
  never_empty  1
 entryfield_ipaddress inet_gateway
  description  str.con_gateway
  never_empty  1
 entryfield_ipaddress inet_dns
  description  str.con_dns
  never_empty  1
```

Der Assistent zeigt die Sektion PPPoE nur dann an, wenn die Variable select_inet den Wert '0' hat.

Auf dieser Seite fragt der Assistent vom Benutzer den Benutzernamen und das Passwort mit einer Länge von jeweils maximal 30 Zeichen ab.

```
section ;---PPPoE---
 only_if wizard.select_inet, "0", equal

 static_text   str.inet_pppoe

 entryfield_text inet_username
  description  str.con_username
  max_len   30
```

```
 entryfield_text inet_password
  description  str.con_password
  max_len   30
```

Auf der letzten Seite zeigt der Assistent zunächst einen zusammenfassenden, statischen Text an. Folgende Aktionen führt der Assistent beim Fertigstellen des Assistenten aus:

- Wenn der Benutzer 'IPoE' ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der Liste der IP-Parameter an.
- Wenn der Benutzer 'PPPoE' ausgewählt hat, legt der Assistent eine passende Gegenstelle und einen Eintrag in der PPP-Liste an.
- Unabhängig von der Auswahl legt der Assistent eine Default-Route an, die den Router 'INTERNET' verwendet.

```
section ;---ende---
 static_text   str.ende

on_init  ;---Befehle, die bei der Initialisierung des Wizards durchgeführt
werden.---

on_apply ;---Befehle, die bei der Fertigstellung des Wizards durchgeführt
werden.---

 ;---Wenn IPoE ausgewählt wurde, werden die entsprechenden Daten nun
eingetragen.
 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "IPOE", "0", "000000000000"

  only_if wizard.select_inet, "1", equal
 ;---IP-Parameter
 set config.1.2.2.20, "INTERNET", wizard.inet_ipaddress, wizard.inet_subnet,
 "0.0.0.0", wizard.inet_gateway, wizard.inet_dns, "0.0.0.0", "0.0.0.0",
"0.0.0.0"
  only_if wizard.select_inet, "1", equal

 ;---Wenn PPPoE ausgewählt wurde, werden die entsprechenden Daten eingetragen.

 ;---Gegenstelle
 set config.1.2.2.19, "INTERNET", "9999", "", "", "PPPOE", "0", "000000000000"

  only_if wizard.select_inet, "0", equal
 ;---PPP-Liste
 set config.1.2.2.5, "INTERNET", "none", "60", wizard.inet_password, "5",
```

```
"5", "10", "5", "2", wizard.inet_username, "1"
  only_if wizard.select_inet, "0", equal

 ;---Setzen der Default Route.
 set config.1.2.8.2, "255.255.255.255", "0.0.0.0", "0", "INTERNET", "0",
"on", "Yes", ""
```

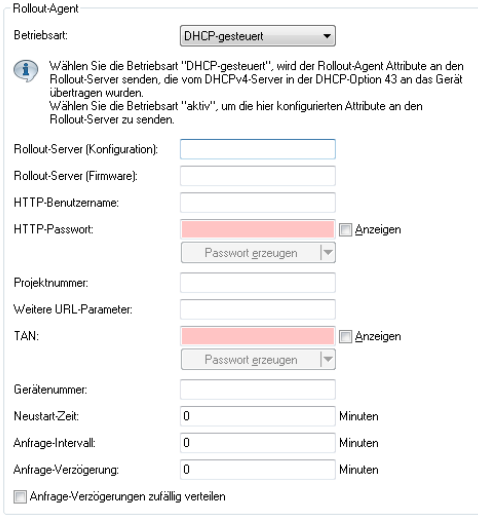
2.16.3 Aktivierung des Rollout-Assistenten im WEBconfig

Um den Rollout-Assistenen allgemein verfügbar zu machen, setzen Sie im Setup-Menü den Parameter **HTTP** > **Rollout-Wizard** > **In-Betrieb** auf **ja**. Dies aktiviert zunächst den Default-Rollout-Wizard. Im WEBconfig erscheint dann unter **Setup-Wizards** ein neuer Assistent mit dem unter **HTTP** > **Rollout-Wizard** > **Titel** vergebenen Namen.

Um ihn anschließend durch einen benutzerdefinierten Rollout-Assistenten zu ersetzen, laden Sie die Beschreibung des Assistenten in das Gerät (siehe hierzu *Dateien für den Assistenten hochladen* auf Seite 188).

2.16.4 Konfiguration mit LANconfig

Mit LANconfig konfigurieren Sie den Rollout-Agent über **Management** > **Rollout-Agent**.



Betriebsart

Wählen Sie die Betriebsart “DHCP-gesteuert”, wenn der Rollout-Agent des Gerätes die Attribute an den Rollout-Server übertragen soll, die er zuvor über die Vendor-spezifische DHCP-Option 43 vom DHCP-Server erhalten hat. In der Betriebsart “Aktiv” überträgt das Gerät die in diesem Dialog konfigurierten Attribute (z. B., wenn im Netzwerk kein DHCP verfügbar ist). Die Betriebsart “Aus” deaktiviert den Rollout-Agenten.

Hinweis: Die Betriebsart “DHCP-gesteuert” überschreibt manuell konfigurierte Attribute nicht. Somit ist eine umfangreiche Vorkonfiguration möglich, bei der das Gerät z. B. nur die vom DHCP-Server übertragene aktuelle Kontaktinformation des Rollout-Servers verwendet (Adresse, Login-Daten).

Rollout-Server (Konfiguration)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Konfiguration zuständig ist.

Hinweis: Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

Rollout-Server (Firmware)

Mit diesem Eintrag definieren Sie die Adresse des Rollout-Servers, der für das Rollout der Firmware zuständig ist.

Hinweis: Ein Eintrag ist in folgenden Formen möglich:

- IP-Adresse (HTTP, HTTPS, TFTP)
- FQDN

HTTP-Benutzername

Legen Sie mit diesem Eintrag den Benutzernamen fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

HTTP-Passwort

Legen Sie mit diesem Eintrag das Benutzerpasswort fest, mit dem sich der Rollout-Agent am Rollout-Server anmeldet.

Projektnummer

Bestimmen Sie mit diesem Eintrag die Rollout-Projektnummer für den Rollout-Agenten.

Weitere URL-Parameter

Legen Sie mit diesem Eintrag weitere Parameter fest, die der Rollout-Agent zum Rollout-Server übertragen soll.

TAN

Legen Sie mit diesem Eintrag die Rollout-TAN fest.

Gerätenummer

Enthält die Gerätenummer des Gerätes, auf dem der Rollout-Agent ausgeführt wird.

Neustart-Zeit

Legen Sie hier die Zeit für einen Neustart des Gerätes nach einem Rollout fest.

Anfrage-Intervall

Legen Sie hier die Zeit in Sekunden für eine erneute Anforderung für ein Konfigurations-Rollout fest, nachdem eine Konfiguration gescheitert ist.

Hinweis: Bei einem Wert “0” startet der erneute Versuch in 1 Minute.

Anfrage-Verzögerung

Dieser Eintrag enthält die Verzögerungszeit für einen Rollout-Request in Sekunden.

Anfrage-Verzögerung zufällig verteilen

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt. Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern.

2.16.5 LSR-Informationen über DHCP-Server erhalten (Zero-Touch-Rollout)

Ein unkonfiguriertes OpenBAT-Gerät startet mit einem aktivierten DHCP-Client und bezieht dadurch IP-Adresse, Netzmaske, DNS-Adresse und Gateway-Adresse vom DHCP-Server im Netzwerk.

Über die Vendor-spezifische DHCP-Option 43 sendet ein entsprechend konfigurierter DHCP-Server u. a. auch Informationen darüber, wie ein LSR-Server (Large Scale Rollout) zu erreichen ist. Der Rollout-Agent des OpenBAT-Gerätes wertet diese Informationen aus, kontaktiert den LSR-Server und bezieht anschließend im Rahmen der bestehenden Rollout-Strategie seine Konfiguration oder aktualisiert seine Firmware.

Diese Funktion erleichtert den Rollout-Prozess, da keine Vorkonfiguration der Geräte mehr notwendig ist.

Die Verbindung zum LSR-Server erfolgt über HTTP, HTTPS oder TFTP, wobei im OpenBAT-Gerät für eine sichere Verbindung ein entsprechendes SSL-Zertifikat gespeichert sein muss.

Eine (auch partielle) Vorkonfiguration des Rollout-Agents ist ebenfalls möglich. So kann z. B. die vom DHCP-Server gesendete Rollout-Server-URL übernommen, eine Projektnummer im Gerät allerdings vorkonfiguriert werden.

Konfiguration des Zero-Touch-Rollouts

Ausgangslage

In einem Filial-Rollout ist es auf Grund der hohen Zahl an Geräten erforderlich, die OpenBAT-Geräte nicht vorkonfigurieren zu müssen. Sie sollen stattdessen in Betrieb gehen, nachdem sie die Konfiguration von einem zentralen LSR-Server erhalten haben, vergleichbar dem “Zero-Touch-Management” bei einem WLC.

Rahmenbedingungen

Damit dieser “Zero-Touch-Rollout” über den Rollout-Agenten des Gerätes funktioniert, sind einige Rahmenbedingungen zu erfüllen:

- Es muss ein zentraler Rollout-Server verfügbar und für die Zero-Touch-Geräte über HTTP/HTTPS erreichbar sein.

- Im Filial-Netz muss DHCP aktiv sein. D. h.,
  - ein filialnetz-eigener DHCP-Server ist erreichbar oder
  - ein DHCP-Relay-Server im Filialnetz vermittelt die DHCP-Datenpakete zwischen den Geräten im Filialnetz und einem DHCP-Server in der Zentrale.
- Der DHCP-Server muss die DHCP-Option 43 ausliefern können.

Wichtig: Der DHCP-Server überträgt sensitive Daten wie z. B. das Rollout-Passwort ungesichert als DHCP-Nachricht. Es ist also darauf zu achten, die Daten nur über entsprechend abgesicherte Verbindungen zu transportieren.

Ablauf

Der Konfigurations-Rollout läuft wie folgt ab:

1. Das unkonfigurierte Gerät wird an das Filial-Netz angeschlossen.
2. Über den DHCP-Server bezieht das Gerät die erforderlichen Verbindungsdaten wie IP-Adresse, Gateway, Netzmaske, DNS-Adresse und die DHCP-Option 43.
3. Aus der DHCP-Option 43 dekodiert das Gerät die URL des Rollout-Servers sowie zusätzliche Informationen und konfiguriert damit den Rollout-Agenten des Gerätes.
4. Der Rollout-Agent kontaktiert daraufhin den Rollout-Server und führt den Rollout nacheinander in zwei Schritten durch:
   - Firmware-Update
   - Konfigurations-Update

Der Rollout-Agent erwartet, dass der unter der konfigurierten Firmware-Server-URL erreichbare Rollout-Server eine Firmware im `.upx`-Format ausliefert, die er anschließend in das Gerät einspielt.

Nach dem Firmware-Update startet das Gerät neu und kontaktiert den Rollout-Server erneut. Der Rollout-Agent prüft, ob die vom Rollout-Server ausgelieferte Firmware bereits installiert ist. Diese Prüfung ist erfolgreich, da das Gerät im ersten Schritt die aktuelle Firmware erhalten hat. Der Rollout-Agent fährt mit dem Update der Konfiguration bzw. dem Download von Skriptdateien fort. Er erwartet, dass der unter der konfigurierten Config-Server-URL erreichbare

Rollout-Server ein Skript im `.lcs`-Format ausliefert, das er anschließend auf in das Gerät einspielt.

Die DHCP-Option 43

Die DHCP-Option 43 ist vendorspezifisch, d. h., jeder Vendor kann selbst entscheiden, wie er diese Option strukturiert und welche Informationen er darin kodiert. Die Option kann mehrere sogenannter Sub-Typen enthalten, die die Daten detaillierter strukturieren.

Für den Rollout-Agenten des Gerätes sind die folgenden Sub-Typen spezifiziert:

Sub-Type 1: Config-Server-URL

Die Angabe der Server-Adresse ist in den folgenden Formaten möglich:

- HTTP, HTTPS, TFTP
- IP-Adresse, FQDN

Beispiele:

- https://rollout:443/
- tftp://10.1.1.1
- http://10.1.1.2/test

Auch die Angabe von HiLCOS-Variablen ist möglich

Der Rollout-Agent erwartet, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin ein Konfigurations-Skript mit der Erweiterung `.lcs` sendet.

Hinweis:

Handelt es sich beim Rollout-Server um einen LSR, muss der Adresse das Präfix `lsr:` vorangestellt sein, z. B. `lsr:https://rollout:443/`. Anschließend baut der Rollout-Agent die korrekte LSR-Rollout-URL aus den Sub-Types 5 und folgende zusammen. Entsprechend sind die Sub-Types ab 5 nur bei der Verwendung dieses Präfixes von Bedeutung.

Handelt es sich beim Rollout-Server um keinen LSR, ist die Angabe der URLs für Config-Server und Firmware-Server von Hand und unter Verwendung von Variablen notwendig.

Sub-Type 2: Firmware-Server-URL

Wie bei Sub-Type 1, allerdings erwartet der Rollout-Agent, dass der unter dieser Adresse erreichbare Rollout-Server auf seine Anfrage hin eine Firmware-Datei mit der Erweiterung `.upx` sendet.

Sub-Type 3: HTTP-Username

Enthält den Usernamen für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 4: HTTP-Password

Enthält das Passwort für die HTTP-Authentifizierung in der URL (entsprechend `http://username:password@server`)

Sub-Type 5: LSR-Projektnummer

Enthält die im Rollout-Server für das erforderliche Rollout-Projekt gespeicherte Projektnummer.

Sub-Type 6: Zusätzliche URL-Parameter für LSR-Keyword

Der Rollout-Agent fügt diesen Inhalt an die konstruierte LSR-URL an (z. B. `?approval=yes`).

Sub-Type 7: Reboot-Time

Gibt die Wartezeit in Minuten für den Restart des Gerätes nach dem Update durch den Rollout-Server an.

Sub-Type 8: Request-Interval

Gibt den Intervall in Minuten an, in dem der Rollout-Agent seine Anfragen an den Rollout-Server sendet.

Sub-Type 9: TAN

Dieser Eintrag enthält die Rollout-TAN.

Sub-Type 10: Gerätenummer

Enthält die Gerätenummer des zu aktualisierenden Gerätes.

Sub-Type 11: Request-Delay

Enthält die Zeit in Minuten, die der Rollout-Agent zwischen Request 1 und Request 2 wartet.

Sub Type 12: Request-Random

Diese Einstellung verhindert, dass alle am Rollout beteiligten Geräte zeitgleich beim LSR-Server eine Konfiguration anfordern. Die folgenden Angaben sind möglich:

0

Die Anfragen erfolgen immer mit fest eingestellten Zeitangaben.

1

Legen Sie mit diesem Eintrag fest, dass die Anfrage nach einem Rollout zufällig erfolgt.

Sub-Type 13: Omit-Certificate-Check

Dieser Wert legt fest, ob der Rollout-Agent die Überprüfung des Rollout-Server-Zertifikats überspringen soll.

Hinweis: Fehlt dieser Sub-Type oder ist sein Inhalt leer, nimmt der Rollout-Agent den Wert “0” an und prüft somit das Server-Zertifikat.

Wichtig: Beachten Sie bitte, dass die vom Rollout-Server erhaltene Konfiguration den Rollout-Agent zum Abschluss abschalten sollte **(`Operating: no`)**, da das Gerät sonst nach der Reboot-Time rebootet.

Variablen

In den URLs sind alle Variablen verwendbar, die die LCOS-Konsole beinhaltet. Diese Variablen lassen sich in der Konsole über den Befehl `printenv` ausgeben.

Die Angabe der Variablen in den URLs erfolgt mit vorangestelltem “$” (z. B. `$__SERIALNO`).

Erzeugung der DHCP-Option 43

Die Erzeugung der DHCP-Option 43 erfolgt auf Grundlage der *RFC 2132, Abschnitt 8.4*.

Bei Verwendung eines ISC DHCPd DHCP-Server kann die Option 43 passend mit dem folgenden Konfigurationsabschnitt beispielhaft erzeugt werden:

Innerhalb der allgemeinen Konfiguration

```
option space Rollout;
option Rollout.config-server code 1 = text;
option Rollout.firmware-server code 2 = text;
option Rollout.HTTP-Username code 3 = text;
option Rollout.HTTP-Password code 4 = text;
option Rollout.Projectnumber code 5 = text;
option Rollout.AdditionalParams code 6 = text;
option Rollout.RebootTime code 7 = text;
option Rollout.RequestInterval code 8 = text;
option Rollout.Tan code 9 = text;
option Rollout.Devicenumber code 10 = text;
option Rollout.RequestDelay code 11 = text;
option Rollout.RequestRandom code 12 = text;
option Rollout.OmitCertCheck code 13 = text;
```

Innerhalb der Subnetz-spezifischen Konfiguration

```
vendor-option-space Rollout;
 option Rollout.config-server "LSR:https://10.200.50.1:443";
 option Rollout.firmware-server "LSR:https:// 10.200.50.1:443";
 option Rollout.HTTP-Username "RolloutUser";
 option Rollout.HTTP-Password "Secret";
 option Rollout.Projectnumber "1";
 option Rollout.RebootTime "300";
 option Rollout.RequestDelay "20";
 option Rollout.RequestRandom "0";
 option Rollout.OmitCertCheck "2";
```

Andere DHCP-Server (z. B. der Microsoft DHCP-Server) lassen keine Definition der Option 43 in der Konfiguration zu. Hier muss die vom Server als Option 43 auszuliefernde Bytefolge vorgefertigt in die Konfiguration eingefügt werden.

Um die Bytefolge nicht manuell erzeugen zu müssen, kann dies auch mit dem auf der folgenden Seite verlinkten Python-Skript erfolgen: *wiki.snom.com/Category:HowTo:Option_43*.

2.17 TCP-Port-Tunnel

In manchen Situationen ist es sinnvoll, einen vorübergehenden Zugriff – z. B. über HTTP (TCP-Port 80) oder TELNET (TCP-Port 23) – auf eine Station in einem Netz einzuräumen. Sofern beispielsweise bei der Konfiguration von Netzwerkgeräten Fragen auftauchen, kann der jeweilige Support besser weiterhelfen, wenn er direkten Zugriff auf das Gerät im Netz des Kunden hat. Die Standardmethode für den Zugriff auf Geräte im Netz über inverses Masquerading (Port-Forwarding) erfordert jedoch in manchen Fällen eine entsprechende Konfiguration der Firewall; zudem sind die dabei angelegten Zugänge schnell vergessen und stellen damit ein potentielles Sicherheitsrisiko dar.

Als Alternative zu den dauerhaften Zugängen über festes Port-Forwarding haben Sie die Möglichkeit, vorübergehende Fernwartungszugänge einzurichten, die nach einer bestimmten inaktiven Zeit automatisch wieder geschlossen werden. Dazu erzeugen Sie z. B. für den Support-Mitarbeiter einen **TCP/HTTP-Tunnel**, über welchen er einen temporären Zugang zum entsprechenden Gerät erhält.

Wichtig: Dieser Zugang ist nur für jene IP-Adresse gültig, von der aus Sie den Tunnel erzeugt haben. Der Zugriff auf das freizugebende Gerät im Netzwerk ist also nicht übertragbar!

2.17.1 TCP/HTTP-Tunnel konfigurieren

Die Konfiguration eines TCP/HTTP-Tunnels erfolgt über das Setup-Menü.

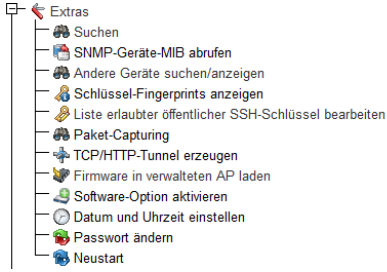
1. Wechseln Sie im Setup-Menü des Gerätes in das Verzeichnis **HTTP**.
2. Geben Sie für den Parameter **Max.-Tunnel-Verbindungen** die maximale Anzahl der gleichzeitig aktiven TCP/HTTP-Tunnel an, die Sie erlauben wollen.
3. Geben Sie für den Parameter **Tunnel-Idle-Timeout** die Lebensdauer eines Tunnels ohne Aktivität an (in Sekunden). Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

Fertig! Damit haben Sie die konfiguration der TCP/HTTP-Tunnel abgeschlossen.

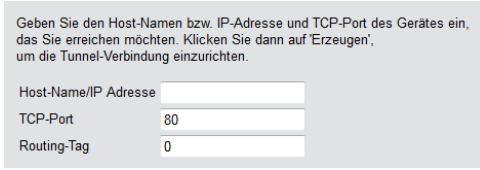
2.17.2 TCP/HTTP-Tunnel erzeugen

Einen TCP/HTTP-Tunnel richten Sie über die WEBconfig-Oberfläche Ihres Gerätes ein.

1. Melden Sie sich im WEBconfig jenes Gerätes an, hinter dem das freizugebende Gerät erreichbar ist.
2. Wählen Sie im Bereich **Extras** den Eintrag **TCP/HTTP-Tunnel erzeugen**.



3. Geben Sie den DNS-Namen bzw. die IP-Adresse des Gerätes ein, das Sie vorübergehend für den Zugriff über HTTP freischalten möchten, und wählen Sie den Port aus, der für den HTTP-Tunnel verwendet werden soll.



   Hinweis: Anstelle von HTTP- oder HTTPS-Fernwartungszugängen sind auch Fernwartungstunnel mit beliebigen anderen TCP-Diensten möglich, beispielsweise TELNET-Verbindungen (TCP-Port 23) oder SSH (TCP-Port 22).

4. Geben Sie ggf. das Routing-Tag des IP-Netzwerks an, in dem sich das freizugebende Gerät befindet.
5. Bestätigen Sie die Angaben mit **Erzeugen**.

Der folgende Dialog zeigt eine Bestätigung über den neu erstellten Tunnel und bietet einen Link auf das freizugebende Gerät.

2.17.3 TCP/HTTP-Tunnel vorzeitig löschen

Das Gerät löscht erstellte TCP/HTTP-Tunnel automatisch nach Ablauf der Tunnel-Idle-Timeouts (siehe *TCP/HTTP-Tunnel konfigurieren* auf Seite 202. Um einen Tunnel vorzeitig zu löschen, rufen Sie im Status-Menü unter **TCP-IP** > **HTTP** > **Aktive-Tunnel** die Liste der aktiven TCP/HTTP-Tunnel auf und entfernen den nicht mehr benötigten Tunnel gezielt.

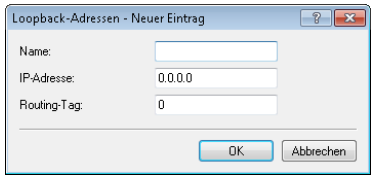
Wichtig: Aktive TCP-Verbindungen in diesem Tunnel werden mit dem Löschen des Tunnels **nicht** beendet, es können aber keine neuen Verbindungen mehr aufgebaut werden.

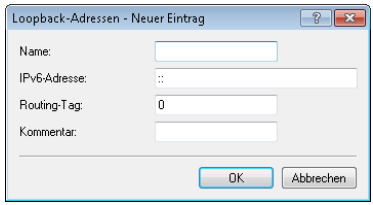
2.18 Benamte Loopback-Adressen einrichten

Ihrem Gerät lassen sich bis zu 16 IPv4- bzw 8 IPv6-Loopback-Adressen definieren, unter denen sich das Gerät (z. B. zum Management größerer Netz-Strukturen) ansprechen lässt. Um die Loopback-Adressen für bestimmte Netzwerke (z. B. im Zusammenhang mit "Advanced Routing and Forwarding") zu nutzen, ordnen Sie den Adressen ausgewählte Routing-Tags zu. Zur leichteren Identifizierung in anderen Konfigurationsteilen erhalten die Loopback-Adressen außerdem einen frei wählbaren Namen.

Nach nachfolgenden Schritte zeigen Ihnen, wie Sie eine Loopback-Adresse einzurichten.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **IPv4** > **Allgemein** > **Loopback-Adressen** bzw. **IPv6** > **Allgemein** > **Loopback-Adressen** und klicken Sie **Hinzufügen**.



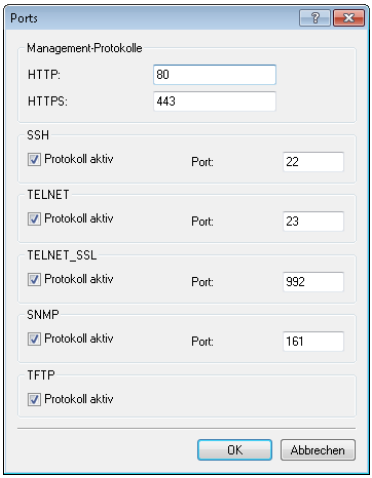


3. Geben Sie im Eingabefeld **Name** einen frei wählbaren Namen für die Loopback-Adresse ein, z. B. `LOOPBACK_1`.
4. Tragen Sie im Eingabefeld **IP-Adresse** bzw. **IPv6-Adresse** die Loopback-Adresse ein, die dieses Gerät erhalten soll, z. B. `10.0.0.99` für einen IPv4-Adresse bzw. `::1` für eine IPv6-Adresse.
   Das Gerät sieht jede dieser Adressen als eigene Adresse an und verhält sich, als hätte es das Paket auf dem (W)LAN empfangen. Dies gilt insbesondere auf maskierten Verbindungen. Antworten auf Pakete an eine Loopback-Adresse werden **nicht** maskiert!
5. Geben Sie im Eingabefeld **Routing-Tag** ein optionales Routing-Tag für die Loopback-Adresse an.
   Loopback-Adressen mit dem Routing-Tag '0' (ungetaggt) sind in allen Netzen sichtbar. Loopback-Adressen mit einem anderen Routing-Tag sind nur in Netzen mit dem gleichen Routing-Tag sichtbar.
6. Bei IPv6-Loopback-Adressen können Sie im Feld **Kommentar** zusätzlich einen Kommentar angeben.

2.19 Management-Ports für den Gerätezugriff anpassen

Sie haben im LANconfig die Möglichkeit, die Portnummern für die Management-Protokolle zu ändern.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in den Dialog **Management** > **Admin** und klicken Sie dort auf **Ports**.
3. Geben Sie die Portnummern für die gewünschten Management-Protokolle ein.



4. Schließen Sie alle geöffneten Dialoge durch einen Klick auf **OK**.

LANconfig schreibt die eingegebene Konfiguration zurück auf das Gerät.

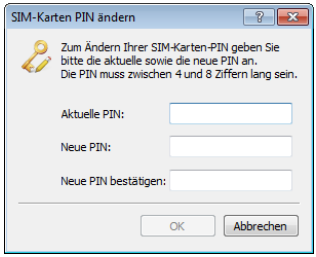
2.20 Ändern der SIM-Karten-PIN

Bei Geräten mit Mobilfunkmodem haben Sie über LANconfig die Möglichkeit, die PIN der SIM-Karte zu ändern. Die Änderung kann einfach vollzogen werden, indem Sie sowohl die alte PIN als auch die neue PIN eingeben. Zur Sicherheit verlangt LANconfig zusätzlich eine Bestätigung der neuen PIN. Alternativ haben Sie auch die Möglichkeit, die Änderung auf der Kommandozeile über die Aktion **PIN-Aendern** durchzuführen.

Die nachfolgenden Schritte beschreiben den Änderungsweg in LANconfig.

1. Wählen Sie in der Geräteübersicht von LANconfig das Gerät aus, dessen PIN Sie ändern wollen.

2. Wählen Sie über die Menüleiste **Gerät** > **SIM-Karten PIN ändern**. Ein neuer Dialog öffnet sich.



3. Geben Sie die bisher aktuelle PIN und die neue PIN ein. Bestätigen Sie die neue PIN durch wiederholte Eingabe.
4. Klicken Sie **OK**, um die Änderung zu übernehmen.

3 LANCOM Management System (LCMS)

Das Gerät unterstützt verschiedene Mittel (sprich Software) und Wege (in Form von Kommunikationszugängen) für die Konfiguration. Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten.

Eine Möglichkeit ist die Konfiguration mit der menügeführten und übersichtlichen Software **LANconfig**, mit der sich nahezu alle relevanten Parameter des Geräts einstellen lassen.

Der aktuelle Zustand des Geräts, der Verbindungen und der Status-Werte wird übersichtlich im **LANmonitor** angezeigt. Bei WLAN-Geräten sind darüber hinaus noch weitere Informationen über die drahtlosen Netze sowie die verbundenen Clients über den **WLANmonitor** abrufbar.

Mit **LANtracer** haben Sie die Möglichkeit, erweiterte Trace-Funktionen auszuführen, mit denen Sie bestimmte Informationen (wie z. B. Statuswerte und Funktionsmeldungen) einmal abrufen oder über einen längeren Zeitraum gezielt überwachen. Die dabei erzeugten Trace-Daten können Sie z. B. zur Protokollierung oder Fehlerdiagnose einsetzen.

Die folgenden Abschnitte behandeln ausführlich die Bedienung der angesprochenen Anwendungen.

Hinweis: Vorraussetzung für die einzelnen Anwendungen des LCMS ist ein Konfigurationsrechner mit einem Windows-Betriebssystem.

3.1 LANconfig - Geräte konfigurieren

Von der komfortablen Inbetriebnahme eines Einzelplatzgerätes mit den einfach zu bedienenden Installationsassistenten bis zum ganzheitlichen Management mit Firmware- und Konfigurationsverteilung größerer Installationen reicht das Anwendungsspektrum von LANconfig.

Basisfunktionen

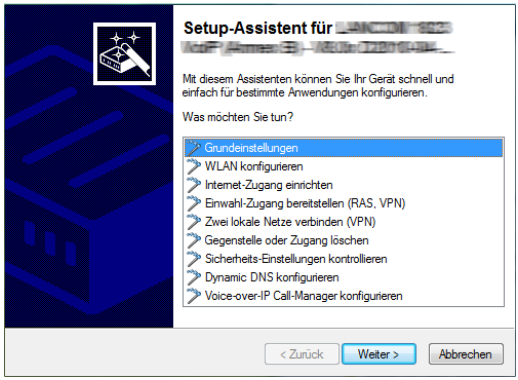
- Automatisches Erkennen von neuen, unkonfiguierten Geräten
- (Fern-)Konfiguration von Geräten über IP-Adresse, URL oder über die serielle Schnittstelle
- Integration von Telnet-, SSH-, HTTPS- und TFTP-Konfiguration
- Kontext-basiertes Hilfesystem zu den Konfigurations-Parametern
- In allen Installationsschritten bieten die Assistenten angepasste Eingabemasken
- Einrichtung von Backup-Verbindungen

Management von größeren Installationen

- Gruppenbildung
- Zentrale Firmware-Verteilung (Multi-Tasking, auch parallel mit mehreren DFÜ-Verbindungen)
- Simultankonfiguration mehrerer Geräte
- Verteilen von Konfigurations-Scripten
- WLAN-Gruppenkonfiguration
- Logging aller Aktionen
- Erstellung von neuen "Offline"-Konfigurationen für alle Geräte und HiLCOS-Versionen

3.1.1 LANconfig starten

Starten Sie LANconfig, z. B. mit einem Doppelklick auf das Desktop-Symbol. LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Wird dabei ein noch nicht konfiguriertes Gerät im lokalen Netz gefunden, startet LANconfig selbstständig den Setup-Assistenten.



Hinweis:

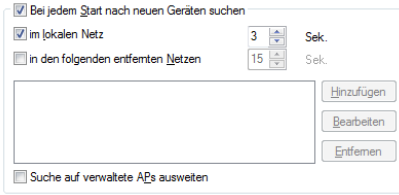
Eine aktivierte "Internetverbindungsfirewall" (Windows XP, Windows Vista, Windows 7) oder eine andere "Personal Firewall" auf dem Konfigurationsrechner kann dazu führen, dass LANconfig neue Geräte im LAN nicht findet. Deaktivieren Sie ggf. die Firewall für die Dauer der Konfiguration, wenn die unkonfigurierten Geräte nicht gefunden werden.

Ihr Gerät verfügt über eine umfangreiche eingebaute Firewall. Diese schützt Ihre Rechner auch dann, wenn keine weitere Firewall auf den Rechnern selbst – wie die "Internetverbindungsfirewall" – eingeschaltet ist.

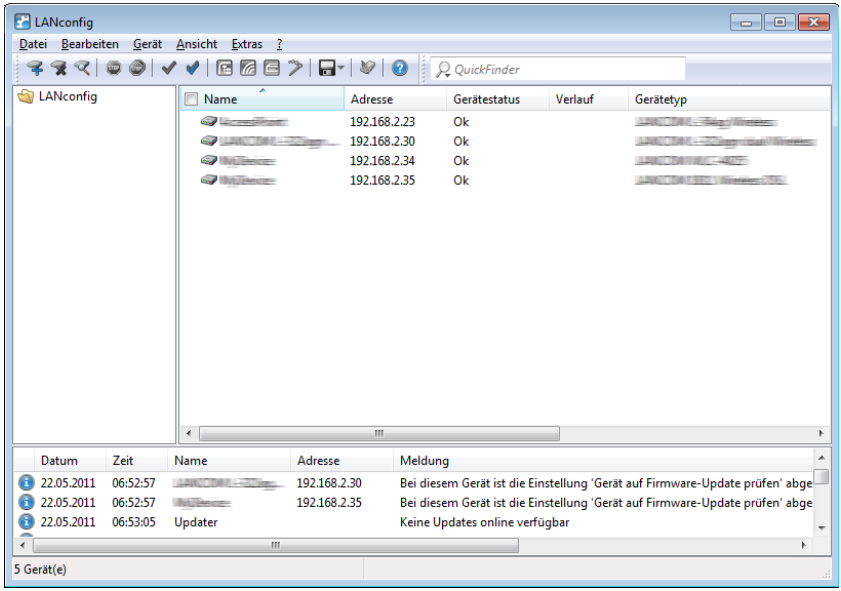
Hinweis: LANconfig kann beim Start des Betriebssystems automatisch geladen werden. Näheres dazu erfahren Sie im Kapitel *Applikation* auf Seite 298.

Neue Geräte suchen

Um die Suche eines neuen Geräts manuell einzuleiten, klicken Sie auf die Schaltfläche**Geräte suchen** ( )oder rufen den Befehl über **Datei** > **Geräte suchen** suchen auf. LANconfig erkundigt sich dann, wo es suchen soll. Um weitere Einstellung der Suche vorzunehmen, klicken Sie auf **Extras** > **Optionen** und wählen Menüpunkt **Start** aus.



Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.



Ein Klick auf die Schaltfläche **Konfigurieren** ( ) oder den Menüeintrag **Gerät** > **Konfigurieren** liest die aktuellen Einstellungen aus dem Gerät aus und zeigt die allgemeinen Geräteinformationen an. Ein Doppelklick auf den Geräteeintrag öffnet wahlweise den Konfigurations-Assistenten oder direkt die Konfiguration des Gerätes.

Die eingebaute Hilfe-Funktion

Die weitere Bedienung des Programms erklärt sich selbst bzw. über die Online-Hilfe. Indem Sie in einem Dialog-Fenster auf das Fragezeichen-Symbol

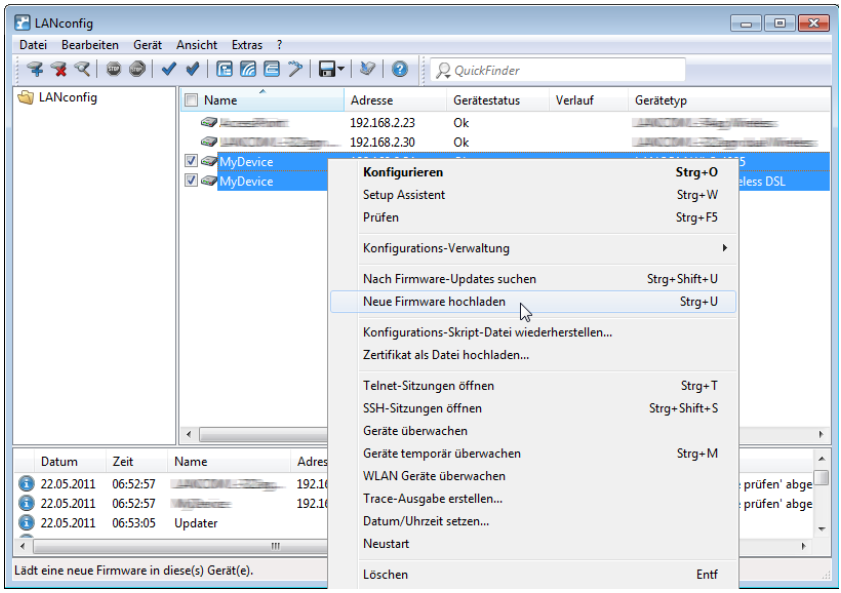
( ) oben rechts und anschließend auf eine Dialogabschnitt klicken, rufen Sie die kontextsensitive Hilfe auf, um weiterführende Informationen zu einer Einstellung zu erhalten. Alternativ genügt auch ein Rechtsklick auf den zu klärenden Dialogabschnitt.

Mehrfachauswahl

Mit LANconfig können mehrere Geräte gleichzeitig komfortabel (fern-)gewartet werden. Um mehrerer Geräte auszuwählen, haben Sie folgende Möglichkeiten:

- Ziehen Sie mit gedrückter Maustaste einen Auswahlrahmen über mehrere Geräte.
- Markieren Sie mehrere untereinander stehende Geräte mit gedrückter Shift-Taste und einem Klick auf das erste und das letzte Gerät der Liste.
- Markieren Sie beliebige Geräte mit gedrückter Strg-Taste und einem Klick auf die gewünschten Geräte.
- Aktivieren Sie die Option **Ansicht** > **Kontrollkästchen** und wählen Sie die Geräte über die entsprechenden Kontrollkästchen an.

LANconfig führt dann alle Aktionen für die ausgewählten Geräte nacheinander durch. So können Sie z. B. gleichzeitg für mehrere Geräte neue Firmwares hochladen.



Zur bequemen Verwaltung lassen sich Geräte zu Gruppen zusammenfassen. Dazu muss die Ansicht **Verzeichnisbaum** aktiviert sein. Im Verzeichnisbaum lassen sich neue Ordner über das Kontextmenü oder durch Auswahl von **Datei** > **Neuer Ordner** anlegen. Anschließend können Sie die Geräte durch einfaches Verschieben per 'drag und drop' in die gewünschten Ordner gruppieren.

Hinweis: In der Mehrgeräte-Konfiguration zeigt LANconfig nur die für die Mehrgeräte-Konfiguration geeigneten Eingabefelder an, z. B. bei Access Points die MAC Access-Control-Liste.

3.1.2 Arbeiten mit LANconfig

LANconfig bietet zahlreiche Funktionen, mit denen Sie die Arbeitsumgebung an Ihre speziellen Anforderungen anpassen können. Der Quickfinder bringt Sie schnell zu der gesuchten Einstellung; das Software-Update für LCMS hält Ihre Anwendung auf Wunsch automatisch aktuell.

Benutzerspezifische Einstellungen für LANconfig

Die Progammeinstellungen von LANconfig werden beim Beenden des Programms in der Datei 'lanconf.ini' im Programmverzeichnis gespeichert. Dazu gehören z. B. die angezeigten Geräte, die Ordnerstruktur, die derzeit gewählte Sprache etc. Beim Programmstart liest LANconfig diese ini-Datei ein und stellt den vorherigen Zustand der Software wieder her. Zum Speichern der ini-Datei benötigt der angemeldete Benutzer Schreibrechte in dem Programmverzeichnis.

Alternativ zum Programmverzeichnis kann LANconfig die ini-Datei auch von einem anderen Pfad laden. Dies kann z. B. das Benutzerverzeichnis des aktuellen Benutzers oder ein beliebiger anderer Speicherort sein:

- Mit der Auswahl des Benutzerverzeichnisses können auch Benutzer ohne Schreibrechte für das Programmverzeichnis ihre persönlichen Einstellungen speichern.
- Mit der Auswahl eines beliebigen anderen Speicherortes können Sie die Programmeinstellungen komfortabel in andere LANconfig-Installationen übertragen oder über eine Netzwerkressource für mehrere Benutzer zentral verwalten.

Sie konfigurieren den Speicherort der Programmeinstellung im Dialog **Extras** > **Optionen** > **Applikation**. Lesen Sie dazu auch das Kapitel *Applikation* auf Seite 298.

Sprache der grafischen Oberfläche umschalten

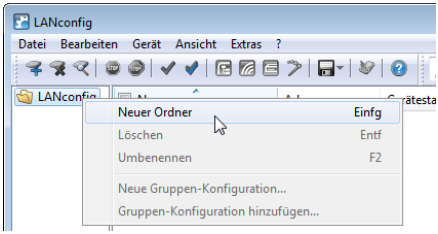
Die Sprache für die grafische Oberfläche von LANconfig können Sie unter **Extras** > **Optionen** > **Applikation** wahlweise auf **Deutsch**, **Englisch** oder **Spanisch** einstellen.

Verzeichnisbäume zur Organisation nutzen

LANconfig erlaubt mit dem Verzeichnisbaum die übersichtliche Verwaltung einer Vielzahl von Geräten. Für jedes Projekt oder jeden Kunden können Sie einen eigenen Ordner anlegen, in dem Sie die entsprechenden Geräte organisieren:

- Einen neuen Ordner legen Sie mit einem rechten Mausklick auf das übergeordnete Verzeichnis über den Kontextmenü-Eintrag **Neuer Ordner** an. Alternativ können Sie auch auf **Datei** > **Neuer Ordner** im Anwendungsmenü klicken.
- Die einzelnen Geräte lassen sich dann via 'drag and drop' aus der Liste mit der Maus in den entsprechenden Ordner ziehen. Auch das Verschieben der Geräte in einen anderen Ordner erfolgt auf diese Weise.

Hinweis: Die Zuordnung von einem Gerät zu einem bestimmten Ordner bezieht sich nur auf die Anzeige im LANconfig. Die Organisation der Ordner hat keine Auswirkung auf die Konfiguration der Geräte.

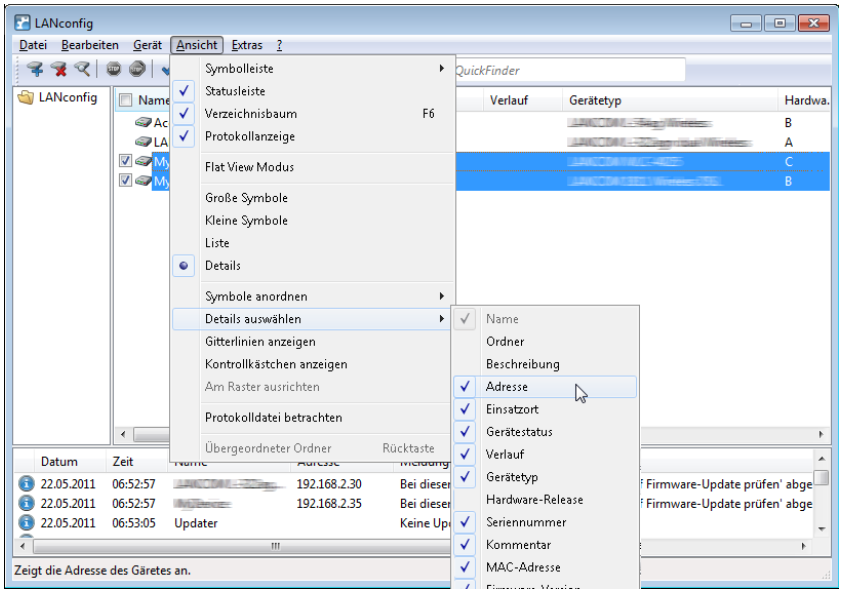


Hinweis: Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann mit der Funktionstaste F6 oder über das Menü **Ansicht** > **Verzeichnisbaum** ein- und ausgeschaltet werden.

Bessere Übersicht in LANconfig durch mehr Spalten

Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können Sie in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- und ausblenden. Wählen Sie unter **Ansicht** > **Details auswählen** die anzuzeigenden Spalten. Über den Menüpunkt **Ansicht** > **Symbole anordnen** können Sie außerdem die gewünschte Sortierung auswählen.

Hinweis: Die Sortierung der Ansicht können Sie auch direkt durch einen Klick mit der linken Maustaste in die entsprechende Spaltenüberschrift ändern. Mit jedem erneuten Klick wechselt die Sortierung.

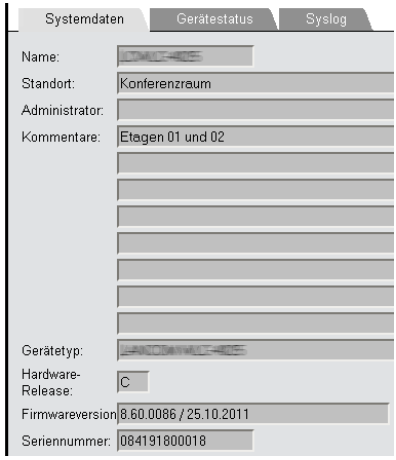


Im Einzelnen können Sie folgende Informationen in den Spalten anzeigen:

- Name
- Ordner
- Beschreibung
- Kommentar
- Adresse
- Standort
- Gerätestatus
- Verlauf
- Gerätetyp
- Produkt-Code
- Hardware-Release
- Seriennummer
- MAC-Adresse
- Firmware-Version
- Firmsafe
- 1. Image-Version
- 2. Image-Version

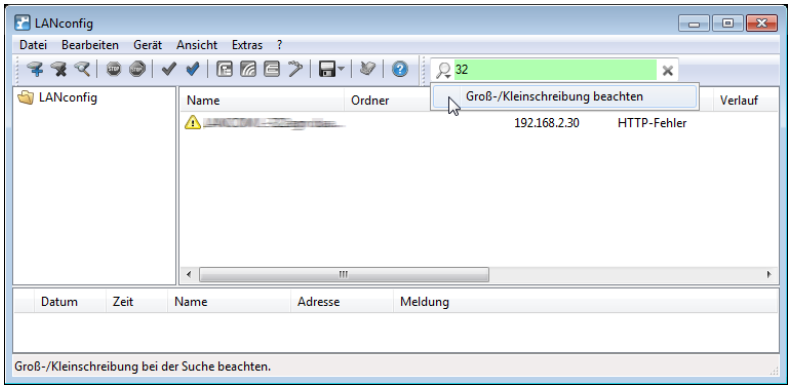
Mit **Alles einblenden** bzw. **Alles ausblenden** zeigen bzw. verbergen Sie alle Spalten mit einem Klick.

Hinweis: Die Spalte **Kommentar** enthält die Informationen des Kommentarfeldes 1 im Gerät.



QuickFinder in LANconfig

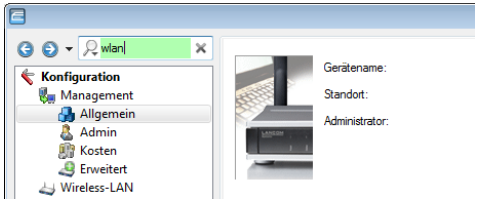
In der Hauptansicht von LANconfig finden Sie den QuickFinder in der Symbolleiste. Geben Sie im Suchfenster einen Suchbegriff ein, um die Liste der angezeigten Geräte zu reduzieren. LANconfig durchsucht dabei alle Werte, die in den Spalten der Geräte-Liste verfügbar sind – auch die derzeit ausgeblendeten Spalten. Klicken Sie auf der Symbol neben der Lupe, um bei der Suche die Groß-/Kleinschreibung zu beachten.



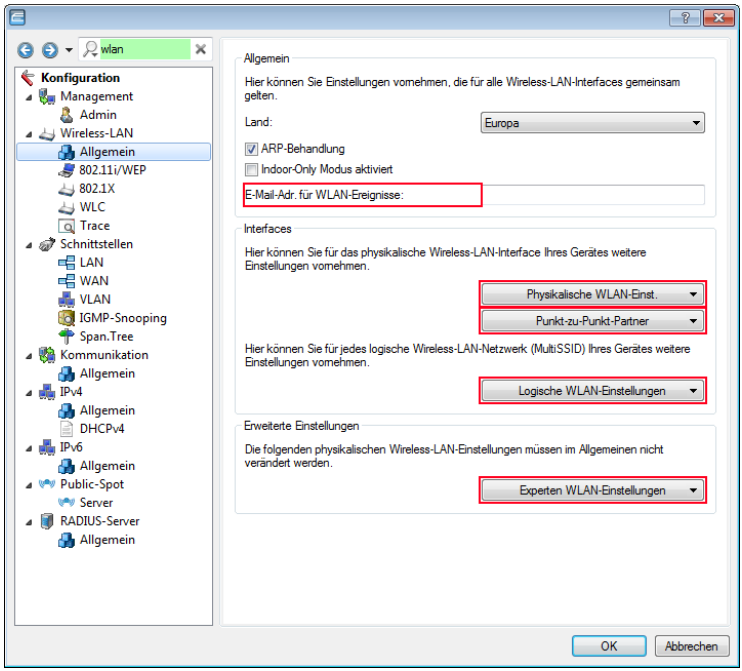
Wenn Sie einen bestimmten Wert oder Begriff in LANconfig oder der Konfiguration suchen, zeigt Ihnen der QuickFinder in den Konfigurationsdialogen von LANconfig schnell alle Stellen, in denen die gesuchte Zeichenkette enthalten ist.

1. Starten Sie LANconfig.
2. Öffnen Sie die Konfiguration des Gerätes, welche Sie durchsuchen möchten.
3. Geben Sie im Suchfeld den gewünschten Begriff ein, z. B. `wlan`. Die Suche unterscheidet nicht nach Groß- und Kleinschreibung. Sie können Teile von Worten oder Zahlen ebenso eingeben wie komplette Suchbegriffe. Leerzeichen in den Suchbegriffen suchen auch nur nach Zeichenketten, welche die entsprechenden Leerzeichen enthalten. Die Suchfunktion unterstützt jedoch keine Wildcards.

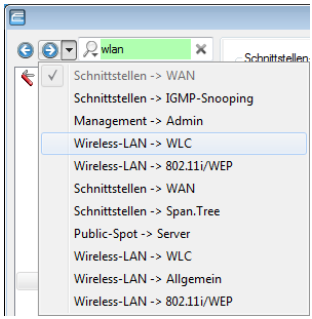
Der Konfigurationsbaum im linken Bereich von LANconfig ist nun reduziert auf alle Bereiche an, in denen der Suchbegriff enthalten ist:



Wählen Sie einen der Bereiche im Konfigurationsbaum (z. B. **Wireless-LAN** > **Allgemein'**), um die entsprechenden Suchergebnisse im Konfigurationsdialog farbig eingerahmt anzuzeigen:

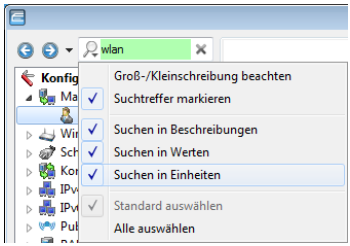


Nutzen Sie die Navigationsschaltflächen 'Zurück' und 'Vor' links neben dem Suchfeld, um in den zuletzt besuchten Dialogen zu blättern. Für einen besonders schnellen Zugriff auf die letzten 10 besuchten Dialoge klicken Sie auf den Pfeil rechts neben der Schaltfläche 'Vor':



Klicken Sie auf das Kreuz rechts neben dem Suchfeld, um die Suche zu löschen und um im Konfigurationsbaum wieder alle Einträge anzuzeigen.

Um die Suchergebnisse optional zu reduzieren, wählen Sie Bereiche aus, die LANconfig in die Suche einbeziehen soll. Klicken Sie dazu auf die Lupe links neben dem Suchfeld und aktivieren oder deaktivieren Sie die gewünschten Bereiche. Legen Sie hier außerdem fest, ob die Suche die Treffer farbig markiert oder nur den Konfigurationsbaum auf die gefundenen Dialoge reduziert:



Hinweis: LANconfig löscht die Einstellung der Suchbereiche und die Liste der zuletzt besuchten Dialoge beim Schließen der Konfiguration.

Wenn Sie z. B. in der Konfiguration bestimmte Einstellungen für Ihren Internet-Provider vorgenommen haben, können Sie einfach mit der Eingabe des Namens alle Stellen in der Konfiguration finden, die sich auf diesen Provider beziehen.

Konkret erfasst die Suche dabei die folgenden Bereiche:

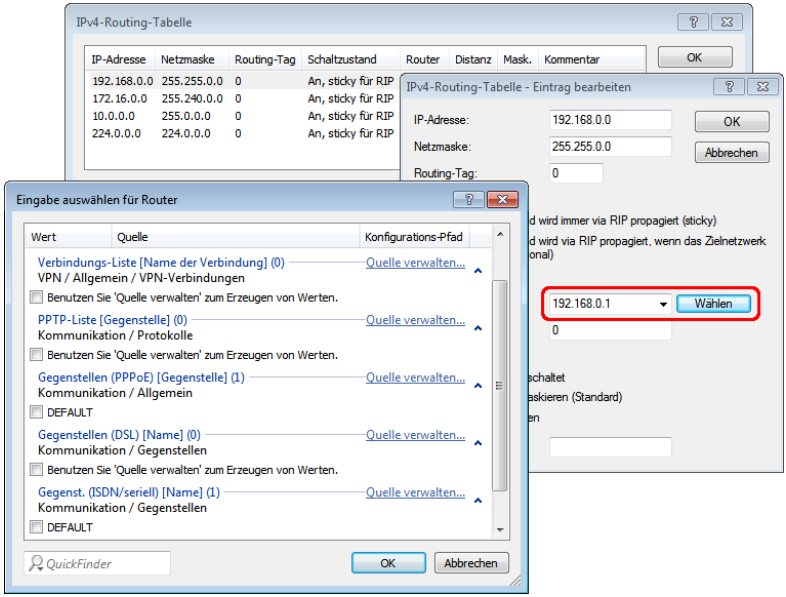
- Einträge im Konfigurationsbaum
- Bezeichnungen der Bereiche (Sektionen) in den einzelnen Konfigurationsdialogen
- Parameter
- Werte der Parameter
- Erläuternde Texte in den Dialogen
- Namen der Tabellen
- Namen der Tabellenspalten

Quicklinks zur Verwaltung von Quelltabellen

Lassen sich in einem Eingabefeld Werte auswählen, die bereits in einer oder mehreren anderen Tabellen vordefiniert sind, steht mit den sogenannten Quicklinks eine direkte Möglichkeit zur Verwaltung dieser Quelltabellen zur

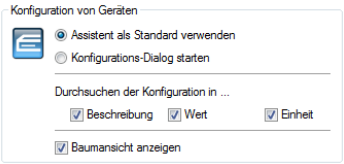
Verfügung. Dies ermöglicht es, die vorgegebene Konfigurationsreihenfolge zu umgehen. Statt zur Neuanlage von gewünschten Elementen zunächst die aktuelle Auswahl verlassen zu müssen, können Sie diese Elemente direkt bei Bedarf anlegen. Diese neuen Elemente stehen sofort für eine Selektion zur Verfügung.

Um die Konfigurationsstruktur zu verdeutlichen, zeigt LANconfig neben den einzelnen Quellen den Konfigurations-Pfad an. Ist die Auswahl der Konfigurationsparameter aus mehreren Quelltabellen möglich, gruppiert LANconfig die Einträge entsprechend. Zu jeder Gruppe gibt LANconfig zusätzlich die Anzahl der enthaltenen Einträge an.



Assistent oder Konfigurationsdialog wählbar

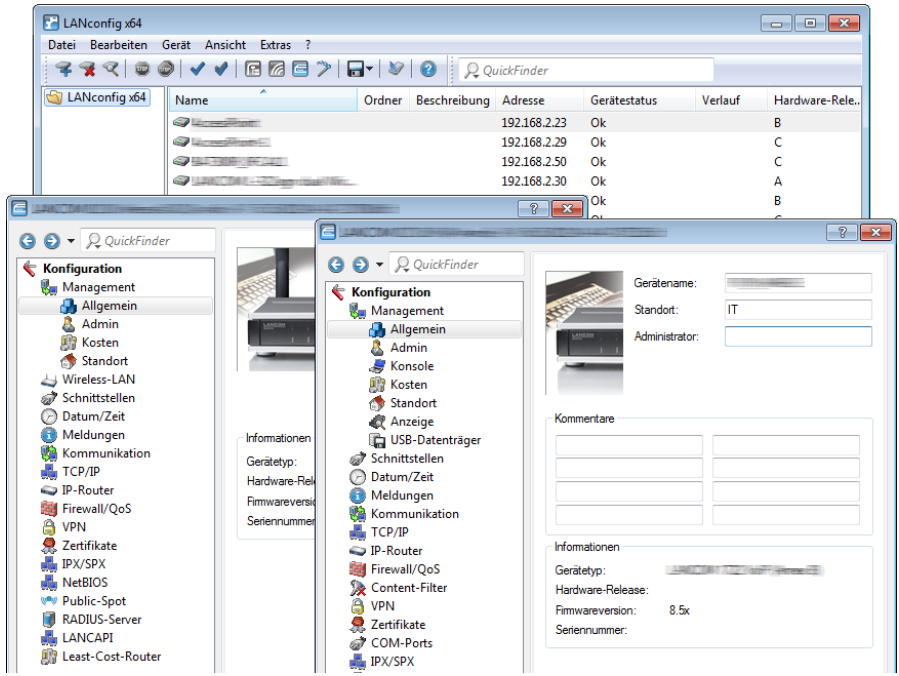
Beim Doppelklick auf einen Eintrag in der Geräteliste von LANconfig kann ausgewählt werden, ob sich der Dialog zur manuellen Bearbeitung der Konfiguration oder ein Setup-Assistent öffnen soll. Das Standardverhalten von LANconfig legen Sie im Dialog **Extras** > **Optionen** auf der Seite **Allgemein** fest.



- **Assistent als Standard verwenden:** Startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Auswahldialog für die Assistenten.
- **Konfigurations-Dialog starten:** Startet beim Doppelklick auf den Geräte-Eintrag in LANconfig den Konfigurations-Dialog.

Multithreading

Bei der Verwaltung von Projekten ist es oft hilfreich, die Konfigurationen von mehreren Geräte gleichzeitig zu öffnen, um darin Gemeinsamkeiten oder Unterschiede abzugleichen. LANconfig erlaubt das gleichzeitige Starten von mehreren Konfigurationsdialogen ("Multithreading"). Nach dem Öffnen einer Konfiguration können aus der Liste der Geräte im LANconfig einfach weitere Konfigurationen geöffnet werden. Alle Konfigurationen können parallel bearbeitet werden.

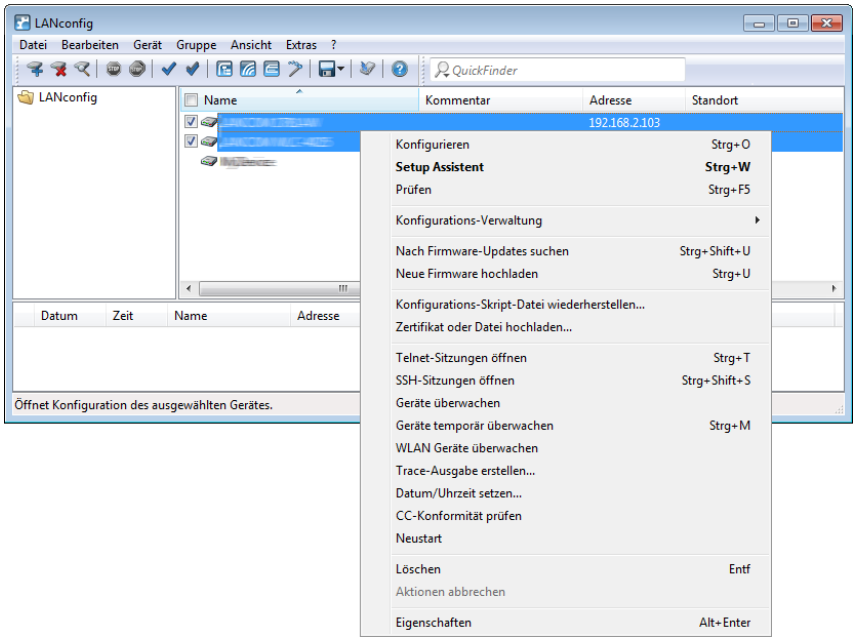


Hinweis: Zwischen den geöffneten Konfigurationen können Inhalte mit "Copy and Paste" über die Zwischenablage übertragen werden.

Beim Multithreading können auch aus den erreichbaren Geräten ausgelesene Konfigurationen und Konfigurationsdateien bearbeitet werden. Jede Konfiguration wird separat beim Schließen des entsprechenden Dialogs in die Datei bzw. das Gerät zurückgeschrieben.

Projektmanagement mit LANconfig

LANconfig erleichtert die Konfiguration von verschiedenen Geräten in einem Projekt mit einigen Funktionen, die gleichzeitig auf mehreren Geräten ausgeführt werden können. Sind in der Liste der Geräte im LANconfig mehrere Einträge markiert, können mit einem rechten Mausklick über das Kontextmenü folgende Aktionen aufgerufen werden:



- **Konfigurieren**

  Öffnet für die ausgewählten Geräte den Konfigurationsdialog unter LANconfig.

- **Prüfen**

  Prüft die ausgewählten Geräte auf Erreichbarkeit.

- **Konfigurationsverwaltung**

  Sichern Sie die aktuelle Gerätekonfiguration als Konfigurationsskript oder als *.lcf-Datei.

- **Nach Firmware-Updates suchen**

  Sucht im unter **Extras** > **Optionen** > **Update** konfigurierten **Firmware-Archiv**-Ordner nach verfügbaren Firmware-Updates.

- **Neue Firmware hochladen**

  Lädt eine Firmware parallel in alle ausgewählten Geräte.

- **Konfigurations-Skript-Datei wiederherstellen**

  Führt ein Konfigurationsscript für alle ausgewählten Geräte aus.

- **Telnet-Sitzungen öffnen**, **SSH-Sitzungen öffnen**

  Öffnet mehrere Kommandozeilen-Fenster und startet zu jedem Gerät eine separate Telnet- bzw. SSH-Verbindung. LANconfig greift dafür auf die in den Einstellungen konfigurierten, externen Client-Programme zurück. Wenn Sie keine Client-Programme installiert und angegeben haben, bricht LANconfig diese Aktion mit einer Fehlermeldung ab.

- **Zertifikat oder Datei hochladen**

  Öffnet den Upload-Dialog für das geräteinterne Dateimanagement.

- **Geräte überwachen**, **Geräte temporär überwachen**

  Öffnet die ausgewählten Geräte im LANmonitor zur Überwachung.

- **WLAN Geräte überwachen**

  Öffnet die ausgewählten Geräte im WLANmonitor zur Überwachung.

- **Trace-Ausgabe erstellen**

  Öffnet mehrere LANtracer-Fenster und erstellt für jedes Gerät eine separate Trace-Ausgabe.

- **Datum/Uhrzeit setzen**

  Stellt auf allen ausgewählten Geräten die Uhrzeit gleich ein.

  Hinweis: Beachten Sie für die Einstellung der Uhrzeit auch die Funktionen des Geätes als NTP-Client und NTP-Server.

- **CC-Konformität prüfen**

  Prüft, ob die Konfiguration der ausgewählten Geräte CC-konform ist. Diese Aktion ist nur bei CC-Geräten sinnvoll.

- **Neustart**

  Startet die ausgewählten Geräte neu.

- **Löschen**

Löscht die ausgewählten Geräte aus der Geräteliste im LANconfig.

- **Aktion abbrechen**

  Erzwingt denn Abbruch einer laufenden LANconfig-Aktion (z. B. den Upload einer Datei).

- **Eigenschaften**

  Öffnet einen gemeinsamen Eigenschaften-Dialog, in dem Sie für mehrere Geräte gleichzeitig identische allgemeine und backupbezogene Einstellungen vornehmen können. Berücksichtigen Sie dabei, dass Ihnen in diesem Sammeldialog –gegenüber einem gerätespezifischen Eigenschaften-Dialog – nicht alle Einstellungsmöglichkeiten zur Verfügung stehen.

Flexible Gruppen-Konfiguration mit LANconfig

Die flexible Gruppen-Konfiguration unterstützt Sie bei der Verwaltung vieler Geräte: eine gezielte Auswahl an Konfigurations-Parametern wenden Sie gemeinsam auf eine Gruppe von Geräten an. Dies ist komfortabler als die Parameter einzeln in jedem Gerät manuell zu setzen, z. B. bei identischen SSID-Einstellungen in WLAN-Access-Points. So vermeiden Sie, komplette Konfigurationsdateien anderer Geräte zu übertragen. Denn dabei werden gerätespezifische Parameter wie die IP-Adresse ebenfalls übernommen. Die Gruppen-Konfiguration von LANconfig ermöglicht das einfache gemeinsame Setzen von Gruppen-Konfigurationsparametern und damit das gleichzeitige Verwalten mehrerer Geräte.

Durch das Zuordnen mehrerer Geräte zu einer Gruppen-Konfiguration fassen Sie diese zu einer gemeinsam verwalteten Gruppe zusammen. Die Gruppen-Konfigurationsdateien, die gemeinsame Parameter für eine Gruppe von Geräten enthalten, speichern Sie wie komplette Konfigurationsdateien auf der Festplatte oder einem Server. Für die Konfiguration von ganzen Geräte-Gruppen legt LANconfig Verweise auf diese Gruppen-Konfigurationsdateien an. Diese Verweise sind eine komfortable Verbindung zwischen den Geräte-Einträgen in LANconfig und den Gruppen-Konfigurationsdateien.

LANconfig stellt in Form der Group Templates allgemeine Vorlagen bereit, die zur Erzeugung von Gruppen-Konfigurationen dienen. Den Umfang der verwendeten Parameter für eine Gruppe definieren Sie individuell für Ihre Bedürfnisse. Verwenden Sie diese Funktion, wenn Sie zusätzliche Konfigura-

tions-Parameter als Gruppen-Parameter aufnehmen oder vorgeschlagene Gruppen-Parameter entfernen. Diese von Ihnen erstellten Konfigurationen speichern Sie wahlweise als Gruppen-Konfiguration oder als kundenspezifische Vorlage für die Erzeugung von weiteren Gruppen-Konfigurationen.

Hinweis: Sie haben später ausschließlich die Option, Ihre erstellten Gruppen-Konfigurations-Vorlagen zu ändern, nicht jedoch die LANconfig-Basis-Vorlagen.

Folgende Vorlagen für Gruppen-Konfigurationen stehen in LANconfig zur Verfügung:

- **Group Template WLAN:** Beinhaltet die Parameter, die auf WLAN-Geräten gemeinsam verwaltet werden.
- **Group Template WLC:** Beinhaltet möglichst viele Parameter von WLC-Geräten, die im Betrieb eines Clusters von WLCs den Bedarf an individueller Konfiguration minimieren.
- **Group Template Empty:** Enthält keine Vorauswahl von Gruppen-Parametern und dient als Basis zur Erstellung eigener Gruppenvorlagen, welche über die Gruppenvorlagen für WLAN und WLC hinausgehen. Wählen Sie hier aus der Gesamtmenge aller verfügbaren Konfigurationsparameter in allen Geräte-Typen diejenigen aus, welche Sie für Ihre Gruppen-Konfiguration nutzen möchten.

Wenn Sie stattdessen die Einstellung **Verwende alternative Basiseinstellungen** aktivieren, bietet Ihnen LANconfig eine Liste an, aus der Sie alternativ eine Gruppen-Vorlage für bestimmte Gerätetypen wählen können. Mit den Group Templates haben Sie die Möglichkeit, die gemeinsamen Parameter für verschiedene Geräte-Typen in die Gruppen-Vorlage zu übernehmen. Einige Parameter überschneiden sich jedoch bei verschiedenen Gerätetypen (z. B. DSL und DSLoL). Die Group Templates stellen daher immer auch einen Kompromiss dar, in dem einige Parameter möglicherweise fehlen. Für homogenen Gruppen, die ausschließlich einen speziellen Gerätetyp umfassen, bietet es sich daher an, eine spezielle Gerätekonfiguration mit einer bestimmten Firmware als Vorlage für die Gruppe auszuwählen. Diese Bassiseinstellung bietet so exakt die für diesen Gerätetyp benötigten Konfigurationsparameter zur Auswahl an.

Neue Gruppen-Konfigurationsdatei anlegen

Voraussetzung für die Verwendung der Gruppen-Konfiguration ist die Gruppierung der Geräte in Ordnern. Diese LANconfig-Ordner enthalten die Geräte-Einträge, für die eine gemeinsame Konfiguration der Gruppen-Konfigurationsparameter sinnvoll ist, sowie einen Verweis auf die Gruppen-Konfiguration. Die nachfolgenden Handlungsschritte beschreiben, wie sie eine neue Gruppen-Konfiguration anlegen.

Hinweis: Mit einer Gruppen-Konfiguration verwalten Sie die Geräte-Parameter, die allen zugeordneten Geräten gemeinsam sind. Eine Geräte-Individualkonfiguration bezieht sich auf die Parameter, die gerätespezifisch sind.

1. Erstellen Sie einen neuen Ordner für die zu gruppierenden Geräte.

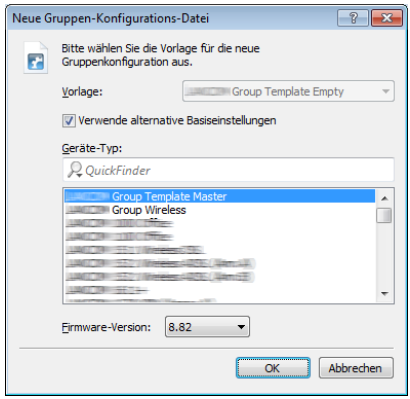
   Sie haben zwei Möglichkeiten, diesen Ordner anzulegen:

   - Klicken Sie mit der rechten Maustaste auf einen existierenden Ordner in der Ordner-Ansicht. Wählen Sie **Neuer Ordner mit Gruppen-Konfiguration**. Der Konfigurationsdialog erstellt zunächst unterhalb der angeklickten Verzeichnis-Ebene einen neuen Ordner und startet mit der Template-Auswahl zur Erstellung einer neuen Gruppen-Konfiguration.
   - Klicken Sie mit der rechten Maustaste in der Ordneransicht auf das Verzeichnis, in dem Sie den neuen Ordner erstellen möchten. Wählen Sie im Kontext-Dialog **Neuer Ordner** aus und vergeben Sie einen Namen. Verschieben Sie die zu gruppierenden Geräte mit der Maus in diesen neuen Ordner. Klicken Sie anschließend mit der rechten Maustaste auf den neuen Ordner und wählen Sie im Kontextmenü den Eintrag **Neue Gruppen-Konfiguration**. Es öffnet sich die Template-Auswahl zur Erstellung einer neuen Gruppen-Konfiguration.

2. Wählen Sie eine **Vorlage** sowie die entsprechende **Firmware-Version** aus. Wenn Sie zuvor eigene Gruppen-Vorlagen gespeichert haben, finden Sie diese ebenfalls in der Auswahlliste der Vorlagen.

   Alternativ haben Sie auch die Möglichkeit, durch aktivieren der Schaltfläche **Verwende alternative Basiseinstellungen** die grundlegenden Einstellungen eines speziellen Geräte-Typs als Basis für die neue Gruppen-Konfigu-

ration zu verwenden. Die neue Gruppen-Konfiguration übernimmt in diesem Fall die Standardwerte vom gewählten Geräte-Typ.

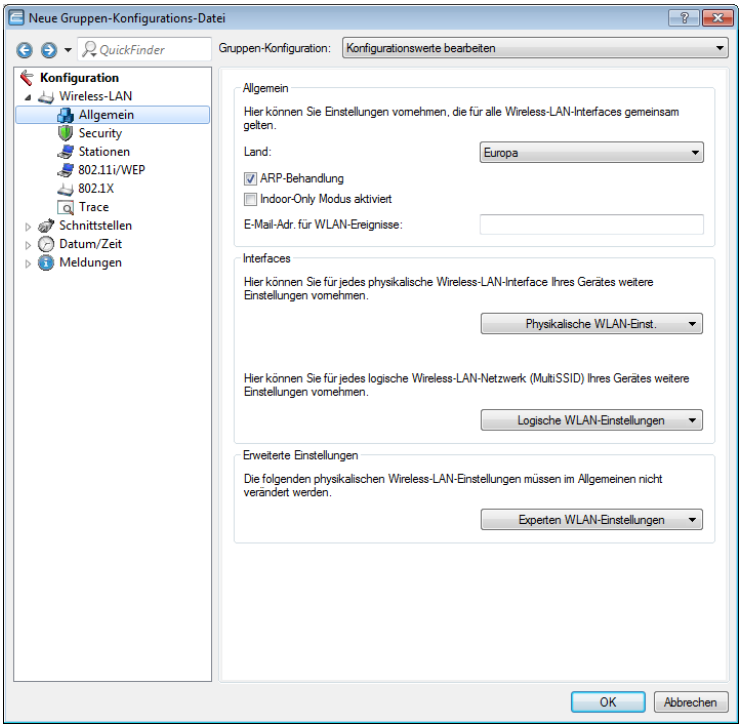


Hinweis: Um inkonsistente Sätze von Konfigurationsparametern zu vermeiden, basieren die alternativen Basiseinstellungen auf einer leeren Vorlage entsprechend dem **Group Template Empty**.

3. Klicken Sie auf **OK**. Es öffnet sich der Konfigurationsdialog für die Geräteparameter.
   Hier stehen Ihnen über die Auswahlliste **Gruppen-Konfiguration** zwei Bearbeitungsmodi zur Auswahl:

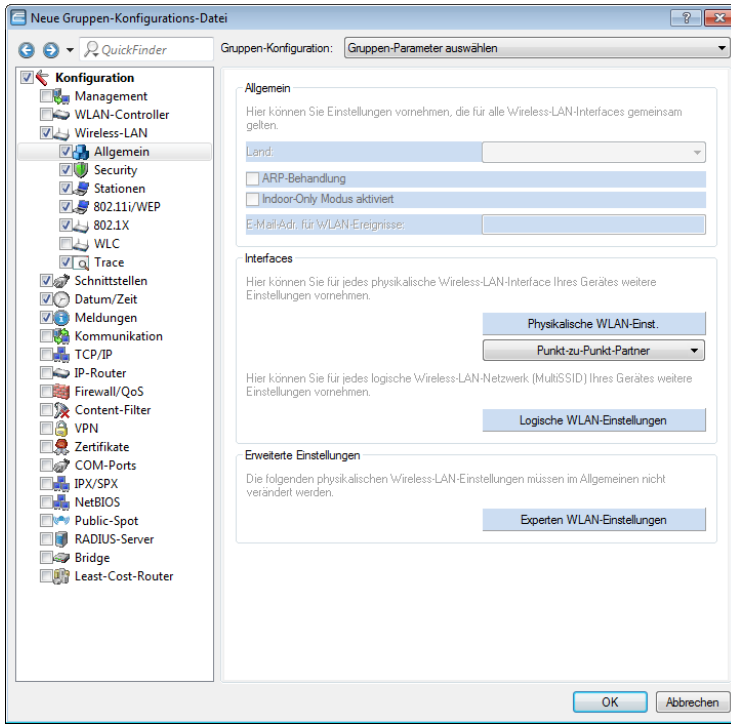
   - Modus **Konfigurationswerte bearbeiten**.
   - Modus **Gruppen-Parameter auswählen**.

   Der Konfigurationsdialog startet mit der Ansicht **Konfigurationswerte bearbeiten**. In dieser Ansicht finden Sie ausschließlich die gemeinsam zu verwaltenden Parameter der Gruppe. Hier ist die Einstellung auf die gewünschten Werte und Inhalte möglich. Alle Parameter, die für die einzelnen Geräte gelten, sind ausgeblendet.



Hinweis: Sofern Sie ein leeres Gruppen-Template gewählt haben, ist der angezeigte Dialog leer. Sie müssen dann zunächst die Gruppen-Parameter auswählen, die Sie im o. g. Modus bearbeiten wollen.

Im Konfigurations-Modus **Gruppen-Parameter auswählen** wählen Sie aus allen verfügbaren Parametern diejenigen an- oder ab, die Sie für eine angepasste Gruppen-Konfiguration benötigen.



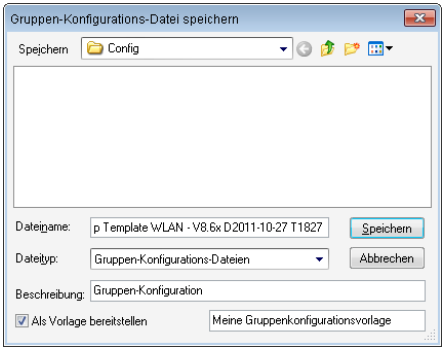
Hellblau eingefärbte Elemente sind für die Verwendung in der Gruppen-Konfiguration ausgewählt. Klicken Sie einmal mit der linken Maustaste auf ein Element, um dessen Auswahlstatus zu ändern.

Beachten Sie folgende Besonderheiten:

- Bei Tabellen mit statisch vorgegebenen Zeilen (z. B. interfacebezogenen Tabellen wie **Logische WLAN-Einstellungen**) haben Sie die Möglichkeit, auch einzelne Parameter in die Gruppen-Konfiguration zu übernehmen. In LANconfig erkennen Sie diese Tabellen oft daran, dass sich bei Anklicken der dazugehörigen Schaltfläche ein Pulldown-Menü öffnet.
- Bei Tabellen mit dynamisch erzeugten Zeilen (wie z. B. der **Routing-Tabelle**) ist ausschließlich die gesamte Tabelle für die Gruppen-Konfiguration an- oder abwählbar.
- Die Firewall ist ebenfalls ausschließlich komplett für die Gruppen-Konfiguration an- oder abwählbar.

4. Bearbeiten Sie gemäß der im vorangegangenen Schritt gegebenen Erläuterungen nun die Konfigurationswerte, und fügen Sie ggf. weitere Gruppenparameter zur Konfiguration hinzu. Klicken Sie zum Abschluss auf **OK**.
5. Geben Sie für die erstellte Gruppen-Konfiguration einen aussagekräftigen **Dateinamen** an und wählen Sie einen Speicherpfad.

   Sie haben zudem die Möglichkeit, diese Gruppen-Konfiguration zukünftig als eigene Vorlage für die Erstellung weiterer Gruppen-Konfigurationen angeboten zu bekommen. Aktivieren Sie hierzu die Option **Als Vorlage bereitstellen** und vergeben Sie eine aussagekräftige Bezeichnung.



   Hinweis: Sie haben auch später noch die Gelegenheit, aus einer bereits existierenden Gruppen-Konfiguration eine Vorlage zu erstellen. Klicken Sie dazu mit der rechten Maustaste im entsprechenden Gruppen-Ordner auf die entsprechende Gruppen-Konfiguration. Wählen Sie anschließend im Kontextmenü **Als Vorlage bereitstellen** und vergeben Sie eine aussagekräftige Bezeichnung.

6. Klicken Sie auf **Speichern**, um die Aktion abzuschließen.

Fertig! Die zugeordnete Gruppen-Konfigurationsdatei erscheint nun in der Geräteliste mit dem vorgegebenen Namen. Um diesen Namen individuell anzupassen, klicken Sie die Gruppen-Konfiguration mit der rechten Maustaste und ändern unter **Eigenschaften** > **Allgemein** den Text für die **Beschreibung.**

Hinweis: Die Gruppen-Konfiguration speichert alle Parameter in eine Gruppen-Konfigurationsdatei, einschließlich solcher Parameter mit voreingestellten

Standardwerten. Verwenden Sie die Scripting-Funktionen, um ausschließlich die von der Standardeinstellung abweichenden Parameter aus dem Gerät auszulesen und ggf. auf andere Geräte zu übertragen.

Bestehende Gruppen-Konfigurationsdatei verwenden

In manchen Fällen ist eine andere Struktur der mit LANconfig verwalteten Geräte sinnvoll, als es die Gruppen-Konfiguration erfordern würde. Die Geräte in standortspezifischen Ordnern sind z. B. teilweise durchaus denselben Gruppen zuzuordnen. Um redundante Gruppen-Konfigurationsdateien für jeden Ordner zu vermeiden, empfiehlt es sich, in mehreren Ordnern Verweise auf eine gemeinsam verwendete Datei zu erstellen.

Wollen Sie eine vorhandene Gruppen-Konfigurationsdatei für eine Gruppe von Geräten verwenden, klicken Sie mit der rechten Maustaste auf den gewünschten Ordner. Wählen Sie anschließend im Kontextmenü den Eintrag **Gruppen-Konfiguration hinzufügen**.

Wählen Sie im folgenden Dialog die bereits bestehende Gruppen-Konfigurationsdatei aus und erstellen Sie so in dem Ordner einen Verweis auf diese Datei.

Hinweis:

Beachten Sie, dass Änderungen der Gruppen-Konfigurationsdatei auch Änderungen der jeweiligen Gruppen-Konfigurationen in verschiedenen Ordnern zur Folge haben.

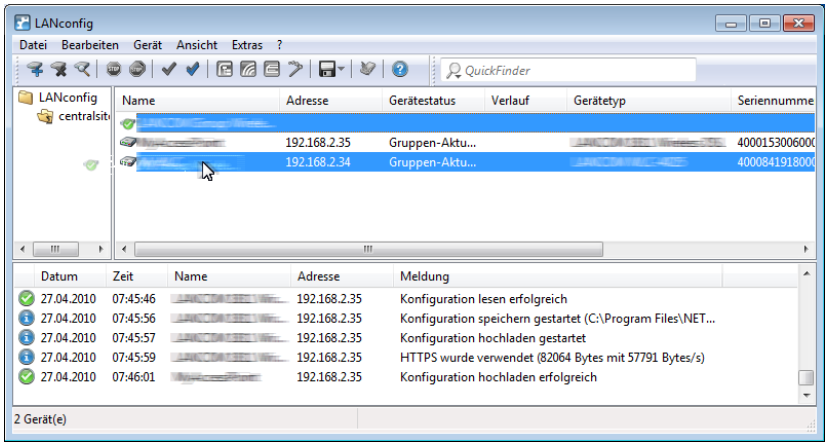
Erstellen Sie in einem Gruppen-Ordner weitere Geräte, oder ändern Sie eine bestehende Gruppen-Konfiguration, informiert Sie LANconfig, dass für die entsprechenden Geräte eine Aktualisierung vorliegt. Diese Aktualisierung ist direkt im Anschluss oder später über das Kontextmenü durchführbar.

Gerätekonfigurationen mit Gruppen-Konfigurationen aktualisieren

Beim Aufrufen oder Aktualisieren eines Ordners prüft LANconfig, ob die Konfiguration der Geräte in diesem Ordner mit den Einstellungen in der aktiven Gruppen-Konfiguration übereinstimmt. Über Abweichungen von der Gruppen-

Konfiguration informiert der Gerätestatus **Gruppen-Aktualisierung empfohlen**.

Um die Gruppen-Konfiguration in das WLAN-Gerät zu laden, ziehen Sie den Gruppen-Konfigurationseintrag auf den entsprechenden Geräteeintrag. Nach erfolgreicher Übertragung der Parameter ändert sich der Gerätestatus auf **Ok**.



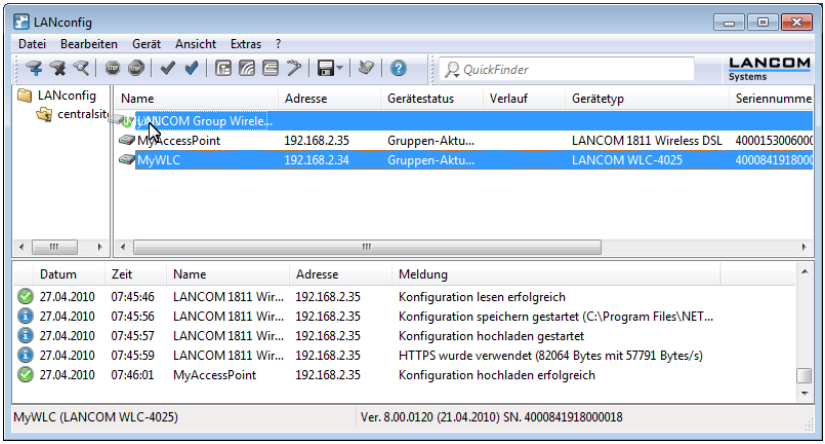
Es ist auch möglich, Teilkonfigurationen eines WLAN-Gerätes als Gruppen-Konfiguration zu verwenden. Ziehen Sie hierzu den Geräteeintrag auf den Gruppen-Konfigurationseintrag.

Gruppen-Konfigurationen mittels Master-Gerät aktualisieren

Neben dem manuellen Verändern der Parameter einer Gruppen-Konfiguration (siehe Kapitel *Gerätekonfigurationen mit Gruppen-Konfigurationen aktualisieren* auf Seite 233) kann auch die aktuelle Konfiguration eines Gerätes als Basis für eine Gruppen-Konfiguration verwendet werden. Ein Gerät wird damit zum "Master" für alle anderen Geräte im gleichen Ordner.

Um die Parameter einer Gruppen-Konfiguration von einer aktuellen Geräte-Konfiguration zu übernehmen, ziehen Sie einfach den Eintrag des Gerätes auf die gewünschte Gruppen-Konfiguration. Alle in der Gruppen-Konfiguration definierten Parameter werden dabei mit den Werten der Geräte-Konfiguration überschrieben.

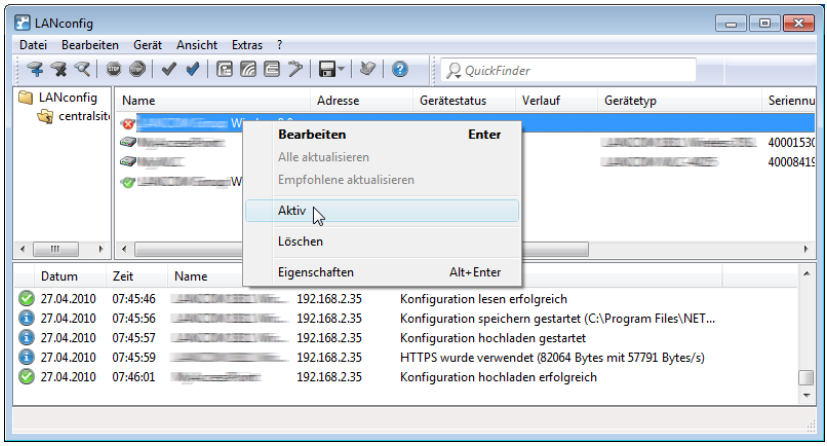
Beim folgenden Prüfen der Geräte wird LANconfig feststellen, dass die Konfigurationen der anderen Geräte im Ordner nicht mehr mit der neuen Gruppen-Konfiguration übereinstimmen und dies über den Gerätestatus entsprechend anzeigen.



Mehrere Gruppen-Konfigurationen verwenden

Innerhalb eines Ordners können mehrere Gruppen-Konfigurationen angelegt werden. Von diesen Gruppen-Konfigurationen darf jeweils nur eine aktiv sein, da sich der Gerätestatus nur auf eine einzelne Gruppen-Konfiguration beziehen kann. Aktive Gruppen-Konfigurationen sind mit einem blauen Häckchen, inaktive Gruppen-Konfigurationen mit einem roten Kreuz gekennzeichnet.Um eine Gruppen-Konfiguration zu aktivieren, klicken Sie mit der rechten Maustaste auf den Eintrag und wählen im Kontextmenü den Eintrag 'Aktiv'. Alle anderen Gruppen-Konfigurationen werden dabei automatisch deaktiviert.

Hinweis: Unterschiedliche Gruppenkonfigurationen in einem Ordner dürfen nicht auf die gleiche Teil-Konfigurationsdatei verweisen.



Übertragen von Gerätekonfigurationen auf ähnliche Modelle

Beim Wechsel auf einen anderen Gerätetyp ist es in manchen Fällen erwünscht, die Konfiguration des vorherigen Modells weitgehend zu übernehmen. Dazu bietet LANconfig die Möglichkeit, die Konfigurationsdatei (*.lcf) von einem Ausgangsgerät in ein ähnliches Zielgerät einzuspielen. Dabei werden alle Konfigurationsparameter, die sowohl im Ausgangs- wie auch im Zielgerät vorhanden sind, nach Möglichkeit mit den bisher verwendeten Werten belegt:

- Wenn das Zielgerät über den entsprechenden Parameter verfügt und der Wert im möglichen Bereich liegt, wird der Wert des Ausgangsgerätes übernommen.
- Wird der Wert eines vorhandenen Parameters im Zielgerät nicht unterstützt, wird der Standardwert verwendet. Beispiel:
  - Das Ausgangsgerät verfügt über vier Ethernetschnittstellen.
  - Das Zielgerät verfügt nur über zwei Ethernetschnittstellen.
  - Die Schnittstelle für ein IP-Netzwerk ist im Ausgangsgerät auf LAN-4 eingestellt.
  - Dieser Wert wird im Zielgerät nicht unterstützt. Daher wird der Wert beim Einspielen der Konfigurationsdatei auf den Standardwert 'LAN-1' gesetzt.
- Alle Parameter im Zielgerät, die im Ausgangsgerät nicht vorhanden sind, behalten ihren jeweiligen Wert bei.

Handlungsschritte

So gehen Sie vor, um die Konfiguration auf ein neues Gerät zu übertragen:

1. Bringen Sie nach Möglichkeit das Ausgangs- und das Zielgerät auf den gleichen Firmware-Stand. Jede neue HiLCOS-Firmware enthält neue Parameter. Mit der gleichen Firmware auf beiden Geräten erzielen Sie die größtmögliche Übereinstimmung bei den verfügbaren Parametern.
2. Speichern Sie die Konfiguration des Ausgangsgerätes mit LANconfig z. B. über **Gerät** > **Konfigurations-Verwaltung** > **Als Datei sichern**.
3. Trennen Sie das Ausgangsgerät vom Netzwerk, um Adresskonflikte zu vermeiden.
4. Spielen Sie die Konfiguration über **Gerät** > **Konfigurations-Verwaltung** > **Aus Datei wiederherstellen** in das Zielgerät ein. Die Meldungen über die Konvertierung der Konfiguration werden in einem Info-Dialog angezeigt.

Hinweis: Bitte beachten Sie, dass diese Funktion in erster Linie für den Ersatz von Geräten gedacht ist und nicht für die Konfiguration von neuen Geräten, die parallel im gleichen Netz wie das Ausgangsgerät betrieben werden sollen. Da auch die zentralen Kommunikationseinstellungen wie z. B. die IP-Adresse des Gerätes und die DHCP-Einstellungen auf das Zielgerät übertragen werden, kann der parallele Betrieb von Ausgangs- und Zielgerät in einem Netzwerk zu unerwünschten Situationen führen. Für die Konfiguration von mehreren Geräten in einem Netzwerk steht die Gruppenkonfiguration oder die Konfiguration über Skripte zur Verfügung.

Automatische Sicherung der Gerätekonfiguration

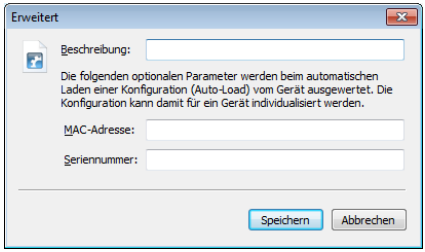
LANconfig kann vor Änderungen der Firmware oder der Konfiguration automatisch Backups der aktuellen Konfiguration speichern. Die globalen Einstellungen dazu, die für alle Geräte verwendet werden, finden Sie unter **Extras** > **Optionen** auf der Seite **Sicherung** (siehe *Sicherung* auf Seite 300).

Für die einzelnen Geräte können ergänzend spezielle Sicherungseinstellungen definiert werden. Klicken Sie dazu auf das entsprechende Gerät mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaften** > **Sicherung** (siehe *Sicherung* auf Seite 264).

Erweiterte Meta-Daten für Konfigurationsdateien

LANconfig bietet beim (manuellen) Speichern einer Geräte-Konfiguration die Möglichkeit, zusätzlich zu den üblichen Meta-Daten erweiterte Meta-Daten – bestehend aus MAC-Adresse und/oder Geräte-Seriennummer – in der Konfigurationsdatei (*.lcf) zu erfassen. Diese erweiterten Meta-Daten werden dann z. B. beim Quick Config Rollback oder Laden einer Gerätekonfiguration via USB berücksichtigt.

Um die erweiterten Meta-Daten in eine Konfigurationsdatei mit aufzunehmen, klicken Sie im Datei-speichern-Dialog von LANconfig auf die Schaltfläche **Erweitert** und geben die Daten – sofern nicht bereits vorausgefüllt – in die jeweiligen Felder ein.



Alternativ haben Sie auch die Möglichkeit, eine lcf-/lcs-Datei in einem Texteditor zu öffnen und die erweiterten Meta-Daten nachträglich von Hand zu ergänzen. Ergänzen Sie dazu die Zeile `(<Firmware>)(<Feature-Mask>;<Feature-IDs>;<Hardware-Mask>)` um die Klammer `(MAC:<MAC-Address>;SERIAL:<Serialnumber>)`.

Beispiel:

```
(Konfiguration von 'DEVICE-01' vom 12.08.2014)
(9.00.0212) (0x0000c010,IDs:4,e,f,2b;0x0c000002)
(MAC:00a0571d12fc;SERIAL:4002578718100036)
```

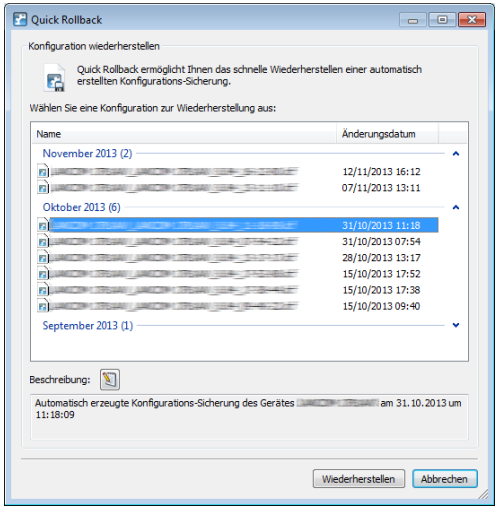
Quick Rollback

Als Ergänzung zur automatischen Sicherung der Gerätekonfiguration haben Sie die Möglichkeit, die gesicherte Konfigurationen mit nur einem Klick wiederherzustellen. Dazu markieren Sie in der Geräteansicht das gewünschte

Gerät und wählen **Gerät** > **Quick Rollback**, um die Funktion für das Quick Config Rollback aufzurufen. LANconfig listet Ihnen daraufhin alle geeigneten Gerätekonfigurationen auf, die sich unter dem Pfad für die automatischen Sicherung der Gerätekonfiguration befinden. Sofern LANconfig für das ausgewählte Gerät keine Sicherungsdatei finden kann, bricht diese Aktion mit einer Warnmeldung ab.

Wichtig: LANconfig nutzt für die Zuordnung von Konfigurationssicherungen zum betreffenden Gerät die in den Meta-Daten hinterlegte Seriennummer. Ab HiLCOS 8.90 wird diese bei der automatischen Sicherung miterfasst; in älteren Konfigurationssicherungen ohne Seriennummer müssen Sie diese jedoch manuell ergänzen, damit Quick Rollback die Dateien erkennt. Lesen Sie dazu auch *Erweiterte Meta-Daten für Konfigurationsdateien* auf Seite 238.

Um eine Konfigurationssicherung wiederherzustellen, markieren Sie einen Eintrag und klicken auf **Wiederherstellen**.



Darüber hinaus haben Sie die Möglichkeit, die Konfigurationssicherungen mit zusätzlichen Kommentaren zu versehen bzw. die darin enthaltenen Kommentare zu bearbeiten und ggf. zu ergänzen: Über die Schaltfläche **Beschreibung bearbeiten** () aktivieren Sie das darunterliegende Kommentarfeld, um den darin enhaltenen Text zu bearbeiten. Über die Schaltfläche **Beschreibung**

speichern (💾) schreiben Sie den Text des Kommentarfeldes anschließend in die Sicherungsdatei.

CSV-Export

Exportieren Sie die Liste der im Netz gefundenen Geräte, um diese später bequem in einem Durchgang wieder in LANconfig zu importieren. LANconfig speichert die Liste der verwalteten Geräte in einer CSV-Datei.

Für den Datenexport gehen Sie wie folgt vor:

1. Wählen Sie im Menü **Datei** > **Geräte-Liste exportieren**.
2. Bestimmen Sie den Speicherort der Datei.
3. Geben Sie einen Dateinamen an.
4. Bestimmen Sie das Spalten-Trennzeichen, welches die jeweiligen Geräteparameter trennt.
5. Starten Sie die Sicherung mit Klick auf **Speichern**.
6. Ein Dialog bestätigt die Anzahl der gespeicherten Geräte-Datensätze.
7. Schließen Sie diesen Dialog mit Klick auf **OK**.

Die erzeugte CSV-Datei enthält folgende Daten (ein Datensatz pro Zeile):

```
DEVICE_PATH;DEVICE_INTERFACE;DEVICE_TIMEOUT;DEVICE_ADDRESS;
DEVICE_ADMIN;DEVICE_PASSWORD;DEVICE_SNMPCOMMUNITY;DEVICE_NAME;
DEVICE_STARTUP;DEVICE_PROTOCOLS;DEVICE_PORTS;DEVICE_DESCRIPTION;
DEVICE_COMMENT;DEVICE_LOCATION;DEVICE_TYPE;DEVICE_EXTENDED_NAME;
DEVICE_PRODUCTCODE;DEVICE_SERNO;DEVICE_HWADDR;DEVICE_HWREL;
DEVICE_BACKUP;DEVICE_VPN;DEVICE_SSH_FINGERPRINT;DEVICE_CREDENTIALS

MyGroup;IP;3;192.168.2.105;;;;BAT-R;1;263;;;;;BAT-R;BAT-R;
BAT-REUWW9AKC99BO7T1SB9DHH08.60.0245;942070999000000157;ece55524d4ac;
0;"31;C:\Users\MyUser\AppData\Roaming\Hirschmann\LANconfig\Config\;
\%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s;12|";;
FE:20:2B:8A:BD:AD:71:13:E4:6B:16:BF:24:5D:FC:BA;
```

Die erste Zeile enthält die Namen der Geräte-Parameter. Darunter sind zeilenweise die einzelnen Geräte aufgeführt, deren Parameter jeweils durch Semikolons voneinander getrennt sind. Folgen 2 Semikolons direkt aufeinander, ist der eingeschlossene Parameter-Wert leer.

Die Variablen-Namen der ersten Zeile entsprechen den folgenden LANconfig-Einträgen:

- **DEVICE_PATH**: Pfad-Name in der Ordner-Ansicht
- **DEVICE_INTERFACE**: Anschlussart
- **DEVICE_TIMEOUT**: Maximale Antwortzeit des Gerätes
- **DEVICE_ADDRESS**: IP-Adresse oder Domain-Name und COM-Port oder Rufnummer
- **DEVICE_ADMIN**: Administrator-Name
- **DEVICE_PASSWORD**: Administrator-Passwort
- **DEVICE_SNMPCOMMUNITY**: SNMP Community des Gerätes
- **DEVICE_NAME**: Gerätename
- **DEVICE_STARTUP**: Überprüfung des Gerätes beim Start
- **DEVICE_PROTOCOLS**: Kommunikationsprotokolle
- **DEVICE_PORTS**: Ports
- **DEVICE_DESCRIPTION**: Beschreibung
- **DEVICE_COMMENT**: Kommentar
- **DEVICE_LOCATION**: Einsatz-Ort
- **DEVICE_TYPE**: Gerätetyp
- **DEVICE_EXTENDED_NAME**: Gerätename, ergänzt um eventuelle Zusätze
- **DEVICE_PRODUCTCODE**: Produkt-Code
- **DEVICE_SERNO**: Seriennummer
- **DEVICE_HWADDR**: MAC-Adresse
- **DEVICE_HWREL**: Hardware-Release
- **DEVICE_BACKUP**: Speicherort des von LANconfig angelegten Konfigurations-Backups
- **DEVICE_VPN**: Parametersatz für 1-Click-VPN
- **DEVICE_SSH_FINGERPRINT**: Zwischengespeicherter Fingerprint des eingespielten SSH-Schlüssels
- **DEVICE_CREDENTIALS**: Zwischengespeicherter Fingerprint des geräteinternen ssh-rsa-Schlüssels

Hinweis: Verwalten Sie die Liste der exportierten Geräte mit einem Text-Editor oder komfortabler in einer Tabellenkalkulation.

Hinweis: LANconfig speichert das Passwort unverschlüsselt in einer CSV-Datei, wenn LANconfig Zugangsdaten für den Zugriff auf Geräte enthält.

Denken Sie daran, diese Zugangsdaten in der Datei zu löschen, bevor Sie diese Datei weitergeben oder auf einem frei zugänglichen Server speichern.

Import aus einer Datenquelle (CSV)

Importieren Sie in LANconfig eine große Anzahl Geräte aus einer Skript-Vorlage gleichzeitig, indem Sie einen Import-Assistenten für entsprechende Geräte-Dateien verwenden. Zusätzlich haben Sie die Möglichkeit, mit dieser Geräte-Datei und einer Konfigurations-Vorlagendatei eine individuelle Konfigurationsdatei pro Gerät erstellen zu lassen. Die Vorlagendatei enthält Variablen für die Werte der Geräte-Datei.

Hinweis: Die Geräte-Datei ist im CSV-Format gespeichert.

Anwendungsbeispiel für den Import aus einer Datenquelle

Das in den nachfolgenden Unterkapiteln behandelte Szenario beschreibt, wie Sie anhand einer allgemeinen Skript-Datei und einer einfachen CSV-Geräte-Datei eine eigene Datenquelle für den Daten-Import erzeugen:

Inhalt der CSV-Datei

Die CSV-Datei enthält Datensätze von Geräten, die LANconfig importieren kann. Sie haben somit die Möglichkeit, diese komfortabel im Netzwerk zu verwalten.

Nachfolgend ein Beispiel einer einfachen CSV-Datei:

```
CONFIG_FILENAME;DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_LOCATION;DEVICE_NAME;KEY;USER
Fil52146.lcs;Filialen/NRW;IP;192.168.1.1;Wuerselen;Fil52146;secret1;user1@internet
Fil80637.lcs;Filialen/BAY;IP;192.168.2.1;Muenchen;Fil80637;secret2;user2@internet
```

Die erste Zeile enthält die Namen der Geräte-Parameter. Darunter sind zeilenweise die einzelnen Geräte aufgeführt, deren Parameter jeweils durch Semikolons voneinander getrennt sind. Folgen 2 Semikolons direkt aufeinander, ist der eingeschlossene Parameter-Wert leer.

Die Parameter-Bezeichnungen der ersten Zeile sind frei bestimmbar. Wenn Sie dennoch die verfügbaren Standardvariablennamen verwenden, ordnet

LANconfig die Geräte-Parameter beim Import automatisch zu. Eine Übersicht der Standardvariablen finden Sie im Kapitel *CSV-Export* auf Seite 240.

Wenn Sie keine Standardvariablennamen verwenden, ist es ggf. notwendig, dass Sie im Verlauf des Imports die Werte den entsprechenden Geräte-Eigenschaften in LANconfig zuordnen.

Inhalt der Konfigurations-Vorlagendatei

Die Vorlagendatei beinhaltet Telnet-Befehle, die Telnet der Reihe nach ausführt. Daher bezeichnet man diese Vorlagendatei auch als "Skript-Datei".

Hinweis: Eine Übersicht der verfügbaren Telnet-Befehle finden Sie im Referenzhandbuch-Kapitel *Terminalprogramm* auf Seite 53.

Eine Konfigurations-Vorlagendatei kann wie folgt aussehen:

```
lang English
flash No
set /Setup/Name "$DEVICE_NAME$"
set /Setup/SNMP/Location "$DEVICE_LOCATION$"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type
Rtg-tag Comment
add "INTRANET" $DEVICE_ADDRESS$ 255.255.255.0 0 any loose Intranet 0 "local
 intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username
 Rights
add "INTERNET" none PAP "$KEY$" 6 5 10 5 2 "$USER$" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type
user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active
Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes
```

```
# done
exit
```

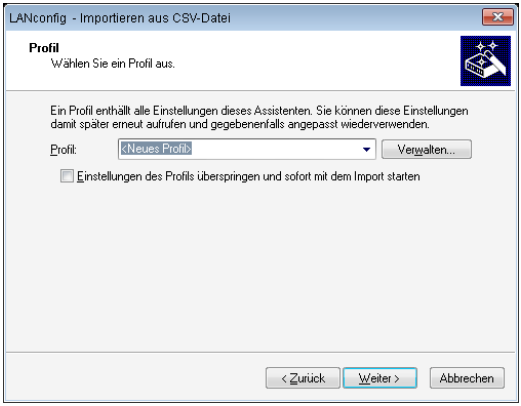
Die Variablen beginnen und enden mit einem Zeichen oder einer Zeichenfolge (hier: '$').

In dieser Vorlagendatei repräsentieren die Variablen bestimmte Geräte-Parameter. Während des Import-Vorgangs verknüpfen Sie diese Variablen mit den entsprechenden Einträgen der Geräte-Datei. Der Konfigurations-Assistent ersetzt die Variablen anschließend mit den zugewiesenen Geräte-Daten aus der CSV-Datei.

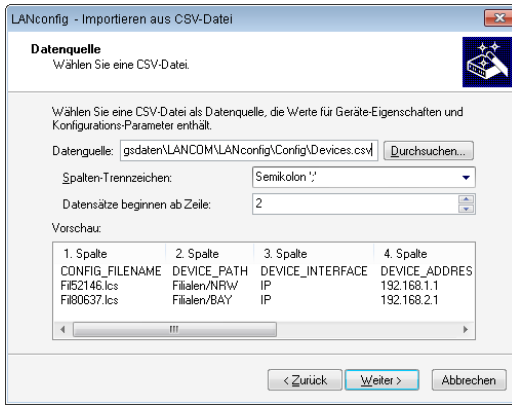
Anlegen von Konfigurationsdateien

Sie erstellen gerätespezifische Konfigurationsdateien wie folgt:

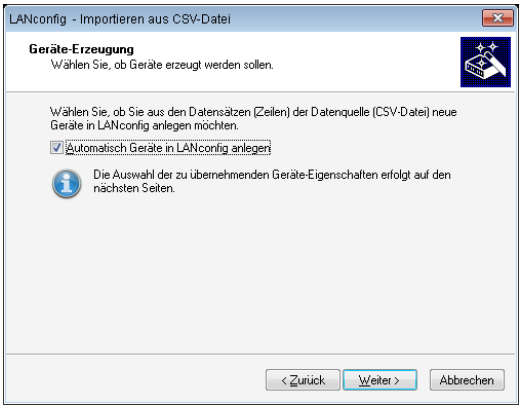
1. Öffnen Sie den Import-Assistenten im Menü über **Datei** > **Geräte/Konfigurationen aus CSV-Datei...**.
2. Bestätigen Sie ggf. den Begrüßungsdialog mit **Weiter**. Die Option **Diese Seite demnächst überspringen** blendet den Begrüßungsdialog beim zukünftigen Aufruf des Assistenten aus.
3. Wählen Sie ggf. das gespeicherte Profil eines vorherigen Datenimports. Mit der Option **Einstellungen des Profils überspringen und sofort mit dem Import starten** übernehmen Sie die Einstellungen des gewählten Profils ohne Änderungen. Um ein neues Profil statt eines vorhandenen Profils zu verwenden, wählen Sie **<Neues Profil>**. Klicken Sie auf **Weiter**.



4. Im Feld **Datenquelle** geben Sie den Pfad zur CSV-Datei an. Mit **Durchsuchen...** wählen Sie diese Datei im lokalen Dateisystem aus.

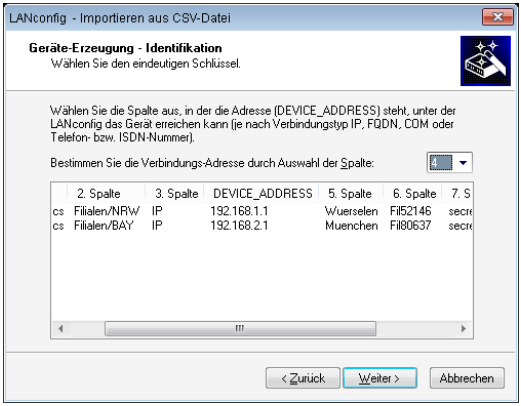


5. Sie können das Spalten-Trennzeichen der CSV-Datei wählen. Die Standardeinstellung ist das Semikolon.
6. Bestimmen Sie, ab welcher Zeile die Datensätze beginnen. Somit schließen Sie aus, dass Sie eventuell vorhandene Spaltentitel und mögliche Zusatzinformationen importieren. Enthält eine Zeile in der CSV-Datei ausschließlich Standardvariablennamen (siehe Abschnitt *Export von CSV-Datensätzen*), dann geschieht die Variablenzuordnung automatisch über diese Zeile. Damit ist gesichert, dass ein Export und der Import derselben Datei ohne manuelle Zuordnung funktioniert. Fügen Sie aber Variablen für die Konfigurationserzeugung hinzu, greift die Autoerkennung nicht.
7. Das Feld **Vorschau** zeigt sofort die anhand Ihrer ausgewählten Parameter zu importierenden Datensätze an. Bestätigen Sie Ihre Eingabe mit **Weiter**.
8. Um anhand der Datensätze neue Geräte in LANconfig anzulegen, aktivieren Sie die Option **Automatisch Geräte in LANconfig anlegen**. Nach einem Klick auf **Weiter** legen Sie auf den folgenden Seiten die Geräte-Eigenschaften fest, die Sie in LANconfig übernehmen.

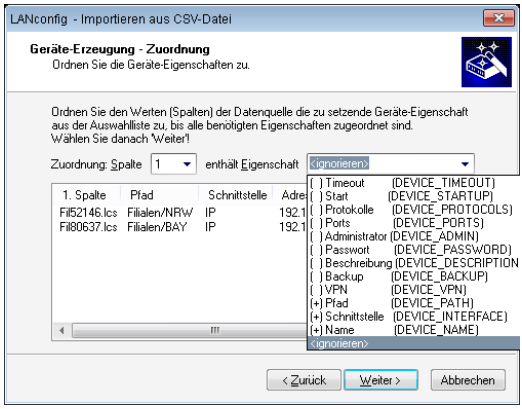


Hinweis: Bei deaktivierter Option überspringt der Assistent die folgenden 2 Schritte.

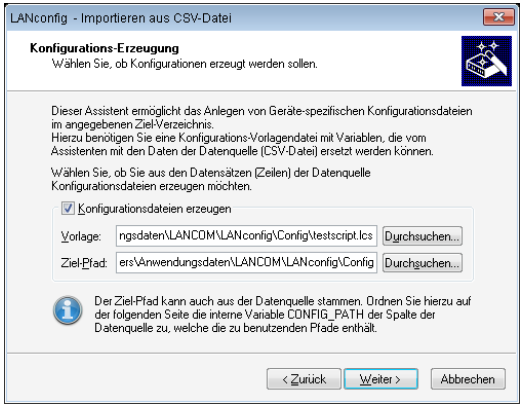
9. Die Identifikation der Geräte erfolgt über die Verbindungsadresse. Wählen Sie entsprechend in der Dropdown-Liste die Spalte des Datensatzes aus, die die Verbindungsadresse enthält, und klicken Sie auf **Weiter**. Bei Verwendung der Standardvariablennamen erfolgt diese Zuordnung automatisch.



10. Ordnen Sie die Spalten den Geräte-Eigenschaften zu. Zugeordnete Eigenschaften erkennen Sie in der Liste an dem vorangestellten "+". Klicken Sie danach auf **Weiter**. Bei Verwendung der Standardvariablennamen erfolgt diese Zuordnung automatisch.



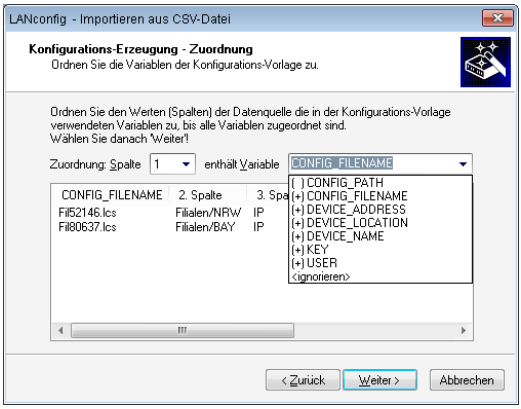
11. Sie haben die Möglichkeit, aus den Datensätzen individuelle Konfigurationsdateien zu erstellen. Aktivieren Sie dazu die Option **Konfigurationsdateien erzeugen**.



12. Bestimmen Sie im Feld **Vorlage** den Pfad zur Vorlagendatei, die als Basis für die individuellen Konfigurationsdateien vorgesehen ist. Mit Klick auf **Durchsuchen** öffnen Sie den Dialog zum Laden einer Konfigurations-Skript-Vorlage. In den Feldern **Variablen-Start** und **Variablen-Ende** definieren Sie, mit welchen Zeichen (oder Zeichenfolgen) die Variablen der Vorlagendatei beginnen und enden. Der Assistent identifiziert dadurch die Variablen der Vorlagendatei.

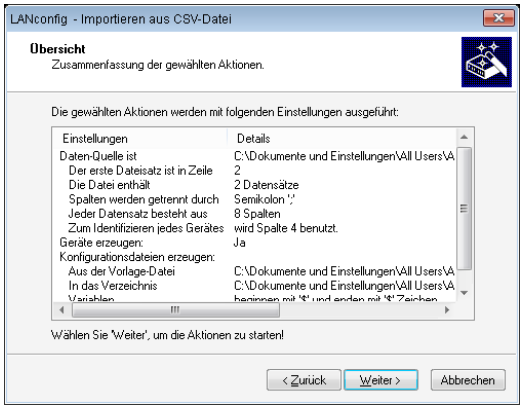
13. Im Feld **Ziel-Pfad** bestimmen Sie den Speicherpfad. Dort legt LANconfig die neuen Konfigurationsdateien ab. Klicken Sie auf **Durchsuchen**, um den Ziel-Pfad im lokalen Dateisystem festzulegen. Klicken Sie auf **Weiter**.

14. Ordnen Sie den Spalten der Datenquelle die in der Vorlagendatei verwendeten Variablen zu. Wählen Sie dazu die Spaltennummer aus der Spalten-Liste aus und weisen Sie dieser Nummer eine Variable aus der Variablen-Liste zu. Existieren im Spaltentitel dieselben Variablennamen, wie Sie sie im Skript zwischen den Start- und Endzeichen angegeben haben, erfolgt ebenfalls eine automatische Zuordnung für alle gefundenen Variablen. Die Spaltentitel in der Ansicht darunter aktualisieren sich sofort bei jeder Änderung. Klicken Sie anschließend auf **Weiter**.



Hinweis: Bei unvollständigen Angaben weist Sie der Assistent auf mögliche Probleme beim Import hin und bietet Ihnen Korrekturen an.

15. Die Zusammenfassung zeigt Ihnen an, welche Aktionen LANconfig im nächsten Schritt ausführt. Sind Änderungen nötig, klicken Sie auf **Zurück**. Sie gelangen somit in die entsprechende Eingabemaske. Mit Klick auf **Weiter** starten Sie den Daten-Import.



Hinweis: Falls Sie ein bereits in LANconfig existierendes Gerät durch den Datenimport überschreiben würden, gibt Ihnen der Assistent die folgenden Optionen zur Auswahl:

- Das betroffene Gerät überschreiben.
- Trotzdem eine Konfigurations-Datei erzeugen.
- Diese Entscheidungen für alle übrigen bereits vorhandenen Geräte übernehmen.

16. Der folgende Statusdialog ist ein Protokoll durchgeführter Aktionen. Mit Klick auf **Kopiere in Zwischenablage** speichern Sie die Statusmeldung in die Zwischenablage. Klicken Sie auf **Weiter**.
17. Zum Abschluss haben Sie die Möglichkeit, die aktuellen Import-Einstellungen für zukünftige Aktionen in einem Profil zu speichern.
18. Beenden Sie den Import mit Klick auf **Fertig stellen**.

Haben Sie die Erstellung einer individuellen Konfigurationsdatei ausgewählt, so speichert der Assistent im angegebenen Ordner je Gerät eine separate Konfigurationsdatei. Diese Konfigurationsdateien werden gemäß dem Dateinamen "<CONFIG_FILENAME>.lcs" benannt, den die CSV-Datei definiert:

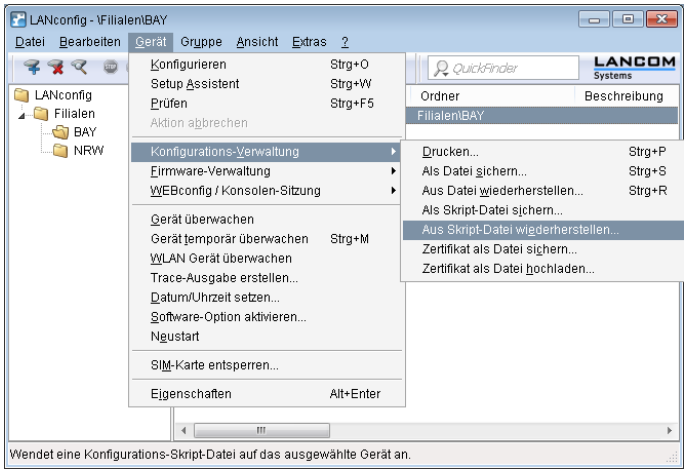
```
lang English
flash No
set /Setup/Name "Fil52146"
```

```
set /Setup/SNMP/Location "Wuerselen"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID Interface Src-check Type
Rtg-tag Comment
add "INTRANET" 192.168.1.1 255.255.255.0 0 any loose Intranet 0 "local
intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try Conf Fail Term Username
 Rights
add "INTERNET" none PAP "secret1" 6 5 10 5 2 "user1@internet" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI ATM-VCI MAC-Type
user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local 000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance Masquerade Active
Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes "default route"
cd /
flash Yes

# done
exit
```

Der Assistent hat alle Variablen durch die entsprechenden Geräte-Daten ersetzt.

Mit dieser Konfigurationsdatei haben Sie die Möglichkeit, die per Vorlagendatei definierten Geräte-Einstellungen mit LANconfig in weitere Geräte zu übertragen. Markieren Sie dazu das entsprechende Gerät und klicken Sie auf **Gerät** > **Konfigurations-Verwaltung** > **Aus Skript-Datei wiederherstellen**.



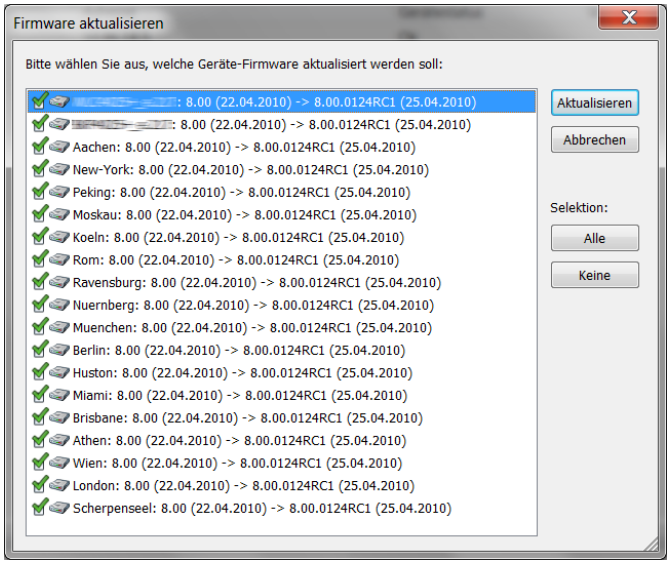
Suche nach Firmware-Updates im Archiv

Um das Update auf neue Firmwareversionen in den Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen Modelle und HiLCOS-Versionen idealerweise in einem zentralen Archiv-Verzeichnis abgelegt. Die Suche nach neuen Firmware-Versionen in diesem Verzeichnis kann entweder manuell angestoßen werden oder nach jedem Start von LANconfig automatisch durchgeführt werden.

Automatische Suche nach Firmware-Updates

Das Verzeichnis, in dem LANconfig nach den Updates sucht, konfigurieren Sie unter **Extras** > **Optionen** > **Update** > **Firmware-Archiv**.

Wenn Sie ein Intervall für die automatische Suche nach Optionen festlegen, zeigt LANconfig nach dem Start automatisch die Geräte an, für die neue Updates zur Verfügung stehen.

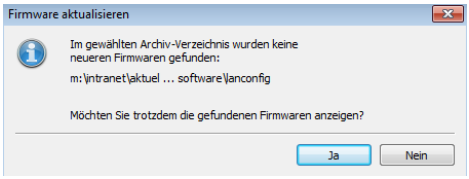


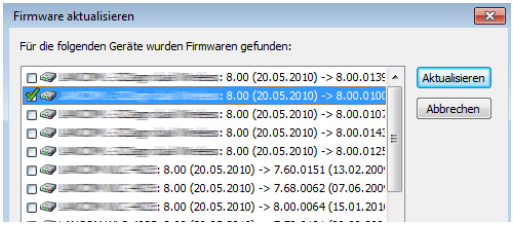
Manuelle Suche nach Firmware-Updates

Für die manuelle Suche nach Firmware-Updates klicken Sie mit der rechten Maustaste auf einen markierten Eintrag in der Geräteliste und wählen im Kontextmenü den Punkt **Firmware-VerwaltungIm lokalen Firmware-Archiv auf Update prüfen**. Wenn Sie mehrere Geräte markiert haben, erscheint der Punkt **Im lokalen Firmware-Archiv auf Update prüfen** direkt im Kontextmenü.

Komplette Liste der Firmware-Versionen einsehen

Wenn bei der Suche im Archiv keine neueren Firmware-Versionen gefunden wurden, können Sie alternativ die komplette Liste alle gefundenen Firmware-Dateien ansehen. So können Sie u. a. auch auf ältere Versionen zurückschalten. LANconfig zeigt alle gefundenen Versionen für alle markierten Geräte an, dabei auch den aktuellen Versionsstand der Geräte. Für jedes Gerät können Sie genau eine Firmware-Version auswählen, die dann in das Gerät eingespielt wird.





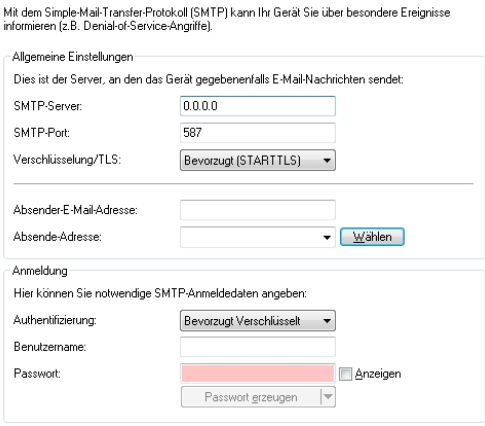
Einrichtung einer E-Mail-Adresse für den Nachrichtenversand

Bei bestimmten Ereignissen können Sie im Gerät festlegen, dass es eine Nachricht an eine definierte E-Mail-Adresse versendet. Diese Ereignisse können z. B. sein:

- Informationen über Verbindungsabbrüche auf einer WAN-Schnittstelle
- Meldungen der Firewall oder des Content-Filters
- Versand von VPN-Profilen

Die E-Mail-Adresse richten sie wie folgt ein:

Im Konfigurationsdialog von LANconfig können Sie die E-Mail-Adresse unter **Meldungen** > **SMTP-Konto** konfigurieren.



SMTP-Server: Geben Sie in diesem Feld die IP-Adresse des SMTP-Servers an.

SMTP-Port: Standardmäßig ist hier der Port 587 für unverschlüsselt übertragene E-Mails voreingestellt.

Verschlüsselung/TLS: Bestimmen Sie hier, ob und wie das Gerät die Verbindung verschlüsseln soll. Die möglichen Werte haben folgende Bedeutung:

- **Keine**: Keine Verschlüsselung. Das Gerät beachtet eine ggf. vom Server gesendete STARTTLS-Antwort nicht.
- **Verschlüsselt (SMTPS)**: Das Gerät verwendet SMTPS, verschlüsselt also ab Verbindungsaufbau.
- **Bevorzugt (STARTTLS)**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server STARTTLS an, verschlüsselt das Gerät. Diese Einstellung ist der Defaultwert.
- **Erforderlich (STARTTLS)**: Der Verbindungsaufbau erfolgt unverschlüsselt. Bietet der SMTP-Server kein STARTTLS an, überträgt das Gerät keine Daten.

Absender-E-Mail-Adresse: Geben Sie hier eine gültige E-Mail-Adresse ein, die das Gerät als Absender-Adresse verwendet. An diese Adresse versendet der angegebene SMTP-Server z. B. Nachrichten bei Zustellproblemen. Ist diese Adresse nicht angegeben oder ungültig, kann ein entsprechend konfigurierter SMTP-Server die Zustellung von Nachrichten verweigern.

Absende-Adresse: Optional können Sie hier eine alternative Absende-Adresse bestimmen, die das Gerät verwenden soll. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absender-Adressen angeben. Das Feld akzeptiert verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse das Gerät einsetzen soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ. Falls es eine Schnittstelle mit Namen "DMZ" gibt, nutzt das Gerät deren Adresse.
- "LB0"..."LBF" für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IP-Adresse in der Form `x.x.x.x`.

Authentifizierung: Bestimmen Sie hier, ob und wie sich das Gerät beim SMTP-Server authentifizieren soll. Die möglichen Werte haben folgende Bedeutung:

- **Keine**: Grundsätzlich keine Authentifizierung.
- **Bevorzugt Klartext**: Die Authentifizierung erfolg im Klartext (PLAIN, LOGIN), wenn der Server eine Authentifizierung verlangt. Ist keine Klartext-Authentifizierung vorgesehen, verwendet das Gerät eine sichere Authentifizierung.
- **Bevorzugt Verschlüsselt**: Eine sichere Authentifizierung findet statt, wenn sie möglich ist. Ansonsten verwendet das Gerät je nach Server-Einstellung eine Klartext- oder gar keine Authentifizierung.
- **Verschlüsselt**: Die Authentifizierung erfolgt mit verschlüsselter Übertragung des Passwortes (z. B. CRAM-MD5), wenn der Server eine Authentifizierung verlangt. Eine Klartext-Authentifizierung findet nicht statt.

Benutzername: Geben Sie hier den Benutzernamen ein, mit dem sich das Gerät am SMTP-Server anmelden soll.

Passwort: Geben Sie hier das Passwort ein, mit dem sich das Gerät am SMTP-Server anmelden soll.

Über RADIUS in die HiLCOS-Verwaltungsoberfläche einloggen

Aktuell können sich Benutzer über RADIUS, TACACS+ oder die interne Benutzerverwaltung des Gerätes in die Verwaltungsoberfläche eines Gerätes einloggen. Mit RADIUS ist das für folgende Protokolle möglich:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Hinweis: Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

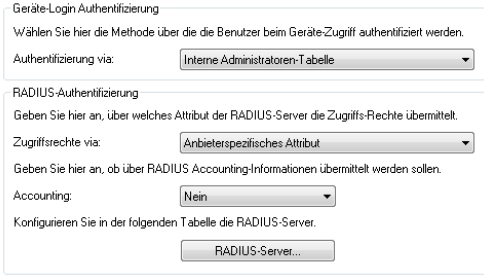
Hinweis: Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im Gerät gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Autorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netz-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

1. Bei der Anmeldung sendet das Gerät die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im Gerät gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem Gerät eine entsprechende Nachricht, und das Gerät bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem Gerät mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das Gerät die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und – wenn vorhanden – den genutzten Port.

Im LANconfig können Sie die Authentifizierungsmethode unter **Management** > **Authentifizierung** festlegen.



Geräte-Login Authentifizierung

Im Abschnitt **Geräte-Login Authentifizierung** wählen Sie die Methode aus, über die sich Benutzer beim Zugriff auf die Verwaltungsoberfläche des Gerätes authentifizieren sollen:

Interne Administratoren-Tabelle

Das Gerät übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.

RADIUS

Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netz.

TACACS+

Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netz.

RADIUS-Authentifizierung

Im Abschnitt **RADIUS-Authentifizierung** geben Sie die notwendigen RADIUS-Server-Daten sowie zusätzliche Verwaltungsdaten an.

Zugriffssrechte via

Im RADIUS-Server ist die Autorisierung der Anwender gespeichert. Bei einer Anfrage sendet der RADIUS-Server die Zugriffs- und Funktionsrechte zusammen mit den Login-Daten an das Gerät, das daraufhin den Anwender mit entsprechenden Rechten einloggt.

Normalerweise sind Zugriffsrechte im RADIUS Management-Privilege-Level (Attribut 136) festgelegt, sodass das Gerät den übertragenen Wert nur auf die internen Zugriffsrechte zu mappen braucht. Es kann jedoch auch sein, dass der RADIUS-Server zusätzlich Funktionsrechte übertragen

soll oder das Attribut 136 bereits anderweitig bzw. andere, herstellerspezifische Attribute für die Autorisierung verwendet. In diesem Fall kann das Gerät auch eine herstellerabhängige Autorisierung auswerten.

- **Anbieterspezifisches Attribut**: Das Gerät wertet das anbieterspezifische Attribut aus.
- **Management-Privilege-Level-Attribut**: Das Gerät wertet das Management-Privilege-Level-Attribut des RADIUS-Servers aus.
- **Shell-Privilege Attribut**: Das Gerät wertet das Shell-Privilege Attribut des RADIUS-Servers aus.

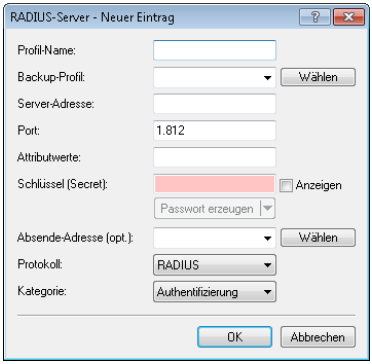
Accounting

Hier bestimmen Sie, ob das Gerät die Sitzung des Anwenders aufzeichnet.

- **Nein**: Das Gerät zeichnet die Sitzung nicht auf.
- **Ja**: Das Gerät zeichnet die Sitzung auf (Start, Ende, Benutzername, Authentifizierungsmodus, Port).

RADIUS-Server

In dieser Tabelle können Sie die Einstellungen für den RADIUS-Server vornehmen



Profil-Name

Vergeben Sie hier einen Namen für den RADIUS-Server.

Backup-Profil

Geben Sie den Namen des alternativen RADIUS-Servers an, an den das Gerät Anfragen weiterleitet, wenn der erste RADIUS-Server nicht erreichbar ist.

Hinweis: Für den Backup-Server müssen Sie einen weiteren Eintrag in der Server-Tabelle vornehmen.

Server-Adresse

Vergeben Sie hier die IPv4-Adresse des RADIUS-Servers.

Port

Geben Sie hier den Port an, über den der RADIUS-Server mit dem Gerät kommuniziert.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Shared Secret

Geben Sie hier das Kennwort für den Zugang zum RADIUS-Server an und wiederholen Sie es im zweiten Eingabefeld.

Absende-Adresse

Hier können Sie optional eine Absende-Adresse festlegen, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.

Protokoll

Geben Sie hier das Protokoll an, mit dem der RADIUS-Server mit dem Gerät kommuniziert.

Kategorie

Bestimmen Sie, für welche Kategorie der RADIUS-Server gelten soll.

3.1.3 Die Menüstruktur in LANconfig

Über die Menüleiste können Sie Geräte und deren Konfigurationen verwalten sowie das Aussehen und die Funktionsweise von LANconfig anpassen.

Datei

Unter diesem Menüpunkt verwalten Sie Geräte allgemein und beenden LANconfig.

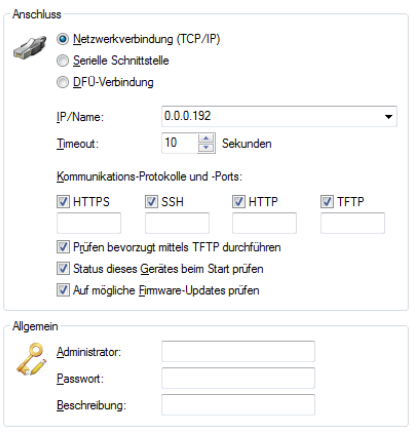
Gerät hinzufügen

Über **Datei** > **Gerät hinzufügen** fügen Sie der Geräteübersicht ein neues Gerät hinzu. Es öffnet sich ein Dialog, in dem Sie u. a. Einstellungen für die Verbindung zum das Gerät und die Sicherung vornehmen.

Allgemein

Auf dieser Seite legen Sie fest, wie sich LANconfig mit einem Gerät verbindet. Zudem können Sie die Zugangsdaten dauerhaft im Programm hinterlegen, um nicht nach jedem Start von LANconfig beim ersten Verbindungsaufbau die Daten manuell einzugeben.

Wichtig: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch LANconfig ausführen darf.



Anschluss

Im Bereich **Anschluss** nehmen Sie die Anschluss-Einstellungen für ein Gerät vor.

Wählen Sie hier aus, wie das Gerät erreichbar ist:

- **Netzwerkverbindung (TCP/IP)**: Wählen Sie diese Option, wenn das Gerät über ein IP-Netzwerk zu erreichen ist.
- **Serielle Schnittstelle**: Wählen Sie diese Option, wenn das Gerät über die serielle Schnittstelle dieses Computers angeschlossen ist.

- **DFÜ-Verbindung**: Wählen Sie diese Option aus, wenn Sie das Gerät über das DFÜ-Netzwerk erreichen wollen.

  Hinweis: Bitte beachten Sie, dass nicht jedes Gerät die Fernkonfiguration über eine DFÜ-Verbindung unterstützt.

- **IP/Name:**: Geben Sie die IP-Adresse des Gerätes an. Sie können auch einen Domain-Namen (DN oder FQDN) oder einen NetBIOS-Namen angeben. Dieser Name wird bei jedem Zugriff überprüft. LANconfig speichert und verwendet die dabei aufgelöste IP-Adresse. Sollte die Überprüfung einmal nicht möglich sein, greift LANconfig auf die letzte erfolgreich aufgelöste IP-Adresse zurück.
- **Timeout**: Geben Sie hier an, wieviele Sekunden das Programm auf Antworten von diesem Gerät warten soll.
- **HTTPS**, **SSH**, **HTTP**, **TFTP**: Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu verwenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.
- **Prüfen bevorzugt mittels TFTP durchführen**: Diese Option bewirkt, dass LANconfig ungeachtet der ausgewählten Protokolle bevorzugt mit TFTP prüft. Dies ist vorteilhaft bei Geräten, die im LAN erreichbar sind. Die Prüfung erfolgt schneller und belastet den Rechner weniger, was sich bei der Bearbeitung einer größeren Anzahl von Geräten bemerkbar macht. Die fehlende HTTPS-Verschlüsselung stellt im LAN keinen Nachteil dar.
- **Status dieses Gerätes beim Start prüfen**: Markieren Sie die Option, wenn LANconfig den Status des Gerätes beim Start prüfen soll.
- **Auf mögliche Firmware-Updates prüfen**: Markieren Sie die Option, wenn LANconfig auf mögliche Firmware-Updates prüfen soll.

Wie im Abschnitt *Kommunikationsprotokolle und Ports* auf Seite 263 erwähnt, testet LANconfig andere Protokolle und führt sie aus, wenn TFTP nicht verfügbar ist. Auch hier sind die globalen Einstellungen den gerätespezifischen übergeordnet.

Nachdem Sie die Einstellungen vorgenommen haben, versucht das Programm das Gerät zu erreichen und dessen Namen und Version abzufragen. Wenn dies fehlschlägt, zeigt LANconfig eine kurze Fehlermeldung in der Spalte **Status**.

Allgemein

In diesem Bereich hinterlegen Sie die Zugangsdaten und eine Beschreibung zum Gerät.

- **Administrator**: Geben Sie hier den Benutzernamen eines Administrators ein.
- **Passwort**: Geben Sie hier das zugehörige Passwort ein.
- **Beschreibung**: Geben Sie hier die Beschreibung des Gerätes ein, die LANconfig im Hauptfenster anzeigen soll.

Kommunikationsprotokolle und Ports

LANconfig führt sowohl die Prüfung der Geräte auf Erreichbarkeit als auch die Aktionen Firmware-Upload sowie Skript-/Konfigurations-Upload bzw. -Download über die hier ausgewählten Kommunikationsprotokolle durch.

LANconfig versucht in der Reihenfolge HTTPS, SSH, HTTP und TFTP und SSH, mit jedem gewählten Protokoll die oben aufgeführten Geräte-Aktionen auszuführen. Endet eine Aktion aufgrund des verwendeten Protokolls fehlerhaft, wiederholt LANconfig sie mit dem nächsten ausgewählten Protokoll.

Damit die Aktion überhaupt funktionieren kann, muss mindestens ein Protokoll ausgewählt sein.

Hinweis: Bei Verwendung von HTTP(S) und einem Proxyserver kann es notwendig sein, diesen Proxyserver zu umgehen, damit LANconfig die Geräte erreichen kann. In den Internetoptionen der Systemsteuerung von Windows können Sie den Proxyserver für lokale Adressen umgehen. In den erweiterten Einstellungen der Internetoptionen können Sie außerdem weitere Adressen definieren, die nicht über den Proxyserver kontaktiert werden sollen.

Zum Einstellen der Protokolle gibt es jeweils eine gerätespezifische und eine globale Einstellmöglichkeit. Die globalen Einstellungen im Options-Menü sind den gerätespezifischen übergeordnet. Dadurch ist es möglich, die einzelnen Protokolle mit Hilfe eines globalen Schalters für alle Geräte auszuschalten.

Tipps

- Wenn sich das Gerät noch im Auslieferungszustand befindet, hat es noch keine eigene IP-Adresse. In diesem Fall geben Sie die IP-Adresse Ihres Computers ein und ersetzen Sie den letzten Abschnitt der Ziffernfolge durch '254': Wenn ihr Computer die IP-Adresse '192.168.1.1' hat, dann weisen Sie dem Gerät die IP-Adresse '192.168.1.254' zu.
- Wenn Sie nicht wissen, welche Adresse ein Gerät hat, können Sie auch danach über **Datei** > **Geräte** suchen.

Mögliche für Probleme beim Herstellen einer Verbindung mit einem neuen Gerät

Wenn LANconfig ein Gerät nicht erreicht, erscheint unter Status eine der unten aufgeführten Fehlermeldungen. Um ein Gerät erneut zu überprüfen, markieren Sie es in der Liste, und klicken Sie dann auf in der Menüleiste auf **Gerät** > **Prüfen**.

- **Serieller Fehler**: LANconfig konnte die serielle Schnittstelle nicht öffnen. Schließen Sie alle Programme, die möglicherweise darauf zugreifen.
- **IP-Fehler**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist und ob Ihr Computer korrekt mit dem Netzwerk verbunden ist. Stellen Sie außerdem sicher, dass das TCP/IP-Protokoll installiert und richtig konfiguriert ist.
- **Keine Antwort**: Überprüfen Sie, ob die IP-Adresse des Gerätes richtig ist. Möglicherweise ist auch die Netzwerkverbindung zwischen Ihrem Rechner und dem Gerät zu langsam oder unzuverlässig.
- **Status unbekannt**: LANconfig hat das Gerät zwar über die angegebene IP-Adresse erreicht, konnte jedoch keine weiteren Informationen abfragen. Möglicherweise unterstützt LANconfig dieses Gerät nicht.
- **Zugriff verweigert:** Das Gerät ist für den Zugriff von Ihrem Rechner aus gesperrt.

Sicherung

Auf dieser Seite aktivieren und konfigurieren Sie die gerätespezifischen Sicherungseinstellungen. Die dazugehörigen Einstellungsmöglichkeiten sind mit den globalen identisch (siehe *Sicherung* auf Seite 300).

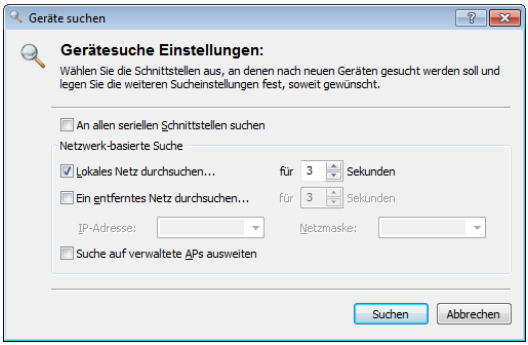
Gerät löschen

Wenn Sie ein Gerät markiert haben, können Sie es unter **Datei** > **Gerät löschen** entfernen. Sie können auch die Taste 'Entf' drücken, um ein Gerät zu löschen.

Hinweis: Mit dem Löschen entfernen Sie das Gerät nur aus der aktuellen Ansicht. Sie können es jederzeit wieder über **Datei** > **Gerät hinzufügen** oder **Datei** > **Geräte suchen** hinzufügen.

Geräte suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach neuen Geräten, um Sie der Geräteübersicht hinzuzufügen.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- An allen seriellen Schnittstellen
- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Hinweis: Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Geräte in dieser Ansicht prüfen

Unter **Datei** > **Geräte in dieser Ansicht prüfen** können Sie den Status von allen Geräten der aktuellen Ansicht abfragen. Der Gerätestatus zeigt z. B. an, dass eine neue Firmware hochgeladen wird oder ein Gerät nicht erreicht werden kann.

Hinweis: Gerät lassen sich nur konfigurieren, wenn der Gerätestatus **Ok** ist.

Alle Geräte-Firmwaren im lokalen Firmware-Archiv auf Updates prüfen

Startet manuell die automatische Suche nach Firmware-Updates. Dabei durchsuchen Sie Ihr lokales Firmware-Archiv nach aktuelleren Firmware-Versionen als derzeit den Geräten installiert.

Alle Aktionen abbrechen

Über diesen Menüpunkt brechen Sie alle laufenden Aktion für alle in der Ansicht gezeigten Geräte ab. Sie können diese Funktion nutzen, um z. B. das Laden einer Firmware oder eines Skripts abzubrechen. Insbesondere Vorgänge, die durch Mehrfachauswahl oder das Ausführen von Aktionen gestartetet wurden, können damit komplett gestoppt werden.

Geräte/Konfigurationen aus CSV-Datei

Importieren Sie in LANconfig eine große Anzahl Geräte aus einer Skript-Vorlage gleichzeitig, indem Sie einen Import-Assistenten für entsprechende Geräte-Dateien verwenden. Zusätzlich haben Sie die Möglichkeit, mit dieser Geräte-Datei und einer Konfigurations-Vorlagendatei eine individuelle Konfigurationsdatei pro Gerät erstellen zu lassen. Die Vorlagendatei enthält Variablen für die Werte der Geräte-Datei.

Weitere Informationen finden Sie im Abschnitt *Import aus einer Datenquelle (CSV)* auf Seite 242.

Geräte-Liste exportieren

Exportieren Sie die Liste der im Netz gefundenen Geräte, um diese später bequem in einem Durchgang wieder in LANconfig zu importieren. LANconfig speichert die Liste der verwalteten Geräte als CSV-Datei.

Weitere Informationen finden Sie im Abschnitt *Import aus einer Datenquelle (CSV)* auf Seite 242.

Neuer Ordner

Über diesen Menüpunkt legen Sie in der Verzeichnisstruktur einen neuen Ordner an. Siehe dazu auch *Verzeichnisbäume zur Organisation nutzen* auf Seite 214.

Beenden

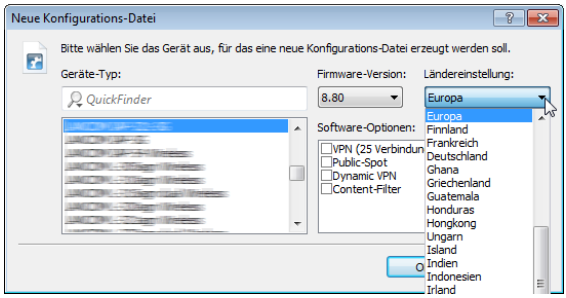
Über diesen Menüpunkt beenden und schließen Sie LANconfig.

Bearbeiten

Unter diesem Menüpunkt verwalten Sie die Konfigurations-Dateien aller Geräte in einer Geräteliste.

Neue Konfigurations-Datei

Mit dieser Funktion lassen sich eine Konfiguration und ein Geräte-Eintrag in der Geräteliste anlegen, ohne dass eine Verbindung zu einem real existierenden Gerät besteht.



Geräte-Typ

Wenn Sie eine Konfigurations-Datei anlegen wollen, müssen Sie angeben, für welches Gerät diese Konfiguration bestimmt ist, damit das Programm die richtigen Parameter für das Gerät anzeigen kann. Wählen Sie aus der Liste das von Ihnen gewünschte Gerät aus.

Hinweis: Nutzen Sie den QuickFinder, um die Liste der verfügbaren Geräte einzuschränken. Geben Sie dazu einen Teil des gewünschten Geräte-Typs in das QuickFinder-Feld ein, der Dialog reduziert die Auswahl automatisch auf die passenden Geräte.

Firmware-Version

Da verschiedene Firmware-Versionen oft voneinander abweichende Einstellungsmöglichkeiten bieten, muss das Programm wissen, für welche Version diese Konfiguration bestimmt ist. Geben Sie hier bitte die Versionsnummer der Firmware in dem gewünschten Gerät an. Das Programm wird Ihnen mitteilen, wenn diese Versionsnummer nicht korrekt ist oder nicht unterstützt wird

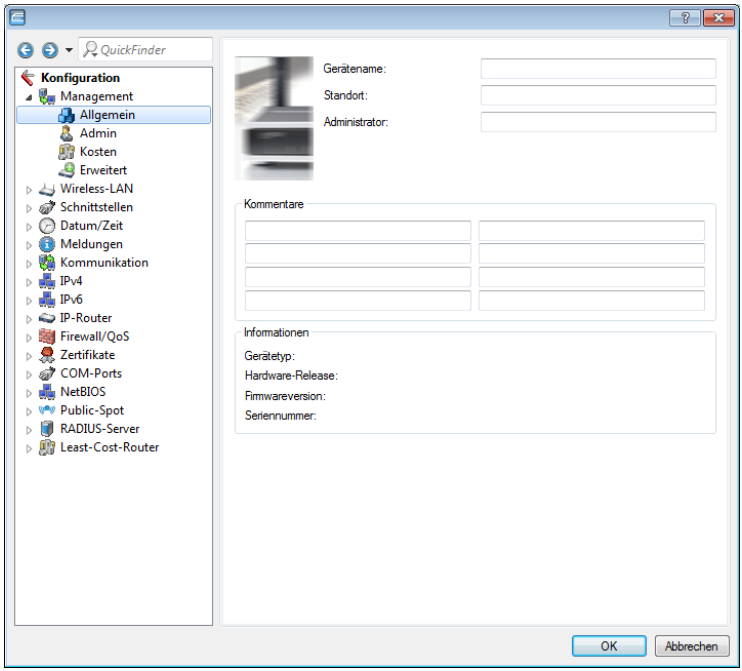
Ländereinstellung

Wählen Sie das Land bzw. die Region, für welche die Konfigurations-Datei gelten soll. Die Konfigurations-Datei bietet dann nur die Parameter an, welche in dem gewählten Land bzw. in der gewählten Region erlaubt sind.

Software-Optionen

Wählen Sie die entsprechenden Software-Optionen aus, die angezeigt werden sollen.

Mit einem Klick auf **OK** öffnet sich der Konfigurationsdialog.

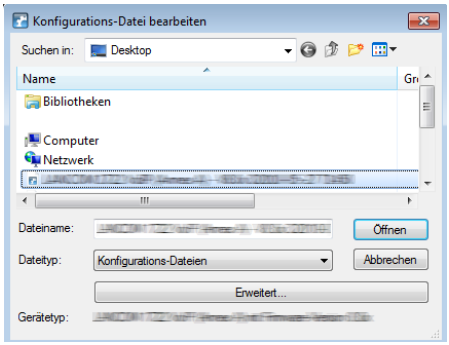


Hinweis: Sie können auch eine neue Konfigurationsdatei erstellen, indem Sie mit einem mit einem Rechtsklick auf Ihren Desktop im Kontext-Menü **Neu** > **LANconfig Konfiguration** auswählen.

Hinweis: Die Informationen zu den einzelnen Konfigurationsparametern finden Sie in der HiLCOS-Dokumentation.

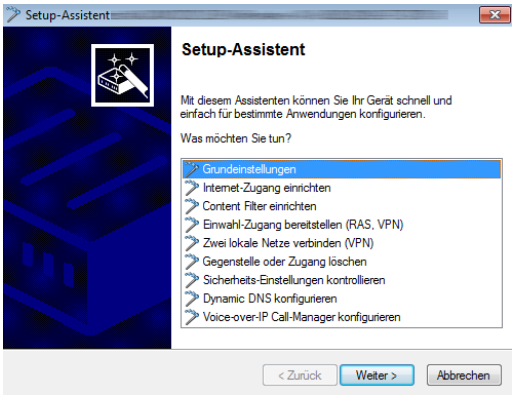
Konfigurations-Datei bearbeiten

Über diesen Menüpunkt wählen Sie eine gespeicherte Konfigurationsdatei aus, um sie im Kofigurationsdialog zu bearbeiten.



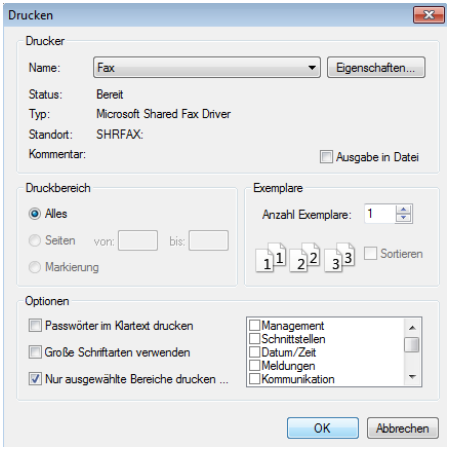
Konfigurations-Datei assistieren

Über diesen Menüpunkt wählen Sie eine gespeicherte Konfigurationsdatei aus, um sie mit dem Setup-Assistenten zu bearbeiten.



Konfigurations-Datei drucken

Über diesen Menüpunkt drucken Sie eine gespeicherte Konfigurationsdatei aus.



Zusätzlich zum normalen Druckdialog haben Sie im Abschnitt **Optionen** folgende Einstellungsmöglichkeiten:

Passwörter im Klartext drucken

Wenn Sie diese Funktion aktivieren werden Ihre Passwörter im Klartext gedruckt. Das Hauptgerätepasswort steht im Ausdruck auf der ersten Seite

Große Schriftarten verwenden

Der Ausrdruck erfolgt in einer größeren Schrift.

Nur ausgewählte Bereiche drucken

Drucken Sie nur bestimmte Konfigurationsbereiche, z. B. nur WLAN-Controller.

Geräte in dieser Ansicht markieren

Über diesen Menüpunkt markieren Sie alle aktuellen Geräteeinträge in der gewählten Ansicht.

Markierung umkehren

Über diesen Menüpunkt kehren Sie die Markierung aller aktuellen Geräteeinträge in der gewählten Ansicht um. Dadurch werden alle Einträge, die vorher markiert waren, unmarkiert und alle Einträge, die vorher nicht markiert waren, markiert.

Gerät

Unter diesem Menüpunkt können Sie die Konfiguration von am Netzwerk angeschlossenen Geräten bearbeiten, Firmware-Updates verwalten und Geräteverbindungen überwachen.

Die dazugehörigen Funktionen sind nur auswählbar, wenn Sie mindestens ein Gerät in der Geräteliste markiert haben. Dieses Menü können Sie ebenfalls über die rechte Maustaste für ein markiertes Gerät aufrufen.

Konfigurieren

Lädt die Konfiguration des markierten Gerätes über die in den Eigenschaften definierten Anschluss-Einstellungen, insofern eine Verbindung auf diesem Weg möglich ist. Die Konfiguration wird dann im Fenster zur Konfigurations-Einstellung angezeigt und kann bearbeitet werden.

Setup Assistent

Lädt die Konfiguration des markierten Gerätes über die in den Eigenschaften definierten Anschluss-Einstellungen, insofern eine Verbindung auf diesem Weg möglich ist. Die Konfiguration wird dann im Setup Assistent geöffnet, welcher Ihnen bei der Konfiguration ausgewählter Einsatzszenarien behilflich ist.

Hinweis: Bei WLCs mit “WLC High Availability Clustering XL-Option” ist es möglich, alle aufgeführten WLCs zu markieren und gemeinsam über den WLC-Clustering-Assistenten zu konfigurieren (siehe *1-Klick WLC High Availability Clustering-Assistent*).

Quick Rollback

Über diesen Menüpunkt haben Sie die Möglichkeit, automatisch erstelle Konfigurationssicherungen für das ausgewählte Gerät mit nur einem Klick wiederherzustellen und die Gerätekonfiguration somit auf einen früheren Konfigurationsstand zurückzusetzen. Mehr zu dieser Funktion erfahren Sie unter *Quick Rollback* auf Seite 238.

Prüfen

Prüft die Geräte bzw. die Auswahl an Geräten durch Auslesen der Geräte-Information über den ausgewählten Anschluss. Aus dem Verlauf dieser Operation wird der Status generiert. Der Gerätestatus zeigt z. B. an, dass eine neue Firmware hochgeladen wird oder ein Gerät nicht erreicht werden kann.

Hinweis: Gerät lassen sich nur konfigurieren, wenn der Gerätestatus **Ok** ist.

Aktion abbrechen

Über diesen Menüpunkt brechen Sie eine laufende Aktion für das ausgewählte Gerät ab. Sie können diese Funktion nutzen, um z. B. das Laden einer Firmware oder eines Skripts abzubrechen. Aktionen auf anderen Geräten, die noch nicht abgeschlossen sind, laufen jedoch weiter.

Konfigurations-Verwaltung

Mit den Funktionen zur Konfigurations-Verwaltung können Sie Konfigurationen sichern und wiederherstellen, und so z. B. die Konfiguration eines Gerätes in ein anderes übertragen. Wenn die Firmware-Versionen der beiden Geräte verschieden sind, zeigt Ihnen das Programm die Unterschiede in der Konfiguration und warnt Sie davor, dass Parameter verloren gehen. Darüber hinaus erfolgt über diesen Menüpunkt auch das Dateimanagement, bei dem Sie besondere Dateien wie Templates oder Zertifikate direkt in das Gerät laden.

Folgende konfigurationsspezifische Aktionen stehen Ihnen zur Auswahl:

Drucken

Lädt die Konfiguration des markierten Geräts über die in den Eigenschaften definierten Anschluss-Einstellungen, sofern eine Verbindung auf diesem Weg möglich ist. Im folgenden Druckdialog können dann dieselben Optionen zur Ausgabe wie unter **Bearbeiten** > **Konfigurations-Datei drucken** gewählt werden. Nach Bestätigung wird die Konfiguration ausgedruckt.

Als Datei sichern

Speichert die Konfiguration des ausgewählten Geräts an einem wählbaren Ort als Konfigurationsdatei. Geben Sie in dem Datei-Auswahldialog einen

Namen für die Konfigurationsdatei ein. Klicken Sie anschließend auf **Speichern**.

Aus Datei wiederherstellen

Lädt in das ausgewählte Gerät eine im Folgenden zu bestimmende Konfigurationsdatei (z. B. aus der automatischen Sicherung). Wählen Sie in dem Datei-Auswahldialog die gespeicherte Konfiguration aus, und klicken Sie auf **Öffnen**.

Als Skript-Datei sichern

Speichert die Konfiguration des ausgewählten Geräts an einem wählbaren Ort als Skript-Datei. Dabei können dieselben Optionen für Skript-Dateien wie unter den Sicherungseinstellungen gewählt werden.

Aus Skript-Datei wiederherstellen

Lädt in das ausgewählte Gerät eine im Folgenden zu bestimmende Skript-Datei (z. B. aus der automatischen Sicherung).

Zertifikat als Datei sichern

Bestimmen Sie in dem sich öffnenden Dialog, welches Zertifikat aus dem gewählten Gerät in einer Datei gesichert werden soll. Der Dateityp hängt von der Auswahl des Zertifikats ab.

Zertifikat oder Datei hochladen

Über diesen Menüpunkt laden Sie Zertifikate und besondere Dateien in das Gerät. Zertifikate benötigen Sie z. B. für eine VPN-Verschlüsselung oder den Betrieb eines WLAN-Controllers. Die 'besonderen Dateien' hingegen stellen Dateien dar, mit denen Sie geräteeigene Vorlagen ersetzen können (z. B. indidivuelle Templates für den Rollout-Assistenten) oder die Sie für die Nutzung bestimmter Funktionen ins Gerät laden müssen (z. B. Nutzungsbedingungen für das Public Spot Modul).

Hinweis: Sie können für jede Konfiguration, die Sie speichern, eine Beschreibung eingeben. So lassen sich bequem verschiedene Konfigurationen für verschiedene Geräte verwalten.

Firmware-Verwaltung

Über diesen Menüpunkt aktualisieren Sie die Geräte-Firmware oder schalten das Gerät auf eine andere Firmware-Version um. Folgende Firmware-spezifische Aktionen stehen Ihnen zur Auswahl:

Im lokalen Firmware-Archiv auf Update prüfen

Startet manuell die automatische Suche nach Firmware-Updates. Dabei durchsuchen Sie Ihr lokales Firmware-Archiv nach aktuelleren Firmware-Versionen als derzeit auf dem ausgewählten Gerät installiert.

Neue Firmware hochladen

Öffnet einen Datei-Auswahldialog, über den Sie eine bestimmte Firmware-Datei in das ausgewählte Gerät hineinladen können.

Hinweis: Weil die vorhandene Firmware eines Gerätes während des Uploads der neuen Firmware überschrieben wird, darf dieser Vorgang auf keinen Fall unterbrochen werden, da das Gerät anschließend möglicherweise nicht mehr lauffähig ist.

Im Testmodus laufende Firmware freischalten ([Speicherplatz-Nummer])

Sofern Sie für ein Gerät ein Firmware-Update durchgeführt und die zugehörige Firmware im (zeitlich beschränkten) Testmodus hochgeladen haben, können Sie über diesen Menüpunkt die Firmware dauerhaft aktivieren. Mehr zu der Funktion erfahren Sie im Abschnitt *FirmSafe* auf Seite 103.

1, 2 [Firmare-Version] vom [Datum]

Geräte mit FirmSafe sind dazu in der Lage, zwei Firmware-Versionen zu verwalten, um z. B. im Falle eines fehlgeschlagenen Updates oder bei Problemen auf die vorherige Firmware zurückzuschalten. Über die Speicherplatz-Nummern 1 und 2 haben Sie die Möglichkeit, einen Firmware-Stand auszuwählen und das Gerät mit einer anderen installierten Firmware zu starten.

Hinweis: Beachten Sie, dass bei einem Umschalten alle bestehenden Verbindungen beendet sowie alle Statistiken und Gebühreninformationen gelöscht werden.

WEBconfig / Konsolen-Sitzung

Über diesen Menüpunkt starten Sie eine neue Konfigurationssitzung über einen alternativen Konfigurationsweg. Folgende Konfigurationswege stehen Ihnen zur Auswahl:

Web-Browser starten

Öffnet die WEBconfig-Oberfläche für das markierte Gerät.

Hinweis: Unter **Extras** > **Optionen** > **Extras** > **Browser zur Darstellung von WEBconfig** können Sie auswählen, ob LANconfig zur Anzeige den Standardbrowser des Systems oder den internen Browser verwenden soll.

Telnet-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten Telnet-Client.

SSH-Sitzung öffnen

Öffnet eine Verbindung zum Gerät mit dem in den Einstellungen konfigurierten SSH-Client.

Gerät überwachen

Über diesen Menüpunkt aktivieren Sie die grundsätzliche Überwachung des Gerätes in LANmonitor.

Das Gerät wird dann in der Liste der zu überwachenden Geräte in LANmonitor ergänzt und liegt auch nach dem Öffnen und Schließen von LANmonitor wieder vor.

Gerät temporär überwachen

Über diesen Menüpunkt aktivieren Sie die temporäre Überwachung des Gerätes in LANmonitor.

Das Gerät wird in einem separaten Fenster von LANmonitor geöffnet. Die Einstellung wird nicht gespeichert, sodass LANmonitor das Gerät beim nächsten Start nicht automatisch wieder anzeigt. Lesen Sie hierzu auch *LANmonitor - Geräte im LAN überwachen* auf Seite 313.

WLAN Gerät überwachen

Über diesen Menüpunkt aktivieren Sie die Überwachung eines WLAN-Gerätes mit WLANmonitor. Lesen Sie hierzu auch *WLANmonitor - WLAN-Geräte überwachen* auf Seite 349

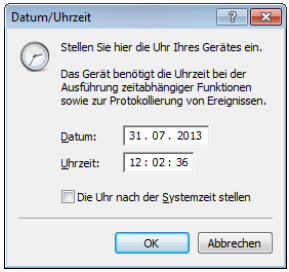
Trace-Ausgabe erstellen

Mit dieser Option starten Sie die Trace-Ausgabe in LANtracer.

Lesen Sie hierzu auch *LANtracer - Tracen mit LANconfig und LANmonitor* auf Seite 372.

Datum/ Uhrzeit setzen

Über diesen Menüpunkt setzen Sie das Datum und die Uhrzeit für das Gerät. Diese Aktion ist für einige Funktionen (z. B. Accounting) und Schritte im Setup Assistenten (z. B. Einrichtung eines Public Spots) zwingend erforderlich.



Wenn Sie die Option **Die Uhr nach der Systemzeit stellen** aktivieren, wird die Uhrzeit des Betriebssystems Ihres Computers übernommen.

Software-Option aktivieren

Wenn Sie zusätzliche Software-Optionen erworben haben, können Sie diese unter **Gerät** > **Software-Option aktivieren** aktivieren, indem Sie den Aktivierungsschlüssel eingeben.

Bereits aktivierte Optionen sehen Sie im Dialog **Gerät** > **Eigenschaften** > **Features & Optionen** ein. Lesen Sie hierzu auch *Features & Optionen* auf Seite 282.

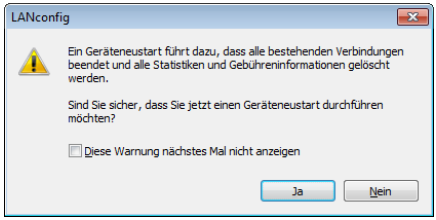
CC-Konformität prüfen

Über diesen Menüpunkt veranlassen Sie die Prüfung, ob die Konfiguration des ausgewählen Gerätes CC-konform ist.

Hinweis: Diese Aktion ist nur für CC-Geräte sinnvoll. Bei Nicht-CC-Geräten ruft diese Aktion stets eine Fehlermeldung hervor.

Neustart

Über diesen Menüpunkt veranlassen Sie einen Neustart des Gerätes.



Hinweis: Bei einem Neustart werden die Zugangsdaten für den Admin-Account abgefragt, insofern diese nicht für das Gerät hinterlegt sind.

Eigenschaften

Über diesen Menüpunkt öffnen Sie den Eigenschaften-Dialog des markierten Geräts, in dem sich auf verschiedenen Seiten gerätespezifische Einstellungen vornehmen oder einsehen lassen.

Allgemein

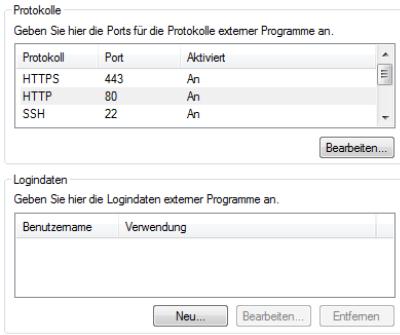
Auf dieser Seite nehmen Sie die gerätespezifischen Verbindungseinstellungen vor. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 261).

Protokolle & Logins

Auf dieser Seite konfigurieren und verwalten Sie die Protokolle, Ports und Zugangsdaten, welche die übrigen Bestandteile des LCMS beim Aufruf aus LANconfig heraus verwenden. Zu den konfigurierbaren Programmen gehören:

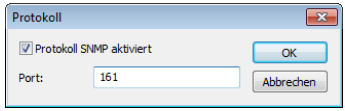
- LANmonitor
- LANtracer
- LCMS-interner sowie externer Webbrowser

Hinweis: Sofern im aufgerufenen Programm z. B. bestimmte Protokolle bereits deaktiviert bzw. anders konfiguriert sind, gelten ausschließlich die Übereinstimmungen.



Protokolle

Wählen Sie ein Protokoll aus und klicken Sie **Bearbeiten**, um das ausgewählte Protokoll zur Verwendung in externen Programmen zu erlauben oder zu verbieten und ggf. den Standard-Port zu verändern.



Logindaten

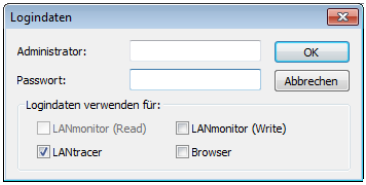
Hinterlegen Sie in diesem Bereich die Zugangsdaten für die externen Programme. Klicken Sie **Neu**, um ein oder mehrere Programm(e) auszuwählen und die dafür geltenden Zugangsdaten einzugeben. Je nach Auswahl fragt das Dialogfenster unterschiedliche Zugangsdaten ab. In jedem Fall haben Sie die Möglichkeit, sich mit dem Benutzernamen und Passwort Ihres Administrator-Zugangs zu authentisieren, wenn Sie das betreffende Programm aus LANconfig heraus aufrufen.

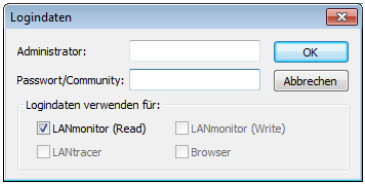
Im Falle von LANmonitor besteht für den reinen Lesezugriff (Read) die Möglichkeit, eine individuelle SNMP-Community anzugeben. Standardmäßig prüft LANconfig beim Öffnen einer Gerätekonfiguration, ob und in welchem Umfang Sie Zugangsdaten für externe Programme hinterlegt haben. Haben Sie für den Lesezugriff keine Zugangsdaten oder lediglich Zugangsdaten in Form einer SNMP-Community konfiguriert, übernimmt

LANconfig beim Programmaufruf von LANmonitor die SNMP-Community ersatzweise aus der geladenen Gerätekonfiguration. Sofern Sie in LANconfig eine Konfiguration bearbeiten und in dieser eine SNMP-Community setzen, speichert LANconfig die SNMP-Community automatisch für das betreffende Gerät. Durch dieses Komfortverhalten wird der Authentisierungsumfang für LANmonitor reduziert, sodass keine gesonderte Konfiguration des Lesezugriffs erforderlich ist.

Hinweis: LANconfig wertet für das oben beschriebene Komfortverhalten ausschließlich den Setup-Parameter 2.9.15 Read-Only-Community aus. Zusätzliche im Gerät konfigurierte, schreibgeschützte SNMP Communities bleiben unbeachtet.

Weitere Informationen zum SNMP-Zugriff über einzelne oder mehrere SNMP-Communities finden Sie im Abschnitt *Konfigurieren des SNMP-Lesezugriffs* auf Seite 140.





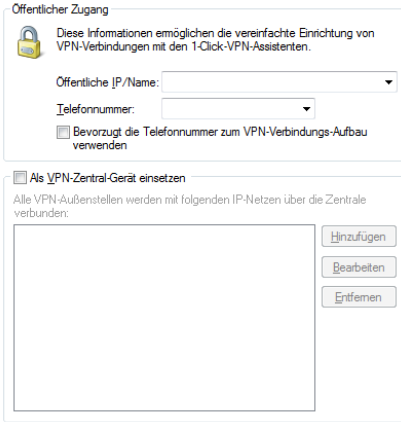
Sicherung

Auf dieser Seite aktivieren und konfigurieren Sie die gerätespezifischen Sicherungseinstellungen. Die dazugehörigen Einstellungsmöglichkeiten sind mit den globalen identisch (siehe *Sicherung* auf Seite 300).

VPN

Auf dieser Seite nehmen Sie Einstellungen für den VPN-Zugang vor.

Hinweis: Diese Dialogseite ist nur für Geräte verfügbar, die auch VPN anbieten.



Öffentlicher Zugang

Geben Sie für die vereinfachte Einrichtung von VPN-Verbindungen eine öffentliche IP bzw. einen Namen und eine Telefonnummer an. Sie können bestimmen, ob die Telefonnummer für den VPN-Verbindungs-Aufbau bevorzugt verwendet werden soll.

Hinweis: Eine Telefonnummer ist nur dann sinnvoll, wenn beide Geräte auch jeweils an das öffentliche Telefonnetz angeschlossen sind und sich über eine entsprechend zugeordnete Rufnummer ("MSN") erreichen können. Geräte können auch gleichzeitig für den Verbindungs-Aufbau per IP oder Telefonnummer konfiguriert werden. Die Verbindung per Telefonnummer ist als zuverlässiger einzustufen, jedoch nicht immer möglich und unter Umständen. aufgrund des Anschlusses mit zusätzlichen Kosten verbunden.

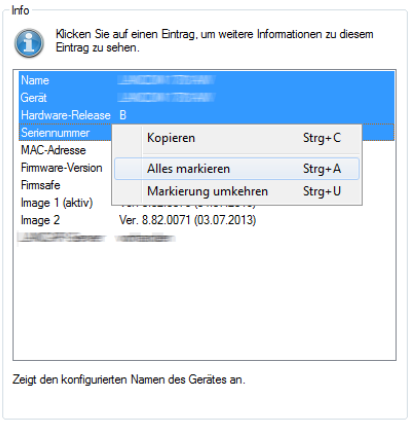
Als VPN-Zentral-Gerät einsetzen

Bestimmen Sie hier, welche IP-Netze mit allen VPN-Außenstellen über die Zentrale verbunden werden sollen.

Informationen

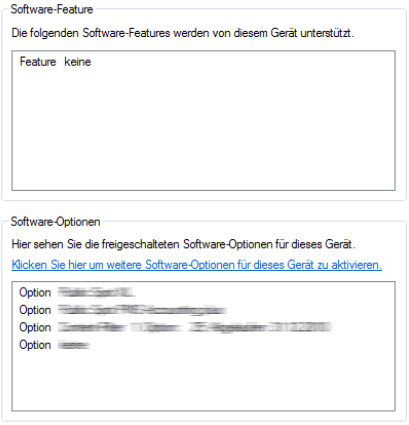
Auf dieser Seite erhalten Sie hardware- und systembezogene Informationen über das Gerät.

Hinweis: Durch einen Klick mit der rechten Maustaste auf die linke Spalte mit den Namen der Einträge, erhalten Sie ein Kontextmenü. Über dieses können Sie die Werte auch in die Zwischenablage übernehmen.



Features & Optionen

Auf dieser Seite erhalten Sie nähere Informationen zu den vom Gerät unterstützten Features und freigeschalteten Optionen.



Gruppe

Unter diesem Menüpunkt verwalten Sie die Gruppen-Konfigurationen.

Weitere Informationen finden Sie im Abschnitt *Flexible Gruppen-Konfiguration mit LANconfig* auf Seite 226.

Neue Gruppen-Konfiguration

Unter **Gruppe** > **Neue Gruppen-Konfiguration** erstellen Sie im aktuellen Ordner eine neue Gruppen-Konfiguration.

Neuer Ordner mit Gruppen-Konfiguration

Unter **Gruppe** > **Neuer Ordner mit Gruppen-Konfiguration** erstellen Sie im aktuellen Ordner einen neuen Unterordner mit einer neuen Gruppen-Konfiguration.

Gruppen-Konfiguration hinzufügen

Unter **Gruppe** > **Gruppen-Konfiguration hinzufügen** speichern Sie eine bereits bestehende Gruppen-Konfiguration in den aktiven Ordner. Wählen Sie hierzu die entsprechende Datei aus.

Gruppen-Konfiguration bearbeiten

Unter **Gruppe** > **Gruppen-Konfiguration bearbeiten** haben Sie die Möglichkeit die ausgewählte Gruppen-Konfiguration zu bearbeiten.

Stellen Sie in der Konfiguration die Parameter so ein, dass sie für die gesamte Gruppe gültig sind. Beim Schließen des Konfigurationsdialogs fordert LANconfig Sie auf, die entsprechende Gruppen-Konfigurationsdatei an einem beliebigen Ort zu speichern.

Alle Geräte aktualisieren

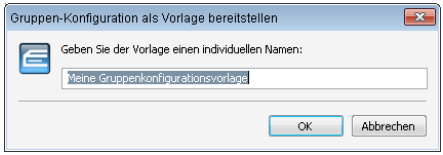
Unter **Gruppe** > **Alle Geräte aktualisieren** haben Sie die Möglichkeit, die ausgewählte und aktivierte Gruppe zu nutzen, um alle Geräte im aktuellen Ordner zu aktualisieren.

Empfohlene Geräte aktualisieren

Unter **Gruppe** > **Empfohlene Geräte aktualisieren** haben Sie die Möglichkeit die ausgewählte und aktivierte Gruppe zu nutzen, um die empfohlenen Geräte im aktuellen Ordner zu aktualisieren.

Als Vorlage bereitstellen

Unter **Gruppe** > **Als Vorlage bereitstellen** haben Sie die Möglichkeit die ausgewählte Gruppen-Konfiguration als Vorlage für zukünftige Gruppen-Konfigurationen zu definieren.



Aktiv

Unter **Gruppe** > **Aktiv** aktivieren oder deaktivieren Sie die ausgewählte Gruppen-Konfiguration.

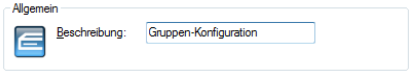
Löschen

Mit **Gruppe** > **Löschen** löschen Sie die ausgewählte Gruppen-Konfiguration.

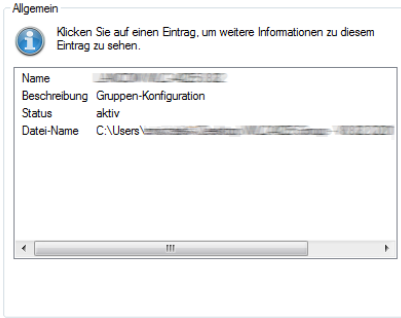
Eigenschaften

Unter **Gruppe** > **Eigenschaften** zeigen Sie Informationen einer bereits bestehenden Gruppen-Konfiguration an. Wählen Sie hierzu die entsprechende Datei aus.

Die Seite **Allgemein** zeigt die Beschreibung der Gruppen-Konfiguration an.



Auf der Seite **Info** finden Sie den Namen, den Status und den Datei-Namen der Gruppen-Konfiguration.



Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANconfig-Bedienoberfläche an.

Symbolleiste

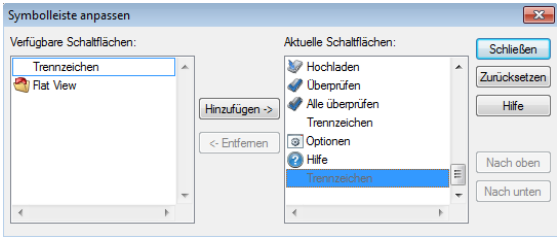
Zur benutzerdefinierten Anpassung der Symbolleiste können im LANconfig die folgenden Optionen gewählt werden:

Schaltflächen
Blendet die Schaltflächen ein oder aus.

QuickFinder
Blendet den QuickFinder ein oder aus.

Große Symbole
Zeigt eine größere Darstellung der Symbole.

Anpassen
Öffnet einen Dialog, in dem die angezeigten Symbole ausgewählt werden können. Zwischen inhaltlichen Gruppen von Symbolen kann dabei ein Trennzeichen eingefügt werden, außerdem kann die Reihenfolge der Symbole verändert werden.



Zurücksetzen

Setzt die Einstellungen für die Symbolleiste auf die Standardwerte zurück.

Eine Übersicht der Symbole finden Sie im Kapitel *Die Symbole der Symbolleiste* auf Seite 306.

Statusleiste

Über diesen Menüpunkt blenden Sie die Statusleiste ein- oder aus.

Verzeichnisbaum

Die Ordnerstruktur am linken Rand des LANconfig-Fensters kann über diesen Menüpunkt (oder alternativ mit der Funktionstaste F6) ein- und ausgeblendet werden. Lesen Sie dazu auch das Kapitel *Verzeichnisbäume zur Organisation nutzen* auf Seite 214.

Protokollanzeige

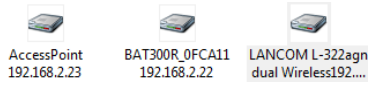
Über diesen Menüpunkt blenden Sie die Protokollanzeige im unteren Teil des LANconfig-Fensters – welche Datum, Zeit, Name, Adresse und Meldung beinhaltet – ein- oder aus.

Flat View Modus

Hier können Sie den Flat View Modus für LANconfig aktivieren.

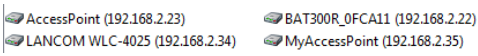
Große Symbole

Im Anzeigemodus 'Große Symbole' werden die Gerätesymbole in einer vergrößerten Darstellung angezeigt.



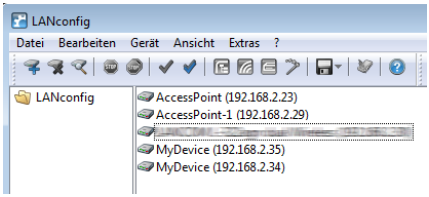
Kleine Symbole

Im Anzeigemodus 'Kleine Symbole' werden die Gerätesymbole klein dargestellt.



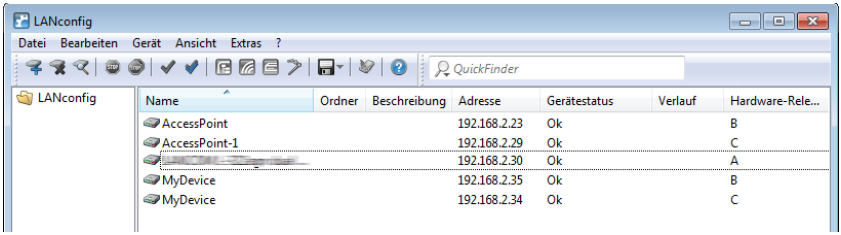
Liste

Im Anzeigemodus 'Liste' werden die Geräte als Liste angezeigt.



Details

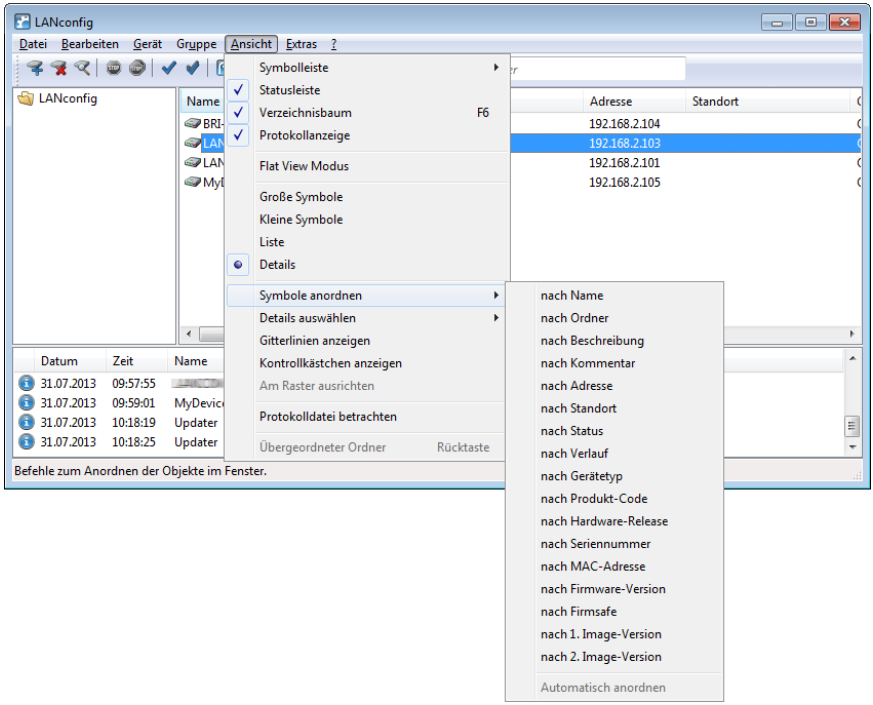
Im Anzeigemodus 'Details' werden Details zu den Geräten angezeigt.



Symbole anordnen

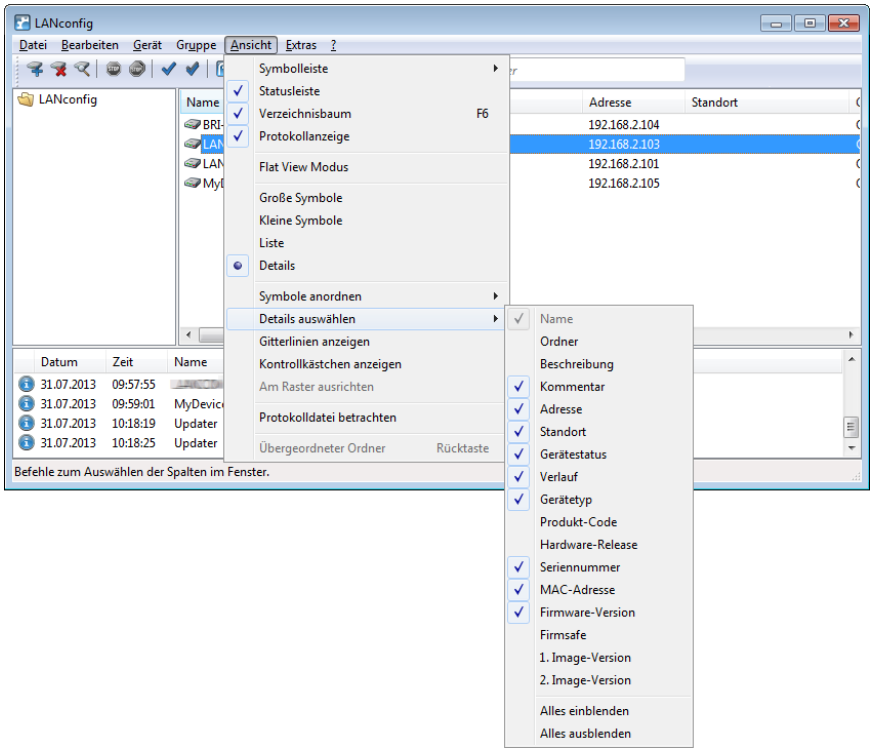
Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- bzw. ausgeblendet werden. Klicken Sie dazu mit der rechten Maustaste auf die Spaltenüberschriften und wählen Sie unter **Ansicht** >

Details auswählen die anzuzeigenden Spalten. Über den Menüpunkt **Symbole anordnen** können Sie ausserdem die gewünschte Sortierung auswählen. Wenn Sie **Automatisch anordnen** auswählen, werden die Symbole im Konfigurationsbereich automatisch angeordnet.



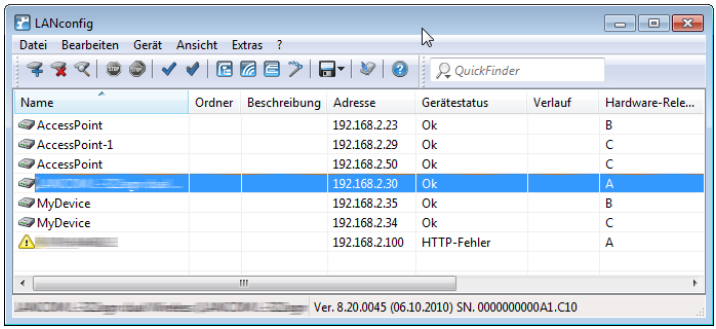
Details auswählen

Für eine bessere und schnellere Übersicht und Orientierung auch in großen Projekten können in LANconfig die Spalten mit gerätebezogenen Informationen einzeln ein- bzw. ausgeblendet werden. Alternativ können Sie auch mit der rechten Maustaste auf die Spaltenüberschriften klicken und im sich öffnenden Kontextmenü das Menü unter **Ansicht** > **Details auswählen** aufrufen.



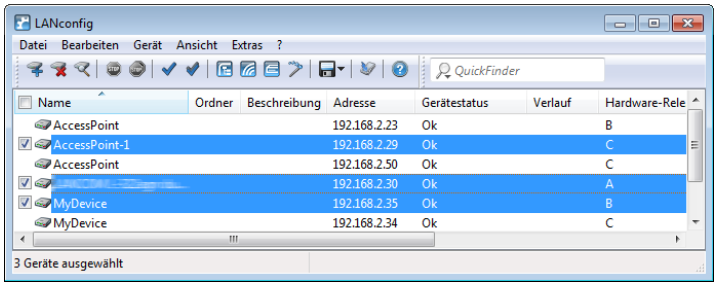
Gitterlinien anzeigen

Über diesen Menüpunkt blenden Sie Gitterlinien in der Geräteansicht ein- oder aus.



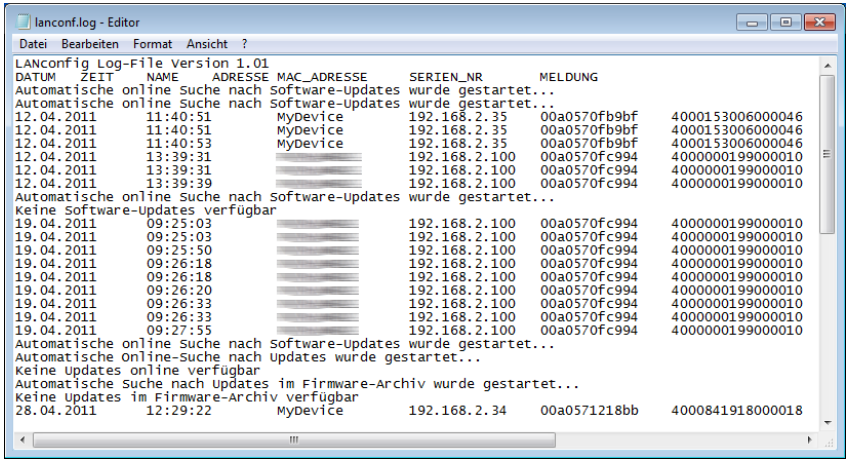
Kontrollkästchen anzeigen

Über diesen Menüpunkt aktivieren Sie die Anzeige von Kontrollkästchen. Links neben dem Geräteintrag erscheint daraufhin ein Kontrollkästchen, mit dem Sie ein Gerät auswählen können. Sie haben so die Möglichkeit, ohne den Einsatz von Tastaturkürzeln mehrere Geräte gezielt auszuwählen und dann Aktionen auf diese Geräte anzuwenden (z. B. neue Firmware hochladen).



Protokolldatei betrachten

Über diesen Menüpunkt können Sie die Protokolldatei von LANconfig ansehen und bearbeiten.



Übergeordneter Ordner

Über diesen Menüpunkt gelangen Sie in der jeweiligen Ordneransicht zu dem übergeordneten Ordner.

Extras

Unter diesem Menüpunkt finden Sie weitere Einstellungsmöglichkeiten LANconfig. Sie erreichen diese Dialogbox auch, indem Sie F7 drücken.

Optionen

Unter dem Menüpunkt **Optionen** können Sie zusätzliche Funktionen von LANconfig aufrufen, z. B. für die Kommunikation mit angeschlossenen Geräten, den Aufruf externer Anwendungen oder die automatische Suche nach Firmware-Updates.

Allgemein

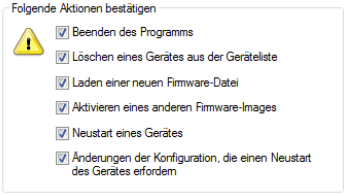
In diesem Dialog legen Sie die allgemeinen Programmeinstellungen fest.

Konfiguration von Geräten

Sie können auswählen, ob Sie für die Konfiguration den Setup-Assistenten als Standard verwenden oder ob Sie standardmäßig den Konfigurations-Dialog zur manuellen Bearbeitung starten wollen, wenn Sie einen Doppeklick auf ein Gerät ausführen. In der Standard-Einstellung wird durch Doppelklick auf ein Gerät die Übersicht der Setup-Assistenten geöffnet.

- **Durchsuchen der Konfiguration in …**
  - **Beschreibung**: Durchsucht die Konfiguration in der Beschreibung
  - **Wert**: Durchsucht die Konfiguration in den Werten
  - **Einheit**: Durchsucht die Konfiguration in den Einheiten

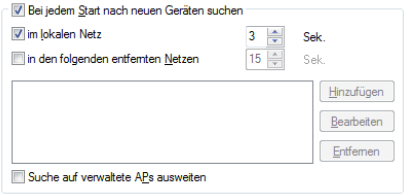
Folgenden Aktionen bestätigen



- **Beenden des Programms**: Schaltet die Sicherheitsabfrage beim Verlassen des Programms ein oder aus.
- **Löschen eines Gerätes aus der Geräteliste:** Schalten Sie diese Option aus, wenn Sie beim Löschen von Geräten nicht mehr von dem Programm gewarnt werden wollen.
- **Laden einer neuen Firmware-Datei:** Wenn Sie diese Option aktivieren, werden Sie gewarnt, wenn Sie eine neue Firmware in das Gerät laden wollen.
- **Aktivieren eines anderen Firmware-Images:** Wenn Sie diese Option aktivieren, werden Sie jedesmal gewarnt, wenn Sie ein anderes Firmware-Image aktivieren wollen.
- **Neustart eines Gerätes:** Wenn Sie diese Option aktivieren, werden Sie gewarnt, bevor das Gerät neu gestartet wird.
- **Änderungen der Konfiguration vornehmen, die einen Neustart erfordern:** Wenn Sie diese Option aktivieren, werden Sie jedesmal gewarnt, wenn Sie die Konfiguration des Gerätes ändern wollen.

Start

In diesem Dialog legen Sie das Verhalten und die Aktionen von LANconfig beim Programmstart fest.



- **Bei jedem Start nach neuen Geräten suchen**: Wenn Sie diese Option aktivieren, sucht das Programm bei jedem Start in vordefinierten Netzen nach neuen Geräten.

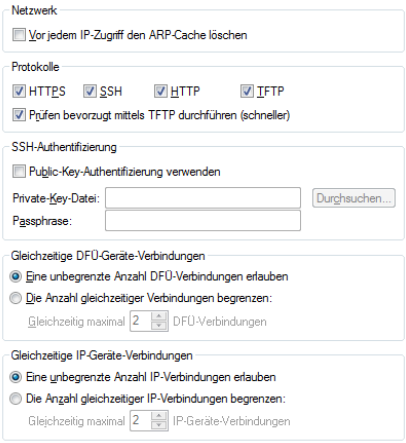
Hinweis: Bei großen Installationen mit vielen Geräten kann dieser Vorgang vergleichsweise viel Zeit in Anspruch nehmen bzw. aufgrund der Verbindungsaufnahme zu den Geräten unerwünscht sein.

- **Im lokalen Netz:** Wenn Sie diese Option aktivieren, sucht das Programm beim Start in Ihrem lokalen Netz nach Geräten und wartet auf die hier eingestellte Zeit auf Antworten.
- **In den folgenden entfernten Netzwerken:** Wenn Sie diese Option aktivieren, sucht das Programm beim Start in entfernten Netzen nach Geräten. Welche Netze durchsucht werden sollen, können Sie in der nachstehenden Liste definieren.
- **Suche auf verwaltete APs ausweiten:** Vollständig gemanagte Access Points (APs) werden normalerweise von der Suche übergangen, da ihre WLAN-Konfiguration gänzlich von einem WLAN-Controller verwaltet wird. Wählen Sie diese Option aus, um vollständig gemanagte APs dennoch zu finden.

Hinweis: Diese Option ist für Sie belanglos, wenn Sie weder über einen WLAN-Controller noch über gemanagte APs in Ihrem Netzwerk verfügen.

Kommunikation

In diesem Dialog nehmen Sie die globalen Einstellungen zu den Verbindungen zwischen LANconfig und den Geräten vor:



Netzwerk

Wenn Sie häufiger wechselnde Geräte mit gleicher IP-Adresse in Ihrem Netz haben, dann sollten Sie die Option **Vor jedem IP-Zugriff den ARP-Cache löschen** einschalten, damit Ihr Rechner diese Geräte erreichen kann.

Protokolle

Zur Übertragung der Daten bei der Konfiguration mit LANconfig stehen wahlweise die Protokolle HTTPS, SSH, HTTP oder TFTP Verfügung.

Die allgemein angebotenen Protokolle werden global definiert. Zusätzlich ist es möglich, Protokolle für bestimmte Geräte zu unterbinden. Es ist jedoch nicht möglich ein global deaktiviertes Protokoll für einzelne Geräte wieder zu aktivieren, da die globalen Kommunikationseinstellungen den gerätespezifischen Einstellungen übergeordnet sind.

Die Konfiguration der Kommunikationsprotokolle unterscheidet zwischen dem Protokoll für das reine Prüfen des Gerätes und den Protokollen für andere Operationen wie z. B. einen Firmware-Upload etc.:

- **HTTPS**, **SSH**, **HTTP**, **TFTP**

  Mit dieser Auswahl aktivieren Sie die einzelnen Protokolle für die Operationen Firmware-Upload sowie Konfigurations- und Script-Upload und -Download. Bei diesen Operationen versucht LANconfig, diese Protokolle in der Reihenfolge HTTPS, SSH, HTTP und TFTP zu ver-

wenden. Schlägt die Übertragung mit einem der gewählten Protokolle fehl, versucht LANconfig automatisch das nächste Protokoll.

- **Prüfen bevorzugt mittels TFTP durchführen**

  Eine Prüfung der Geräte überträgt mit den Systeminformationen nur geringe Datenmengen. Gerade im LAN ist also die Geräteprüfung durchaus mit dem TFTP-Protokoll sinnvoll. Wenn diese Option aktiviert ist, verwendet LANconfig zum Prüfen der Geräte zunächst das TFTP-Protokoll, unabhängig von den zuvor eingestellten Kommunikationsprotokollen. Schlägt die Prüfung über TFTP fehl, versucht LANconfig im Anschluss die Protokolle HTTPS, SSH und HTTP.

SSH-Authentifizierung

Sofern Sie als Protokoll SSH ausgewählt haben, können Sie die Authentifizierung alternativ über einen privaten Schlüssel durchführen. In diesem Fall entfällt die Authentifizierung über eine Dialog zur Kenntworteingabe. Wenn Sie **Public-Key-Authentifizierung verwenden** aktivieren, tragen Sie in die Eingabefelder den Pfad zu Ihrer privaten Schlüsseldatei und ggf. die Passphrase ein, mit der Sie die Datei zusätzlich verschlüsselt haben. Den dazugehörigen öffentlichen Schlüssel laden Sie über LANconfig oder WEBconfig in die einzelnen Geräte.

Eine detaillierte Anleitung zur Konfiguration der Public-Key-Authentifizierung für Ihre Geräte finden Sie im Kapitel *SSH-Authentifizierung mit Hilfe eines Public-Keys* auf Seite 146.

Gleichzeitige DFÜ-Geräte-Verbindungen

Die Anzahl der gleichzeitig über RAS aufgebauten Verbindungen kann künstlich begrenzt werden. Dies ist insbesondere dann sinnvoll, wenn die Menge der physikalisch verfügbaren RAS-Kanäle begrenzt ist oder eine zu hohe System- oder Netzlast vermieden werden soll.

Überschreitet die für entsprechende Aktionen notwendige Anzahl RAS-Verbindungen dieses Limit, so werden die überzähligen Aktionen in eine Warteschlange eingereiht und erst wieder gestartet, wenn ein RAS-Kanal verfügbar wird.

Wenn Sie die Anzahl nicht begrenzen oder eine höhere Begrenzung gewählt haben, als zu irgendeinem Zeitpunkt tatsächlich physikalisch verfügbar ist, so werden überzähligen Aktionen ebenfalls in die oben erwähnte Warteschlange eingereiht.

Hinweis: Mit dieser Option kann beim Start einer großen Zahl gleichzeitiger Aktionen die erzeugte System- oder Netzlast gemindert werden.

Hinweis: Wenn Sie die Anzahl nicht begrenzen und genügend Resourcen zur Verfügung stehen, kann die erzeugte System- oder Netzlast beliebig hoch werden!

Gleichzeitige IP-Geräte-Verbindungen

Die Anzahl der gleichzeitig über IP aufgebauten Verbindungen kann künstlich begrenzt werden. Dies ist insbesondere dann sinnvoll, wenn die Verbindungen über physikalisch begrenzt vorhanden Kanäle laufen oder eine zu hohe System- oder Netzlast vermieden werden soll.

Überschreitet die für entsprechende Aktionen notwendige Anzahl an IP-Verbindungen dieses Limit, so werden die überzähligen Aktionen in eine Warteschlange eingereiht und erst wieder gestartet, wenn ein logischer IP- Kanal verfügbar wird.

Wenn Sie die Anzahl nicht begrenzen oder eine höhere Begrenzung gewählt haben, als zu irgendeinem Zeitpunkt tatsächlich physikalisch verfügbar ist, so werden überzähligen Aktionen mit einem Fehler abgebrochen

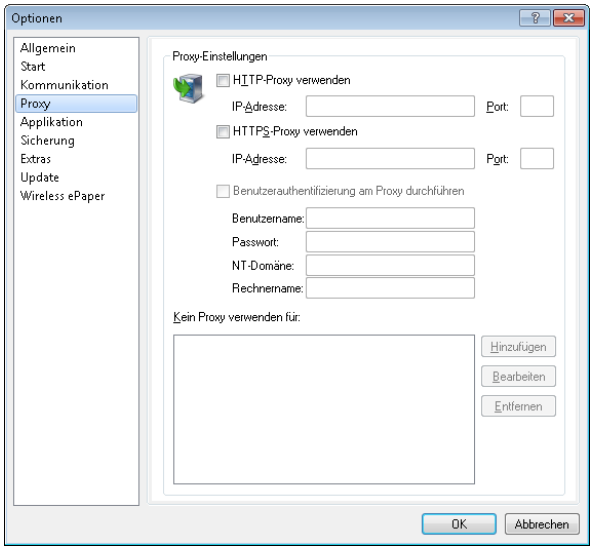
Hinweis: Mit dieser Option kann beim Start einer großen Zahl gleichzeitiger Aktionen die erzeugte System- oder Netzlast gemindert werden.

Hinweis: Wenn Sie die Anzahl nicht begrenzen und genügend Resourcen zur Verfügung stehen, kann die erzeugte System- oder Netzlast beliebig hoch werden!

Proxy

Wenn Sie für den Zugriff auf Ihre Geräte einen Proxy-Server verwenden möchten, können Sie diesen hier konfigurieren. Aktivieren Sie dazu das gewünschte Protokoll und tragen Sie die Adresse und den Port ein, über den der Proxy-Server erreichbar ist.

Protokollunabhängig ist die Angabe einer Liste von Netzen oder einzelnen Hosts möglich, für die die Proxy-Einstellungen nicht gelten.



HTTP-Proxy verwenden

Aktiviert die Verwendung eines HTTP-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTP-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTP-Proxy-Server verwendet.

HTTPS-Proxy verwenden

Aktiviert die Verwendung eines HTTPS-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTPS-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTPS-Proxy verwendet.

Benutzerauthentifizierung am Proxy durchführen

Falls der Proxy-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Passwort ein. Wenn die Authentifizierung über NTLM (NT LAN Manager) erfolgen soll, geben Sie zusätzlich die NT-Domäne und den Rechnernamen ein.

Hinweis: Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

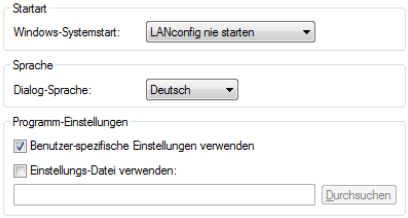
Kein Proxy verwenden für

Tragen Sie hier die IP-Adressen und die zugehörige Netzmaske ein, für die die Proxy-Einstellungen nicht gelten.

Hinweis: Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

Applikation

In diesem Dialog nehmen Sie die Einstellungen zur Benutzeroberfläche vor.



Startart

LANconfig kann beim Start des Betriebssystems automatisch geladen werden. Folgende **Windows-Systemstart**-Arten stehen Ihnen zur Verfügung:

- **LANconfig nie starten**

  Die Anwendung startet nicht automatisch mit dem Betriebssystem, sondern muss manuell gestartet werden.

- **LANconfig immer starten**

  Die Anwendung startet immer automatisch nach dem erfolgreichen Start des Betriebssystems.

- **LANconfig wie zuvor starten**

  Die Anwendung startet in dem Zustand, in dem Sie sich beim Herunterfahren des Betriebssystems befand. War die Anwendung aktiv, wird sie wieder gestartet; war sie nicht aktiv, wird sie auch nicht automatisch gestartet.

Hinweis: Beim Wechsel auf eine Einstellung, die ein automatisches Starten der Anwendung ermöglicht, wird ein Eintrag in der Registry des Betriebssystems vorgenommen. Firewall-Applikationen auf dem Rechner oder die Betriebssysteme selbst (Windows XP, Windows Vista oder Windows 7) können diesen Eintrag ggf. als Angriff deuten und eine Warnung ausgeben bzw. den Eintrag verhindern. Um das gewünschte Startverhalten zu ermöglichen, ignorieren Sie diese Warnungen bzw. lassen Sie die durchzuführenden Aktionen zu.

Sprache

Hierüber ändern Sie die Sprache des Benutzer-Interfaces (GUI). Die Auswahl der Sprache erfolgt normalerweise automatisch anhand der Sprache des Betriebssystems.

Hinweis: Damit die Änderung der Spracheinstellung wirksam wird, ist ein Neustart der Anwendung erforderlich.

Programm-Einstellung

Hier kann die Verwendung benutzerspezifischer LANconfig-Einstellungen gewählt werden. Lesen Sie dazu auch das Kapitel *Benutzerspezifische Einstellungen für LANconfig* auf Seite 214.

- **Benutzerspezifische Einstellungen verwenden**

  Aktiviert die Verwendung der lanconf.ini aus dem aktuellen Benutzer-Verzeichnis unter …`\Anwendungsdaten\Hirschmann\LANconfig\`.

  Wenn diese Option aktiviert ist, werden Änderungen an den Programmeinstellungen in dieser ini-Datei gespeichert.

- **Einstellungs-Datei verwenden**

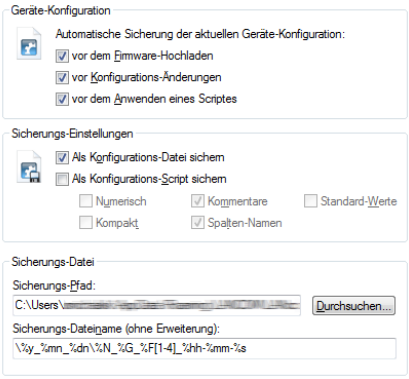
  Aktiviert die Verwendung der lanconf.ini aus dem angegebenen Verzeichnis. Wenn diese Option aktiviert ist, werden Änderungen an den Programmeinstellungen in der im Eingabefeld angegebenen ini-Datei gespeichert.

Hinweis: Bei der gewählten Datei muss es sich um eine gültige LANconfig-Einstellungsdatei handeln.

Hinweis: Wenn keine der beiden Optionen aktiviert ist, wird die ini-Datei aus dem Programmverzeichnis verwendet.

Sicherung

Auf dieser Seite stellen Sie die globalen Sicherungseinstellungen ein.



Geräte-Konfiguration

Hier können Sie wählen, vor welcher Aktion eine automatische Sicherung der aktuellen Gerätekonfiguration durchgeführt werden soll. Um die automatische Sicherung zu aktivieren, müssen Sie mindestens eine der folgenden Einstellungen wählen:

- **Vor dem Firmware-Hochladen:** Vor dem Hochladen einer Firmware wird eine automatische Sicherung der Gerätekonfiguration durchgeführt.
- **Vor Konfigurations-Änderungen:** Vor dem Hochladen oder bei Änderungen der Gerätekonfiguration wird automatisch eine Sicherung der Gerätekonfiguration durchgeführt.
- **Vor dem Anwenden eines Scriptes:** Vor dem Anwenden eines Scriptes am Gerät wird automatisch eine Sicherung der Gerätekonfiguration durchgeführt.

Sicherungs-Einstellungen

Hier können Sie die Sicherungsart wählen. Mindestens eine der folgenden Sicherungsarten muss für die automatische Sicherung der aktuellen Gerätekonfiguration gewählt werden:

- **Als Konfigurations-Datei sichern:** Die automatische Sicherung sichert die aktuelle Gerätekonfiguration als Konfigurations-Datei.
- **Als Konfigurations-Script sichern:** Die automatische Sicherung sichert die aktuelle Gerätekonfiguration als Konfigurations-Script.
  - **Numerisch**: Mit dieser Option werden die Sektionsnamen in numerischer Form dargestellt.
  - **Kommentare**: Mit dieser Option werden zusätzliche Kommentare eingefügt.
  - **Standard-Werte**: Normalerweise werden nur die von den Standardwerten abweichenden Einstellungen gesichert. Mit dieser Option werden zusätzlich die Standardwerte gesichert.
  - **Kompakt**: Mit dieser Option wird die Ausgabe kompakt formatiert. Leerzeilen und Tabulatoren werden beispielsweise unterdrückt.
  - **Spalten-Namen**: Normalerweise werden Tabellen befüllt, indem zuerst die Spalten mit dem Tab-Befehl beschrieben werden und danach jede Zeile mit einem Set-Befehl befüllt wird, welcher nur die zu setzenden Werte enthält. Wird diese Option eingeschaltet, werden die Tabellen-Spalten nicht mit dem Tab-Befehl beschrieben, sondern in jedem Tabellen-Set-Befehl werden die Spalten-Bezeichner eingefügt.

Sicherungs-Datei

- **Sicherungs-Pfad:** Geben Sie hier einen Pfad zu einem Ablage-Ordner auf Ihrem Rechner oder im Netzwerk an. Mit **Durchsuchen** können Sie auch einen Browser öffnen, um den Pfad zu bestimmen. In der Voreinstellung werden Sicherungen im Ordner 'Config' unterhalb des Programmverzeichnisses auf dem lokalen Rechner abgelegt.
- **Sicherungs-Dateiname (ohne Erweiterung):** Sie können hier einen frei wählbaren Dateinamen ohne Erweiterung angeben. Die Erweiterung wird je nach Sicherungs-Dateityp ergänzt. Der Dateiname kann die in der folgenden Tabelle aufgeführten Variablen enthalten, welche erst bei der entsprechenden Aktion zu einem konkreten Dateinamen expandiert werden. Ausserdem können dem Sicherungs-Dateinamen

auch weitere Ordner mit diesen Variablen im Namen vorangestellt und infolgedessen erzeugt werden.

Name	%N
MAC-Adresse	%M
Gerätetyp	%G
Hardware-Release	%W
Firmware-Version	%F
IP-Adresse	%I
Firmware-Datum	%D
Adresse	%H
Seriennummer	%S

Tabelle 15: Geräteinformation

Mit den folgenden regulären Ausdrücken können Sie auch Teile der Geräteinformation anzeigen lassen. Zahlen in eckigen Klammern, welche den Variablen folgen, bilden eine Teilinformation, wie etwa %N[5]. Es wird das n-te Zeichen aus dieser Variable expandiert. Mit einem Bindestrich wird eine Zeichenkette definiert, etwa %H[2-5].

[]	Expandiert alle Zeichen
[1]	Expandiert nur das erste Zeichen
[12], [12-12]	Expandiert nur das zwölfte Zeichen
[1-5]	Expandiert vom Anfang bis zum fünften Zeichen
[2-5]	Expandiert vom zweiten bis zum fünften Zeichen
[6-]	Expandiert alles ab dem sechsten Zeichen

Tabelle 16: Beispiele der Variablen

%y	Jahr
%hh	Stunde
%mn	Monat des Jahres (1-12)
%mm	Minute
%ma	Monat des Jahres (Januar - Dezember)
%s	Sekunde
%dn	Tag des Monats (1-31)

%ms	Millisekunde
%da	Wochentag (Sonntag - Samstag)
%dw	Wochentag (Sonntag ist 0, 0-6)
%%	% (einzelnes Prozent-Zeichen)

Tabelle 17: Datum und Uhrzeit

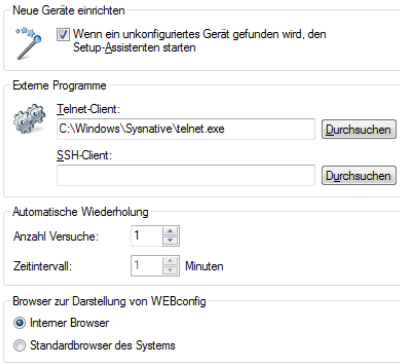
Falls eine Datei mit dem gleichen Namen im Ziel-Verzeichnis existieren sollte, so wird der Name der Sicherungs-Datei automatisch um einen aufsteigenden Zähler erweitert.

Sicherungs-Dateiname: MeinBackup_%N_%S_%I	Resultat: MeinBackup_MeinGeraet_12481632_10.10.1.1
Sicherungs-Dateiname: %d_%mn_%y\Ordner_2\%N	Resultat: 25_08_2008\Ordner_2\MeinGeraet

Tabelle 18: Beispiele

Extras

In diesem Dialog nehmen Sie zusätzliche Einstellungen vor.



Neue Geräte einrichten

Wenn diese Option markiert ist, startet LANconfig bei jedem gefundenen, aber noch nicht konfigurierten Gerät den Setup-Assistenten.

Externe Programme

Bestimmen Sie hier jeweils die Programmdatei des Telnet-Clients und des SSH-Clients, die LANconfig für Verbindungen zu den Geräten benutzen soll.

Automatische Wiederholung

Anzahl Versuche

Geben Sie hier die Anzahl der Versuche für einen Firmware- oder Konfigurations-Upload an. Die Anzahl können Sie im Bereich von 1 bis 9999 einstellen. Einen Verbindungsversuch führt LANconfig immer durch. Schlägt dieser fehl, erfolgt eine Wiederholung der Aktion nach abgelaufener Intervall-Zeit. Es erfolgen so viele Wiederholungen, bis LANconfig entweder die eingestellte Anzahl von Versuchen durchgeführt hat oder die Aktion erfolgreich war. Es ist jedoch auch möglich, dass LANconfig die Wiederholungen vorzeitig abbricht, wenn eine Situation eintritt, die voraussichtlich nicht ohne weitere Einflussnahme zum Erfolg führt. Dies kann z. B. eine Datei sein, die das Gerät nicht öffnen kann.

Zeitintervall

Geben Sie hier die Intervalldauer in Minuten an, die zwischen zwei Firmware- oder Konfigurations-Upload-Versuchen verstreichen soll. Die Intervalldauer können Sie im Bereich von 1 bis 9999 einstellen.

Browser zur Darstellung von WEBconfig

Bestimmen Sie hier, welchen Browser LANconfig standardmäßig für die Anzeige von WEBconfig verwenden soll. Zur Auswahl stehen der Standard-Browser des Betriebssystems und der LANconfig-interne Browser LCCEF (LANCOM Chromium Embedded Framework).

Update

In diesem Dialog nehmen Sie die Einstellungen für das Automatische Update vor.

Um das Update auf neue Firmwareversionen in den Geräten möglichst komfortabel zu gestalten, werden die Firmware-Dateien für die verschiedenen Modelle und HiLCOS-Versionen idealerweise in einem zentralen Archiv-Verzeichnis abgelegt. Die Suche nach neuen Firmware-Versionen in diesem Verzeichnis kann entweder manuell angestoßen werden oder nach jedem Start von LANconfig automatisch durchgeführt werden.

- **Automatisch nach Updates suchen**

  Wählen Sie das zeitliche Intervall für die automatische Suche nach Updates (**Täglich**, **Wöchentlich** oder **Monatlich**) aus. Alternativ deaktivieren Sie die automatische Suche mit der Einstellung **Nie**.

- Wählen Sie für das lokale **Firmware-Archiv** einen geeigneten Speicherort. LANconfig sucht bei der automatischen Suche nach Updates an diesem Speicherort nach neuen Versionen von LCMS und der Firmware.

LANmonitor starten

Startet LANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *LANmonitor - Geräte im LAN überwachen* auf Seite 313.

WLANmonitor starten

Startet den WLANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *WLANmonitor - WLAN-Geräte überwachen* auf Seite 349.

Trace-Ausgabe analysieren

Startet LANtracer. Mehr Informationen dazu erhalten Sie im Kapitel *LANtracer - Tracen mit LANconfig und LANmonitor* auf Seite 372.

Software-Download

Dieser Menüpunkt ruft die Webseite zum Software-Download auf.

Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Support

Dieser Menüpunkt ruft die Webseite des Supports auf.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.1.4 Die Symbole der Symbolleiste

	Hinzufügen		Hochladen
	Löschen		Überprüfen
	Suchen		Alle überprüfen
	Aktion abbrechen		Hilfe
	Aktionen abbrechen		Aufwärts
	Prüfen		Flat View
	Alle prüfen		Wiederherstellen
	Überwachen		Ordner
	WLAN überwachen		Protokollanzeige
	Konfigurieren		Optionen
	Setup-Assistent		Ansicht
	Sicherung		Eigenschaften

Tabelle 19: Bedeutung der Symbole

Informationen zu den Einstellungsmöglichkeiten der Symbolleiste finden Sie im Kapitel *Symbolleiste* auf Seite 285.

3.1.5 Das Kontextmenü in LANconfig

Das Kontextmenü in der Geräteansicht enthält die Funktionen, die Sie auch unter Menü **Gerät** finden.

3.1.6 LANconfig Tastaturbefehle

Einfg	Gerät hinzufügen
Entf	Gerät löschen
F3	Geräte suchen
F5	Alle Geräte prüfen
Alt+F4	Beenden
Strg+N	Neue Konfigurations-Datei
Strg+E	Konfigurations-Datei bearbeiten
Strg+Shift+W	Konfigurations-Datei assistieren
Strg+Shift+P	Konfigurations-Datei drucken
Strg+A	Alles markieren
Strg+O	Gerät > Konfigurieren
Strg+W	Gerät > Setup Assistent
Strg+F5	Gerät > Prüfen
Strg+P	Drucken
Strg+S	Als Datei sichern
Strg+R	Aus Datei wiederherstellen
Strg+Shift+U	Auf Firmware-Update prüfen
Strg+U	Neue Firmware hochladen
Strg+B	Web-Browser gesichert starten
Strg+T	Telnet-Sitzung öffnen
Strg+Shift+S	SSH-Sitzung öffnen
Strg+M	Gerät temporär überwachen
Alt+Enter	Eigenschaften
F6	Verzeichnisbaum
Rücktaste	übergeordneter Ordner
Leertaste, ENTER	Ausgewählten Tabelleneintrag bearbeiten
+	Tabelleneintrag nach oben springen (nur dynamische Tabellen)
-	Tabelleneintrag nach untern springen (nur dynamische Tabellen)

Einfg	Neuen Tabelleneintrag hinzufügen (nur dynamische Tabellen)
Entf	Markierten Tabelleneintrag entfernen (nur dynamische Tabellen)
F7	Extras > Optionen
F1	Hilfethemen

3.1.7 LANconfig Kommandozeilen-Parameter

Sie haben die Möglichkeit, LANconfig über die Windows-Kommandozeile mit bestimmten Optionen und Befehlen zu starten. Die Eingabe erfolgt gemäß der nachfolgend beschriebenen Syntax. Schrägstrich und Bindestrich werden als Parameter-Präfix unterstützt. Bei allen Parametern ist die Groß- und Kleinschreibung nicht relevant.

Die Syntax sieht folgendermaßen aus:

```
lanconf.exe [(-|/)<Option>[:<Value>]] [(-|/)<Command>[:<Value>]]
```

- In eckigen Klammern stehen die optionalen Parameter.
- In runden Klammern stehen die nötigen Parameter.
- Alternativen werden durch einen vertikalen Gedankenstrich getrennt.
- In spitzen Klammern stehen die Objekte, die unter *Optionen* auf Seite 308 und *Befehle* auf Seite 309 beschrieben werden.

Um also z. B. die LANconfig mit englischer Benutzeroberfläche zu starten, geben Sie `lanconf.exe /language:English` ein. Um zusätzlich noch den Konfigurationsassistenten für eine bestimmte Konfigurationsdatei zu öffnen, ergänzen Sie die Angabe um den Wizard-Befehl, also `lanconf.exe /language:English /wizard:MyConfig.lcf`.

Optionen

In diesem Abschnitt werden die Optionen für die Kommandozeile beschrieben.

Restart

Prüft die Startoptionen von LANconfig in der INI-Datei. Nutzen Sie diesen Parameter, um beim Start von Windows das Startverhalten von LANconfig zu beeinflussen. Ein automatischer Start von LANconfig erfolgt

ausschließlich dann, wenn Sie in LANconfig unter **Extras** > **Optionen** > **Applikation** die Startart **LANconfig immer starten** oder **LANconfig wie zuvor starten** (Programm war beim Herunterfahren von Windows aktiv) ausgewählt haben.

WizStyle

Legt die Erscheinung der Konfigurationsassistenten fest. Mögliche Werte für `<Value>` sind:

- `0`: Alter Wizard Style. Kopfzeile (Titel und Untertitel) auf den Dialog-Seiten sind durch eine horizontale Linie von den übrigen Dialog-Inhalten abgegrenzt.
- `1`: Aktueller Wizard Style (seit Windows 98). Kopfzeile (Titel und Untertitel) auf den Dialog-Seiten sind durch eine horizontale Linie sowie einen andersfarbigen Hintergrund von den übrigen Dialog-Inhalten abgegrenzt.

Language

Verändert temporär die Sprache für die Benutzeroberfläche.
Standardmäßig verwendet LANconfig die System-Sprache, sofern diese implementiert ist. Andernfalls ist die Sprache Englisch. Mögliche Werte für `<Value>` sind:

- `English`
- `German`
- `Spanish`

Befehle

In diesem Abschnitt werden die Befehle für die Kommandozeile beschrieben. Befehle im Zusammenhang mit Konfigurationsdateien erfordern die Angabe eines Dateinamens als `<Value>`, z. B. `lanconf.exe /printto:MyConfig.lcf`.

Close

Beendet das Programm nach der Ausführung der noch ausstehenden Befehle. LANconfig startet nach der Ausführung der Befehle normal, es sei denn, eine andere Einstellung wird vorgenommen.

Owner

Übernimmt das Fenster mit Handle [hwndParent]. Optional wird es bei den Befehlen `Print`, `PrintTo` und `AutoUpdate` genutzt.

Edit

Bearbeitet eine Konfigurationsdatei, wenn diese nicht schon bearbeitet wird. Wenn eine Konfigurationsdatei bearbeitet wird, wird diese in den Fokus gebracht.

Wizard

Starten Sie den Assistenten für die Konfigurationsdatei. Wenn dieser bereits geöffnet wurde, gelangt er in den Vordergrund.

Print

Druckt die Konfigurationsdatei, wenn nicht bereits ein Druckaufttrag ausfgeführt wird.

PrintTo

Druckt die Konfigurationsdatei mit einem bestimmten Drucker.

ShellNew

Erstellt eine neue Konfigurationsdatei.

AutoUpdate

So starten Sie ein Firmware Auto-Update:

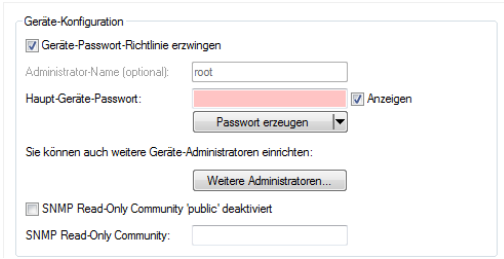
1. Suchen Sie die Geräte.
2. Suchen Sie die Firmware-Dateien.
3. Wählen Sie die neue Firmware.
4. Bestimmen Sie die Geräte, für die ein Firmware-Update durchgeführt werden soll.

3.1.8 Anwendungskonzepte für LANconfig

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANconfig.

Passwort erzeugen in LANconfig

LANconfig bietet an allen Stellen der Konfiguration, welche die Eingabe eines Passworts oder einer Passphrase erfordern, die Möglichkeit zur automatischen Erzeugung eines Passwortvorschlags.

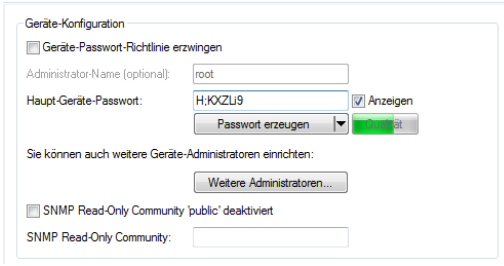


Der Schalter **Geräte-Passwort-Richtlinie erzwingen** legt die folgenden Richtlinien für das Hauptgeräte- und die Administrator-Passwörter fest:

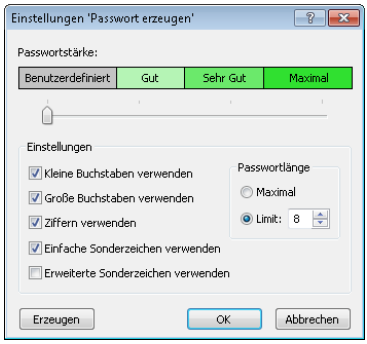
- Die Passwortlänge beträgt mindestens 8 Zeichen.
- Das Passwort beinhaltet mindestens 3 der 4 Zeichenklassen Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen.

Hinweis: Beachten Sie bitte, dass sich die Aktivierung dieser Funktion nicht auf aktuelle Passwörter auswirkt. Nur bei Änderungen der Passwörter werden diese auf ihre Richtlinienkonformität überprüft.

Aktivieren Sie die Option **Anzeigen** neben dem Feld zur Eingabe des Passworts. Klicken Sie dann auf die Schaltfläche **Passwort erzeugen**, um einen Passwortvorschlag zu erzeugen.



Klicken Sie optional auf den Pfeil neben der Schaltfläche **Passwort erzeugen**, um den Dialog für die Einstellungen der Passwort-Richtlinien zu öffnen.



Stellen Sie mit dem Schieberegler die gewünschte Passwortstärke ein. In der Einstellung **Benutzerdefiniert** haben Sie die Möglichkeit, die maximale Passwortlänge und die erforderlichen Zeichentypen zu definieren. In den Einstellungen **Gut**, **Sehr Gut** und **Maximal** sind die Einstellungen mit sinnvollen, nicht veränderbaren Werten vorbelegt.

Klicken Sie nach einer Änderung der Einstellungen erneut die Schaltfläche **Passwort erzeugen**, um einen neuen Passwortvorschlag entsprechend den aktuellen Passwort-Richtlinien zu erzeugen.

Hinweis: LANconfig speichert die gewählten Einstellungen in diesem Dialog für den aktuellen Benutzer.

Unterschiedliche Schreibweisen für MAC-Adressen

Um MAC-Adressen per Kopieren und Einfügen aus anderen Anwendungen einfach in LANconfig zu übernehmen, erlaubt LANconfig bei der Eingabe von MAC-Adressen die folgenden Formate:

- 000000000000
- 00:00:00:00:00:00
- 00-00-00-00-00-00
- 000000-000000

Es konvertiert die Eingabe anschließend automatisch in die Form `00:00:00:00:00:00`.

3.2 LANmonitor - Geräte im LAN überwachen

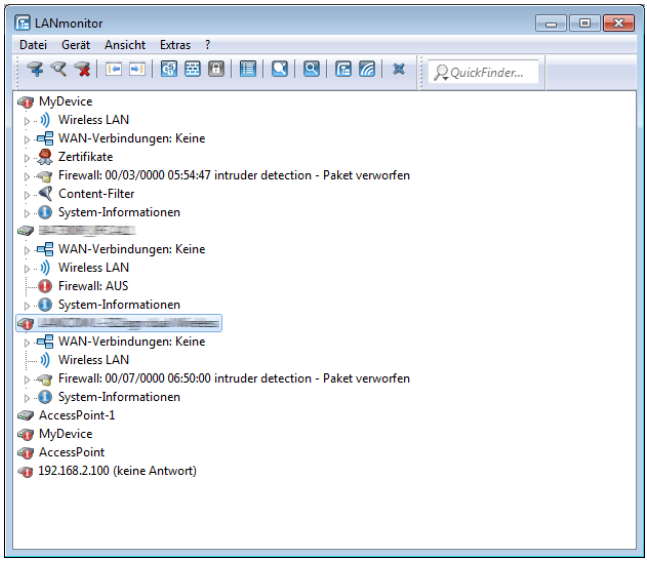
Mit dem Überwachungstool LANmonitor lassen sich unter Windows-Betriebssystemen die wichtigsten Informationen über den Status aller Geräte im Netz bequem und strukturiert überwachen:

- Anzeige von Verbindungen und Schnittstellen
- Interface-Stati
- Übertragungsraten, Protokolle und IP-Adressen
- Fehlerstati
- Anzeige von Geräteinformationen SW-Version, CPU-Last und Speicherverbrauch
- Anzeige von Accounting-Informationen (Online-Zeiten, Gebühren und Transfer-Volumina)
- Anzeige und Protokollierung von Geräteaktivitäten
- Auf- und Abbauten von WAN-, VPN- und WLAN-Verbindungen
- LANCAPI Verbindungen
- Firewall Ereignisanzeige(n)

Viele der internen Meldungen der Geräte werden dabei in Klartext umgewandelt, zeigen Ihnen den aktuellen Zustand des Gerätes und helfen Ihnen bei der Fehlersuche.

Sie können mit LANmonitor auch den Datenverkehr auf den verschiedenen Schnittstellen der Router beobachten und erhalten so wichtige Hinweise darüber, mit welchen Einstellungen Sie den Datenverkehr optimieren können.

Neben den Statistiken des Geräts, die Sie zum Beispiel auch in einer Telnet- oder Terminalsitzung oder mit WEBconfig auslesen können, stehen Ihnen im LANmonitor noch weitere nützliche Funktionen zur Verfügung, wie beispielsweise die Freischaltung eines Gebührenlimits.



Hinweis: Sie können mit LANmonitor nur solche Geräte überwachen, die Sie über IP erreichen (lokal oder remote). Über die serielle Schnittstelle können Sie ein Gerät mit diesem Programm nicht ansprechen.

Hinweis: Wenn Sie ein Gerät in LANmonitor nicht finden können, kann es sein, dass das Auslesen von Geräteinformationen über den von Ihnen gewählten Zugriffsweg (z. B. remote via VPN) nicht erlaubt ist. LANmonitor verwendet für das Auslesen von Geräteinformationen das SNMP-Protokoll, das vom Administrator für jedes Gerät individuell konfiguriert und eingeschränkt werden kann.

3.2.1 LANmonitor starten

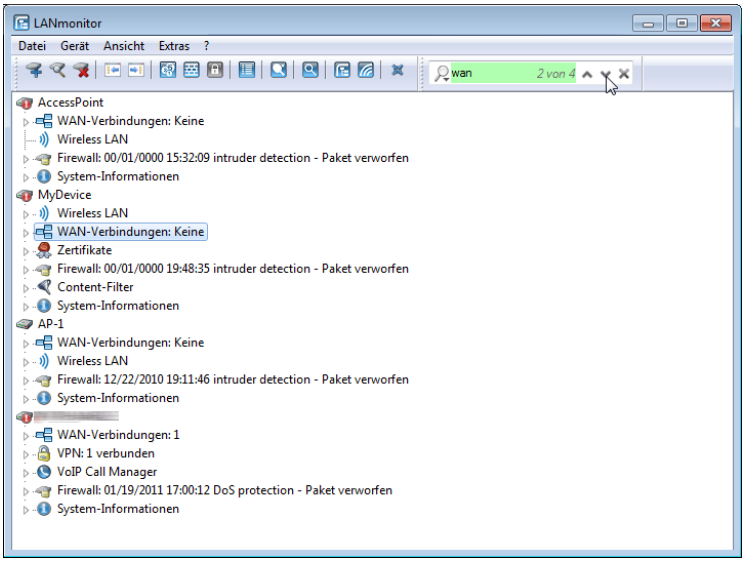
Starten Sie LANmonitor, z. B. mit einem Doppelklick auf das Desktop-Symbol.

Hinweis: Sie können im LANmonitor das Startverhalten unter **Extras** > **Optionen** einstellen. Lesen Sie hierzu auch *Optionen* auf Seite 342.

Sie können den LANmonitor auch in LANconfig über das Kontextmenü für ein bestimmtes Gerät oder über die Tastenkombination 'Strg+M' starten.

3.2.2 QuickFinder im LANmonitor

Der LANmonitor zeigt je nach Anwendung zahlreiche Geräte, die den gesuchten Begriff enthalten können. Nach dem Start der Suche hebt LANmonitor zunächst die erste Fundstelle hervor. Wechseln Sie entweder mit den Pfeiltasten am rechten Rand des Suchfensters oder mit den der Tastenkombination 'Strg+F3' zur nächsten Fundstelle oder mit der Tastenkombination 'Strg+Shift+F3' zur vorherigen Fundstelle.



3.2.3 Anzeige-Funktionen im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen Anwendungen mit einer Reihe von Funktionen, die das Überwachen von Geräten an verteilten Standorten erleichtern. Schon in der Übersicht der überwachten Geräte zeigt LANmonitor die wichtigsten Informationen über den Status der Geräte an. Zu den Informationen, die der Übersicht ablesbar sind, gehören u. a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

Mit einem rechten Mausklick auf die Geräte lassen sich im LANmonitor über das Kontextmenü Listen mit weiteren Informationen aufrufen, darunter u. a.:

- *Aktivitätsprotokoll*
- *DHCP-Zuweisungen*
- *VPN-Verbindungen*
- Firewall-Ereignisanzeigen für *IPv4* sowie *IPv6*
- *Syslog*
- *Accounting-Informationen*

3.2.4 Die Menüstruktur im LANmonitor

LANmonitor unterstützt den Administrator von umfangreichen Anwendungen mit einer Reihe von Funktionen, die das Überwachen von Geräten an verteilten Standorten erleichtern. Über die Menüleiste können Sie dabei Statusinformationen aus den Geräten abrufen, diese zurücksetzen oder weitere Analysen durchführen (z. B. Spectral Scan, Trace-Ausgabe). Zahlreiche Menüpunkte finden Sie auch im Kontextmenü in der Geräteübersicht wieder, verteilt auf die einzelnen Informationspunkte zu den Geräten.

Schon in der Übersicht der überwachten Geräte zeigt LANmonitor die wichtigsten Informationen über den Status der Geräte an. Zu den Informationen, die in der Übersicht abgelesen werden können, gehören u. a. die Details über die aktiven WAN-Verbindungen, die letzten fünf Meldungen der Firewall, die aktuellen VPN-Verbindungen, sowie die Systeminformationen mit Gebühren und Verbindungszeiten.

Datei

Unter diesem Menüpunkt verwalten Sie Geräte allgemein und beenden LANmonitor.

Gerät hinzufügen

Über **Datei** > **Gerät hinzufügen** fügen Sie der Geräteübersicht ein neues Gerät hinzu. Es öffnet sich ein Dialog, in dem Sie u. a. Einstellungen für die Verbindung zum das Gerät und die Protokollierung vornehmen.

Sie haben alternativ aber auch die Möglichkeit, neue Geräte unter Angabe von IP-Adresse und SNMP-Port direkt beim Programmaufruf zu konfigurieren.

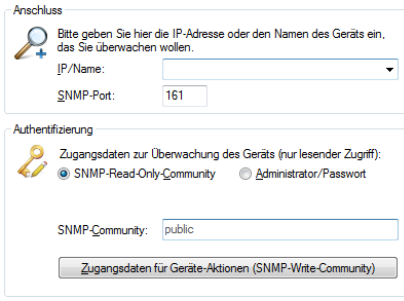
Starten Sie LANmonitor dazu über die Syntax `lanmon /add:[<IPv6-Address>]:<Port>`, also z. B. `lanmon /add:[fe80::2a0:57ff:fe1b:3302]:161`.

Allgemein

Auf dieser Seite geben Sie die IP-Adresse und den SNMP-Port des neuen Gerätes an, das LANmonitor künftig überwachen soll. Sofern das Auslesen von Gerätedaten und/oder Durchführen von Aktionen eine Authentisierung am Gerät erfordert, müssen Sie außerdem diese Zugangsdaten in LANmonitor hinterlegen.

Das dauerhafte Hinterlegen der Daten ist mindestens für den Lesezugriff erforderlich; andernfalls kann das Programm keine Verbindung zum betreffenden Gerät aufbauen. Das dauerhafte Hinterlegen der Daten für den Schreibzugriff ist optional, um nicht nach jedem Start von LANmonitor bei der ersten ausgeführten Aktion die Daten manuell einzugeben.

Wichtig: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch LANmonitor ausführen darf.



Anschluss

- **IP/Name:**: Geben Sie die IP-Adresse des Gerätes an. Sie können auch einen Domain-Namen (DN oder FQDN) oder einen NetBIOS-Namen angeben. Dieser Name wird bei jedem Zugriff überprüft. LANmonitor speichert und verwendet die dabei aufgelöste IP-Adresse. Sollte die Überprüfung einmal nicht möglich sein, greift LANmonitor auf die letzte erfolgreich aufgelöste IP-Adresse zurück.
- **SNMP-Port:** Geben Sie den Port an, unter dem der SNMP-Dienst auf dem Gerät zu erreichen ist. Standardmäßig lautet dieser `161`. Je nach

Einstellung im Gerät (vgl. Setup-Parameter 2.9.21) oder ARF-Kontext kann aber auch ein abweichender Port erforderlich sein.

- **Authentifizierung:** Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses hier ein, um beim Auslesen der Statuswerte die Passworteingabe zu automatisieren.
- **Protokoll:** Setzen Sie ein Häkchen in die Box, wenn Sie die Verbindungen protokollieren wollen.

Authentifizierung

Wählen Sie in diesem Abschnitt aus, wie und mit welchen Zugangsdaten Sie sich am Gerät authentisieren. Die zu wählende Einstellung hängt davon ab, ob Sie den SNMP-Lesezugriff auf dem Gerät eingeschränkt und eine eigene Community definiert haben. Mehr dazu erfahren Sie im Abschnitt *Konfigurieren des SNMP-Lesezugriffs* auf Seite 140.

- **SNMP-Read-Only-Community**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - die öffentliche Community `public`; oder
  - eine eigene Community in Form eines Master-Passworts oder Benutzername:Passwort-Paares

  erfolgt. Diese geben Sie anschließend im Eingabefeld **Community** an.
- **Administrator/Passwort**: Wählen Sie diese Einstellung, wenn die Authentisierung am Gerät über
  - eine eigene Community in Form eines Benutzername:Passwort-Paares; oder
  - die Zugangsdaten eines Administratorkontos

  erfolgt. Den Benutzernamen geben Sie anschließend im Eingabefeld **Administrator**, das Passwort im Eingabefeld **Passwort** an.

Wichtig: Achten Sie dabei auf die korrekte Schreibweise, da bei Eingabe falscher Daten der SNMP-Zugang zum Gerät gesperrt wird.

Darüber hinaus haben Sie optional die Möglichkeit, die **Zugangsdaten für Geräte-Aktionen (SNMP-Write-Community)** wahlweise für die aktuelle Sitzung oder dauerhaft in LANmonitor zu speichern. Diese Daten sind für alle Geräte-Aktionen (z. B. das Löschen oder Zurücksetzen von

Status-Werten) erforderlich. Wenn Sie keine Daten hinterlegen, fragt das Programm sie bei der nächsten Aktion ab.

Hinweis: Für den reinen Lesezugriff ist die Angabe einer Read-Only-Community anstelle eines Administratorkontos die bevorzugte Wahl, da SNMP-Pakete bei SNMPv2 im Klartext übertragen werden.

Protokolle & Logins

Auf dieser Seite konfigurieren und verwalten Sie die Protokolle, Ports und Zugangsdaten, welche die übrigen Bestandteile des LCMS beim Aufruf aus LANmonitor heraus verwenden. Zu den konfigurierbaren Programmen gehören:

- LANconfig
- LANtracer
- LCMS-interner sowie externer Webbrowser

Hinweis: Sofern im aufgerufenen Programm z. B. bestimmte Protokolle bereits deaktiviert bzw. anders konfiguriert sind, gelten ausschließlich die Übereinstimmungen.

Die Einstellungsmöglichkeiten sind äquivalent zu denen von LANconfig. Bitte entnehmen Sie die weitere Konfiguration dem Abschnitt *Protokolle & Logins* auf Seite 278.

Ansicht

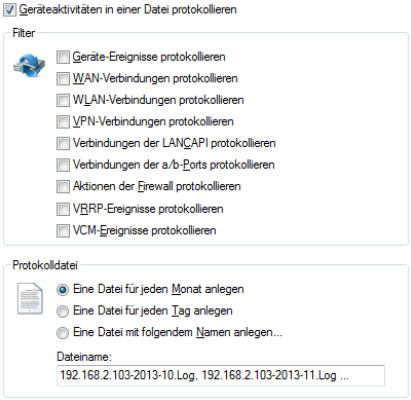
Auf dieser Seite nehmen Sie darstellungsspezifische Einstellungen vor.

Wenn Sie die Option **Tooltips im Systray für dieses Gerät verbergen** aktivieren, zeigt LANmonitor keine Tooltips für dieses Gerät im Systray an.

Protokollierung

Auf dieser Seite steuern Sie die Protokollierung der Geräteaktivitäten durch LANmonitor. Dafür bestimmen Sie nach Aktivieren der Protokollierung durch

die **Filter**-Auswahl, welche Aktivitäten LANmonitor erfassen und in welche Protokoll-Datei schreiben soll.



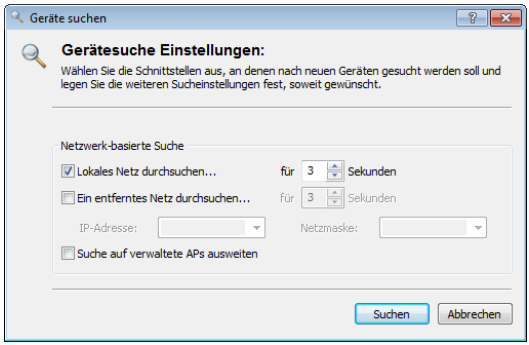
Gerät entfernen

Wenn Sie ein Gerät markiert haben, können Sie es unter **Datei** > **Gerät löschen** entfernen. Sie können auch die Taste 'Entf' drücken, um ein Gerät zu löschen.

Hinweis: Mit dem Löschen entfernen Sie das Gerät nur aus der aktuellen Ansicht. Sie können es jederzeit wieder über **Datei** > **Gerät hinzufügen** oder **Datei** > **Geräte suchen** hinzufügen.

Geräte suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach neuen Geräten, um Sie der Geräteübersicht hinzuzufügen.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

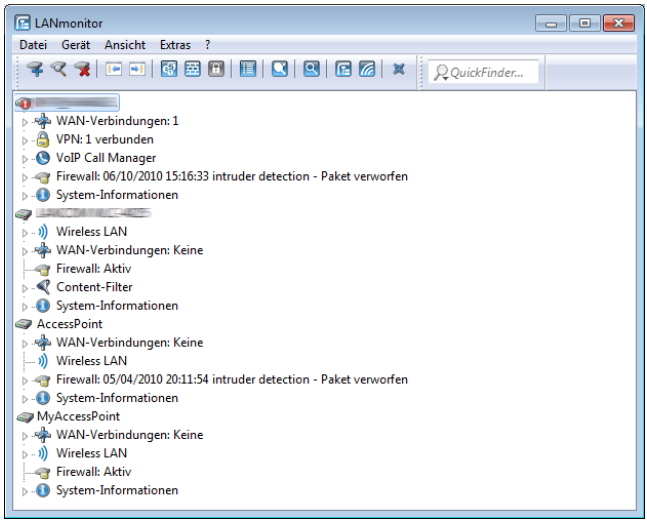
Hinweis: Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle Geräte aktualisieren

Aktualisiert die Verbindung zu allen Geräten.

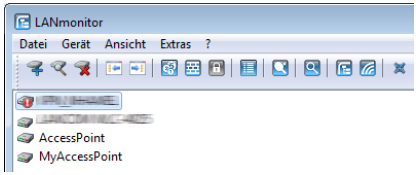
Geräte erweitern

Erweitert die Ansicht der Geräte in der Liste, das Gegenteil ist die *reduzierte Ansicht*. Die erweiterte Ansicht sieht folgendermaßen aus:



Geräte reduzieren

Reduziert die Ansicht der Geräte in der Liste, das Gegenteil ist die *erweiterte Ansicht*. Die reduzierte Ansicht sieht folgendermaßen aus:



Beenden

Schließt und beendet LANmonitor.

Gerät

Unter diesem Menüpunkt verwalten und überwachen Sie ein ausgewähltes Gerät im Netz.

Aktualisieren

Aktualisiert die Anzeige für ein ausgewähltes Gerät.

VPN-Verbindungen anzeigen

Sie können sich die VPN-Verbindungen von einem bestimmten Gerät anzeigen lassen. In der Liste der VPN-Verbindungen werden die letzten 100 VPN-Verbindungen protokolliert. Dabei werden folgende Detailinformationen erfasst:

Name
Name der Gegenstelle

Status
Status der Verbindung (z. B. **Verbunden** oder **Nicht Verbunden**)

Letzter Fehler
Zuletzt aufgetretener Fehler

Haltezeit
Für diese Verbindung festgelegte Haltezeit. Die Haltezeit gibt an, nach wieviel Sekunden das Gerät die Verbindung zur Gegenstelle trennt, wenn in dieser Zeit keine Daten mehr übertragen worden sind. Besondere Werte sind:

- '0': Die selbstständige Trennung durch das Gerät ist deaktiviert. Im Falle eines Verbindungsabbruchs bleibt die Verbindung getrennt und muss vom Benutzer manuell aufgebaut werden.
- '9999': Die selbstständige Trennung durch das Gerät ist deaktiviert. Im Falle eines Verbindungsabbruchs zur Gegenstelle baut der Router sie umgehend selbstständig wieder auf.

Verbindung
Kennung des Netzwerks, das für die physikalische Verbindung zur Gegenstelle genutzt wird

Gateway
IP-Adresse des enfernten VPN-Gateways bzw. der Gegenstelle

Nat-Erkennung
Zeigt an, ob ein NAT vorhanden ist

Verschlüsselungs-Algorythmus

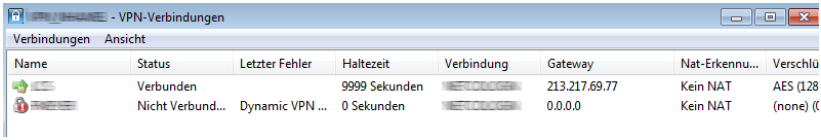
Verwendeter Verschlüsselungsalgorithmus

Hash-Algorythmus
Verwendeter Hash-Algorithmus und Länge des Hash-Codes (in Bit)

Hmac-Algorythmus
Verwendeter Hmac-Algorithmus und Länge des Hmac-Codes (in Bit)

Kompressions-Algorythmus
Verwendeter IPCOMP-Algorithmus

SSL-Kapselung
Zeigt an, ob eine SSL-Kapselung genutzt wird



Unter dem Menüpunkt **Verbindungen** finden Sie folgende Funktionen:

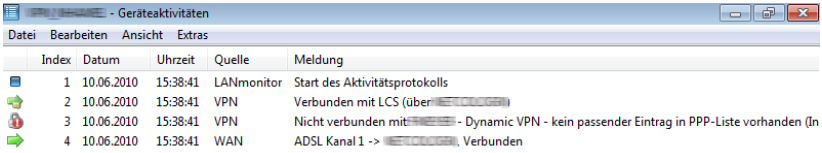
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Geräteaktivitäten anzeigen

Sie können sich die Geräteaktivitäten von einem bestimmten Gerät anzeigen lassen. Mit dem Aktivitätsprotokoll werden die Aktivitäten auf WAN-, WLAN-, VPN-, LANCAPI- und a/b-Port-Verbindungen sowie der Firewall protokolliert. Dabei werden folgenden Detailinformationen erfasst: **Index**, **Datum**, **Uhrzeit**, **Quelle** und **Meldung**. Das Aktivitätsprotokoll wird fortlaufend aktualisiert.



Unter dem Menüpunkt **Verbindungen** finden Sie folgende Funktionen:

- **Geräteaktivitäten speichern**: Speichert die angezeigten Geräteaktivitäten an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.log).
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Bearbeiten** finden Sie folgende Funktionen:

- **Auswahl speichern**: Speichert die markierten Einträge an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.log).
- **Auswahl löschen**: Löscht die markierten Einträge.

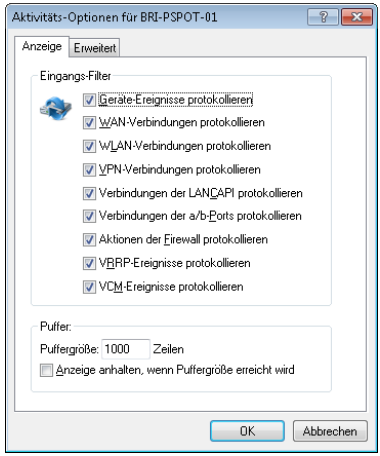
Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

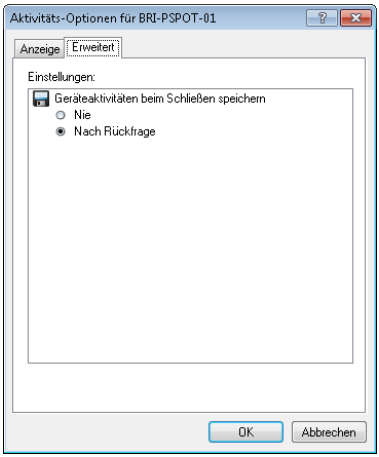
Unter dem Menüpunkt **Extras** finden Sie folgende Funktionen:

- **Optionen**:

  Über diesen Menüpunkt steuern Sie die Protokollierung der gerätespezifischen Aktivitäten durch LANmonitor. Dafür bestimmen Sie durch die **Eingangs-Filter**-Auswahl auf der Registerkarte **Anzeige**, welche Aktivitäten LANmonitor in welchem Umfang (**Puffer**) erfassen soll.



  Auf der Registerkarte **Erweitert** legen Sie zusätzlich fest, ob LANmonitor die aufgezeichneten Daten in einer Datei speichert.



Hinweis: Unter **Gerät** > **Eigenschaften** > **Protokollierung** können Sie die Protokolldatei genauer definieren.

Syslog anzeigen

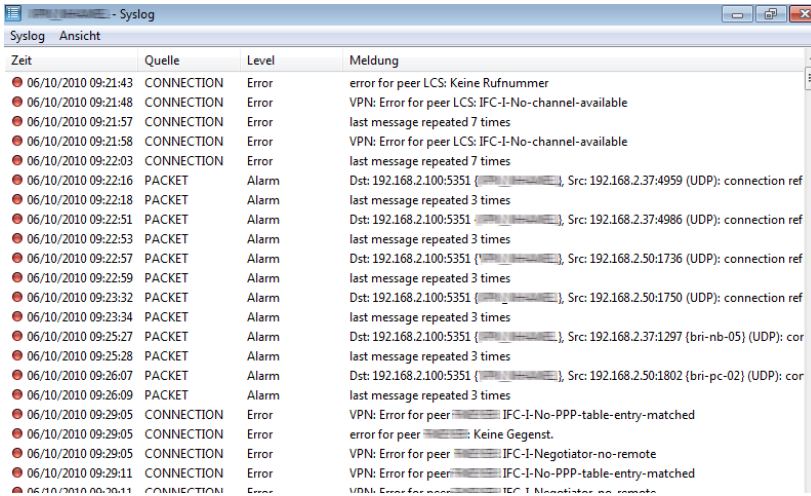
Sie können sich den Syslog von einem bestimmten Gerät anzeigen lassen. Dabei werden folgende Detailinformationen erfasst:

Zeit
Datum Uhrzeit des Syslog-Eintrags

Quelle
Quelle der Syslog-Meldung

Level
Level der Syslog-Meldung, z. B. Alarm oder Fehler

Meldung
Details der Syslog-Meldung



Unter dem Menüpunkt **Syslog** finden Sie folgende Funktionen:

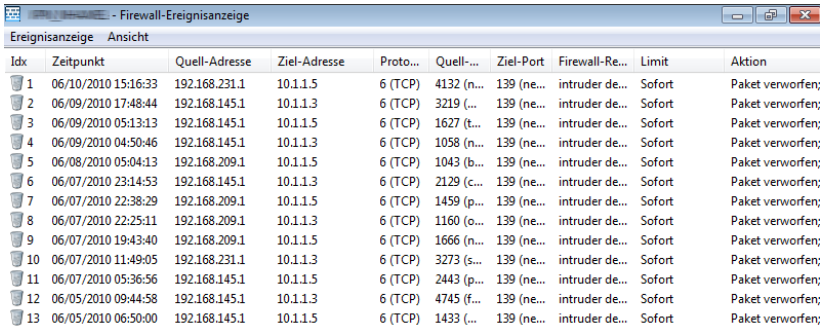
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Syslog speichern**: Speichert die angezeigte Syslog-Ausgabe an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.lsl).
- **Syslog laden**: Lädt eine gespeicherte Syslog-Datei.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

IPv6-Firewall-Ereignisse anzeigen

Über **Gerät** > **Firewall-Ereignisse anzeigen** lassen Sie sich im LANmonitor die Firewall-Ereignisse eines markierten Geräts anzeigen. Die Firewall-Ereignisanzeige listet die letzten 100 Aktionen der Firewall auf. Die angezeigten Detailinformationen und ihre Erläuterungen sind identisch mit denen der *IPv4-Firewall*.



Idx	Zeitpunkt	Quell-Adresse	Ziel-Adresse	Proto...	Quell-...	Ziel-Port	Firewall-Re...	Limit	Aktion
1	06/10/2010 15:16:33	192.168.231.1	10.1.1.5	6 (TCP)	4132 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
2	06/09/2010 17:48:44	192.168.145.1	10.1.1.3	6 (TCP)	3219 (...	139 (ne...	intruder de...	Sofort	Paket verworfen;
3	06/09/2010 05:13:13	192.168.145.1	10.1.1.5	6 (TCP)	1627 (t...	139 (ne...	intruder de...	Sofort	Paket verworfen;
4	06/09/2010 04:50:46	192.168.145.1	10.1.1.3	6 (TCP)	1058 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
5	06/08/2010 05:04:13	192.168.209.1	10.1.1.5	6 (TCP)	1043 (b...	139 (ne...	intruder de...	Sofort	Paket verworfen;
6	06/07/2010 23:14:53	192.168.145.1	10.1.1.3	6 (TCP)	2129 (c...	139 (ne...	intruder de...	Sofort	Paket verworfen;
7	06/07/2010 22:38:29	192.168.209.1	10.1.1.5	6 (TCP)	1459 (p...	139 (ne...	intruder de...	Sofort	Paket verworfen;
8	06/07/2010 22:25:11	192.168.209.1	10.1.1.3	6 (TCP)	1160 (o...	139 (ne...	intruder de...	Sofort	Paket verworfen;
9	06/07/2010 19:43:40	192.168.209.1	10.1.1.5	6 (TCP)	1666 (n...	139 (ne...	intruder de...	Sofort	Paket verworfen;
10	06/07/2010 11:49:05	192.168.231.1	10.1.1.3	6 (TCP)	3273 (s...	139 (ne...	intruder de...	Sofort	Paket verworfen;
11	06/07/2010 05:36:56	192.168.145.1	10.1.1.5	6 (TCP)	2443 (p...	139 (ne...	intruder de...	Sofort	Paket verworfen;
12	06/05/2010 09:44:58	192.168.145.1	10.1.1.3	6 (TCP)	4745 (f...	139 (ne...	intruder de...	Sofort	Paket verworfen;
13	06/05/2010 06:50:00	192.168.145.1	10.1.1.5	6 (TCP)	1433 (...	139 (ne...	intruder de...	Sofort	Paket verworfen;

Unter dem Menüpunkt **Ereignisanzeige** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

IPv4-Firewall-Ereignisse anzeigen

Sie können sich die Firewall-Ereignisse von einem bestimmten Gerät anzeigen lassen. Mit der Firewall-Ereignisanzeige werden die letzten 100 Aktionen der Firewall protokolliert. Dabei werden folgende Detailinformationen erfasst:

Idx
Fortlaufender Indexeintrag der Ereignisse

Zeitpunkt
Zeitpunkt des Eintrages

Quell-Adresse
Quell-Adresse des gefilterten Pakets

Ziel-Adresse
Ziel-Adresse des gefilterten Pakets

Protokoll
Protokoll (TCP, UDP etc.) des gefilterten Pakets

Quell-Port
Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)

Ziel-Port

Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)

Firewall-Regel

Name der Regel, die den Eintrag erzeugt hat

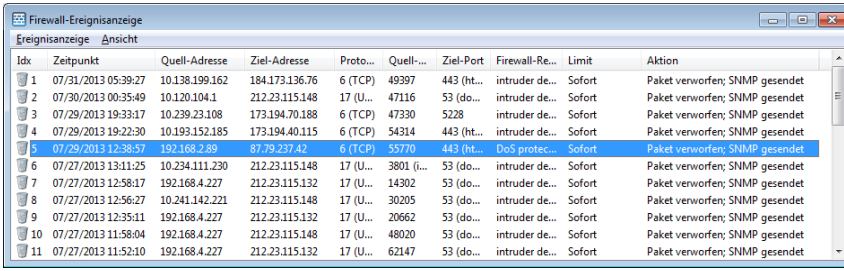
Limit

Limit, welches mit der betreffenden Firewall-Aktion verknüpft ist. Sofern eine Firewall-Aktion nicht mit einem Limit verknüpft ist, wird ein Paket-Limit impliziert, das sogleich beim ersten Paket überschritten wird. In diesem Fall zeigt die Spalte den Wert **Sofort**.

Weitere Informationen zu den Limits finden Sie in der Menüreferenz unter "2.8.10.4 Aktions-Tabelle" im Abschnitt "Limits".

Aktion

Kurzbeschreibung der ausgeführten Aktion



Unter dem Menüpunkt **Ereignisanzeige** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

DHCP-Tabelle anzeigen

Sie können sich die DHCP-Tabelle von einem bestimmten Gerät anzeigen lassen. Dabei werden folgende Detailinformationen erfasst:

IP-Adresse

IP-Adresse des lokalen Netzwerkgerätes

MAC-Adresse

MAC-Adresse des lokalen Netzwerkgerätes

Timeout

Gültigkeitsdauer der Adresszuweisung in Minuten.

Rechnername

Names des lokalen Netzwerkgerätes im Netzwerk (sofern bekannt)

Typ

Typ der Adresszuweisung

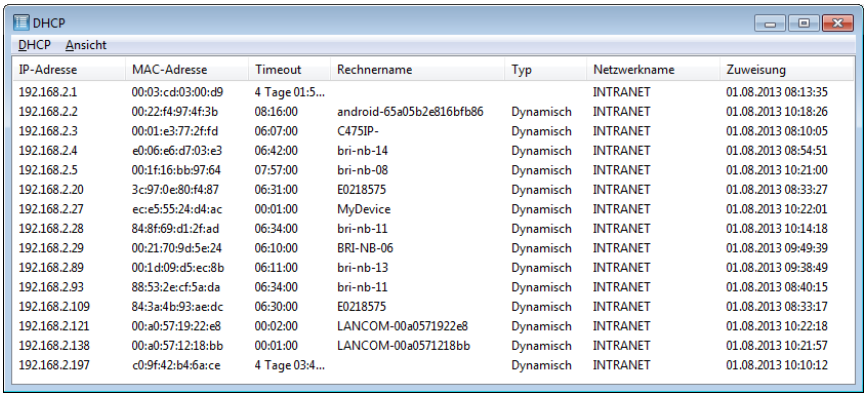
- **Neu**: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
- **Unbekannt**: Bei der Überprüfung der Eindeutigkeit wurde festgestellt, dass die Adresse bereits an einen anderen Rechner vergeben wurde. Der DHCP-Server hat leider keine Möglichkeit, weitere Informationen über diesen Rechner zu erhalten.
- **Statisch**: Ein Rechner hat dem DHCP-Server mitgeteilt, dass er eine feste IP-Adresse besitzt. Diese Adresse darf nicht mehr für andere Stationen im Netz verwendet werden.
- **Dynamisch**: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.

Netzwerkname

Anzeige des Netzwerknamen, mit dem das lokale Netzwerkgerät verbunden ist

Zuweisung

Datum und Uhrzeit der Adresszuweisung.



IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ	Netzwerkname	Zuweisung
192.168.2.1	00:03:cd:03:00:d9	4 Tage 01:5...			INTRANET	01.08.2013 08:13:35
192.168.2.2	00:22:f4:97:4f:3b	08:16:00	android-65a05b2e816bfb86	Dynamisch	INTRANET	01.08.2013 10:18:26
192.168.2.3	00:01:e3:77:2f:fd	06:07:00	C475IP-	Dynamisch	INTRANET	01.08.2013 08:10:05
192.168.2.4	e0:06:e6:d7:03:e3	06:42:00	bri-nb-14	Dynamisch	INTRANET	01.08.2013 08:54:51
192.168.2.5	00:1f:16:bb:97:64	07:57:00	bri-nb-08	Dynamisch	INTRANET	01.08.2013 10:21:00
192.168.2.20	3c:97:0e:80:f4:87	06:31:00	E0218575	Dynamisch	INTRANET	01.08.2013 08:33:27
192.168.2.27	ec:e5:55:24:d4:ac	00:01:00	MyDevice	Dynamisch	INTRANET	01.08.2013 10:22:01
192.168.2.28	84:8f:69:d1:2f:ad	06:34:00	bri-nb-11	Dynamisch	INTRANET	01.08.2013 10:14:18
192.168.2.29	00:21:70:9d:5e:24	06:10:00	BRI-NB-06	Dynamisch	INTRANET	01.08.2013 09:49:39
192.168.2.89	00:1d:09:d5:ec:8b	06:11:00	bri-nb-13	Dynamisch	INTRANET	01.08.2013 09:38:49
192.168.2.93	88:53:2e:cf:5a:da	06:34:00	bri-nb-11	Dynamisch	INTRANET	01.08.2013 08:40:15
192.168.2.109	84:3a:4b:93:ae:dc	06:30:00	E0218575	Dynamisch	INTRANET	01.08.2013 08:33:17
192.168.2.121	00:a0:57:19:22:e8	00:02:00	LANCOM-00a0571922e8	Dynamisch	INTRANET	01.08.2013 10:22:18
192.168.2.138	00:a0:57:12:18:bb	00:01:00	LANCOM-00a0571218bb	Dynamisch	INTRANET	01.08.2013 10:21:57
192.168.2.197	c0:9f:42:b4:6a:ce	4 Tage 03:4...		Dynamisch	INTRANET	01.08.2013 10:10:12

Unter dem Menüpunkt **Accounting** finden Sie folgende Funktionen:

- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Accounting-Informationen anzeigen

Sie können sich die Accounting-Informationen von einem bestimmten Gerät anzeigen lassen. Mit den Accounting-Informationen werden die Verbindungen der einzelnen Stationen im LAN zu den erreichbaren Gegenstellen im WAN protokolliert. Dabei werden folgende Detailinformationen erfasst:

Benutzer
: Name der Verbindung, in der Regel der Name des Netzwerkgerätes, welches über das ausgewählte Gerät eine Verbindung aufgebaut hat.

Gegenstelle
: Name der Gegenstelle, zu der das ausgewählte Gerät eine Verbindung aufgebaut hat.

Typ
: Typ der Verbindung

Verbindungen

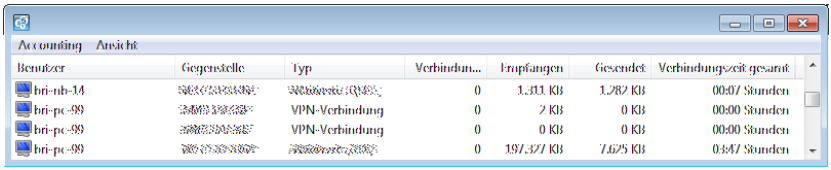
Anzahl der Verbindungen, die vom betreffenden Typ zur gelisteten Gegenstelle derzeit offen sind.

Empfangen, Gesendet

Datenmenge, die der Benutzer innerhalb der Verbindungszeit empfangen/gesendet hat.

Verbindungszeit insgesamt

Gesamte Verbindungszeit in Stunden, Minuten und Sekunden.



Unter dem Menüpunkt **Accounting** finden Sie folgende Funktionen:

- **Zurücksetzen**: Löscht alle Accounting-Informationen und setzt alle Zähler auf '0' zurück.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Accounting-Informationen speichern**: Speichert die angezeigten Accounting-Informationen an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.acc).
- **Accounting-Informationen laden**: Lädt eine gespeicherte Datei mit Accounting-Informationen.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.
- **Accounting-Liste (aktuelle)**: Zeigt die aktuelle Accounting-Liste.
- **Accounting-Liste (letzter Abrechnungszeitraum)**: Zeigt die Accounting-Liste des letzten Abrechnungszeitraums.

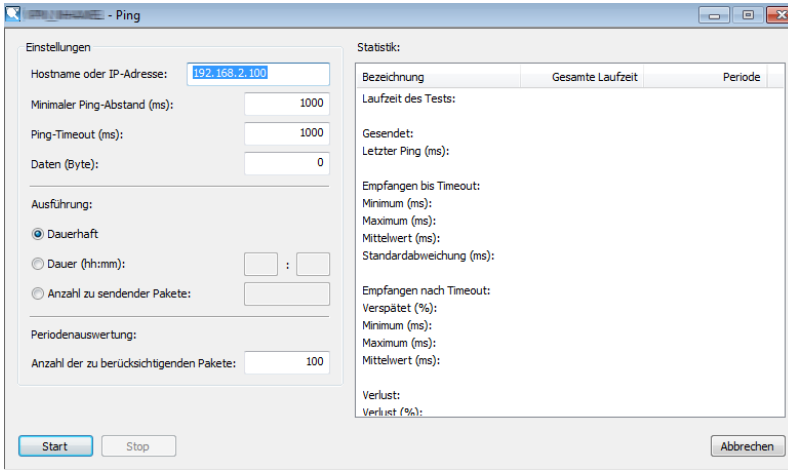
Zeit- und Gebührenlimits zurücksetzen

Hier können Sie das Zeit- und Gebührenlimit des markierten Geräts auf Null zurücksetzen. Damit beginnt die Zeit-/Gebührenzählung erneut, auch wenn der nächste Zeitrahmen zur Limitierung nicht erreicht ist.

Ping

Mit dem LANmonitor haben Sie die Möglichkeit, die Qualität der Verbindung zu Gegenstellen in LAN, WAN oder WLAN zu prüfen. Dazu sendet der LANmonitor von dem Arbeitsplatzrechner, auf dem er installiert ist, regelmäßig Ping-Befehle an eine Gegenstelle und erstellt mit den empfangenen Antworten zusammen einen Bericht.

Zur Eingabe der Parameter und zur Anzeige der Auswertung des Ping-Tests dient ein eigener Dialog, der aus dem LANmonitor heraus aufgerufen werden kann:



Konfiguration der Ping-Ausführung

- **Hostname oder IP-Adresse**: Hier wird die Gegenstelle eingetragen, die mit dem Ping erreicht werden soll. Möglich sind folgende Angaben für alle in LAN, WAN oder WLAN erreichbaren Netzwerkgeräte (Server, Clients, Router, Drucker etc.):

Hinweis: Sofern beim Öffnen des Ping-Dialogs über Gerät > Ping oder über das Kontextmenü im LANmonitor ein Gerät ausgewählt ist, wird die IP-Adresse des Geräts als Gegenstelle übernommen.

- **Minimaler Ping-Abstand**: Zeitlicher Abstand zwischen zwei Ping-Befehlen in [ms].

Hinweis: Die Abstände zwischen zwei Pings können nicht kleiner sein als die Paketlaufzeit, d. h. vor Versenden eines Pings muss der vorherige Ping beantwortet oder der Ping-Timeout abgelaufen sein.

- **Ping-Timeout**: Wartezeit für die Antwort auf den Ping in [ms]. Wenn nach Ablauf der Wartezeit keine Antwort empfangen wurde, wird das Paket als verloren gewertet.
- **Daten**: Größe der für den Ping verschickten Pakete [Byte]. Ein "Ping" ist ein ICMP-Paket, das üblicherweise ohne Inhalt verschickt wird, also nur aus seinem Header besteht. Um die Last der Verbindungsüberprüfung zu erhöhen, kann eine Payload, also ein Inhalt, künstlich erzeugt werden. Die gesamte Paketgröße ergibt sich dann aus IP-Header (20 Byte), ICMP-Header (8 Byte) und Nutzlast.

Hinweis: Wenn durch die Payload der ICMP-Pakete die maximale Paketgröße der IP-Pakete überschritten wird, werden die Pakete fragmentiert.

- **Ausführung**: Wiederholungsmodus für den Ping-Befehl. Sie haben die Möglichkeit, die Ping-Prüfung neben dem manuellen Stopp auch nach Ablauf einer bestimmten Zeit oder definierten Anzahl gesendeter Datenpakete zu beenden.
- **Periodenauswertung**: Im rechten Teil des Ping-Dialogs werden die Ergebnisse der Ping-Prüfung dargestellt. Die erste Spalte zeigt die summierten Werte der gesamten Laufzeit, die zweite Spalte zeigt nur die Ergebnisse der Prüfperiode, also die summierten Werte der letzten Pakete. Unbeantwortete Pings gehen nicht in die Auswertung mit ein.

Hinweis: Bei der Periodenauswertung werden nur die in der Periode gesendeten Pings ausgewertet.

Statistik

Folgende Daten werden zur Auswertung angezeigt:

- Laufzeit des Tests: Gesamte Laufzeit [Std. / Min. / Sek.]

- Gesendet: Gesamte Anzahl der gesendeten Pings
- Laufzeit des letzten Pings [ms]
- Empfangen bis Timeout: Anzahl der Pings, die im Timeout-Zeitraum beantwortet wurden
- Minimale Laufzeit
- Maximale Laufzeit
- Mittelwert
- Standardabweichung von der mittleren Laufzeit
- Empfangen nach Timeout: Anzahl der Pings, die nach dem Timeout beantwortet wurden
- Anteil der verspäteten Pakete an der Gesamtzahl
- Minimale Laufzeit
- Maximale Laufzeit
- Mittelwert
- Verlust
- Letzter Fehler

Trace-Ausgabe erstellen

Mit dieser Option starten Sie die Trace-Ausgabe in LANtracer.

Lesen Sie hierzu auch *LANtracer - Tracen mit LANconfig und LANmonitor* auf Seite 372.

Spectral-Scan anzeigen

Über diesen Menüpunkt starten Sie für das ausgewählte Gerät das Spectral-Scan-Modul im LANmonitor-internen Webbrowser. Weitere Informationen zur Konfiguration finden Sie unter *Funktionen des Software-Moduls* auf Seite 1209

Punkt-zu-Punkt WLAN-Antennen einrichten

Wenn es sich bei dem ausgewählten Gerät um ein WLAN-Gerät handelt, können Sie die Punkt-zu-Punkt WLAN-Antennen einrichten.

Hinweis: Dieser Menüeintrag ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (in LANconfig unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** > **Punkt-zu-Punkt**).

Ausrichten der Antennen für den P2P-Betrieb

Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der "Ideallinie" der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite. Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten.

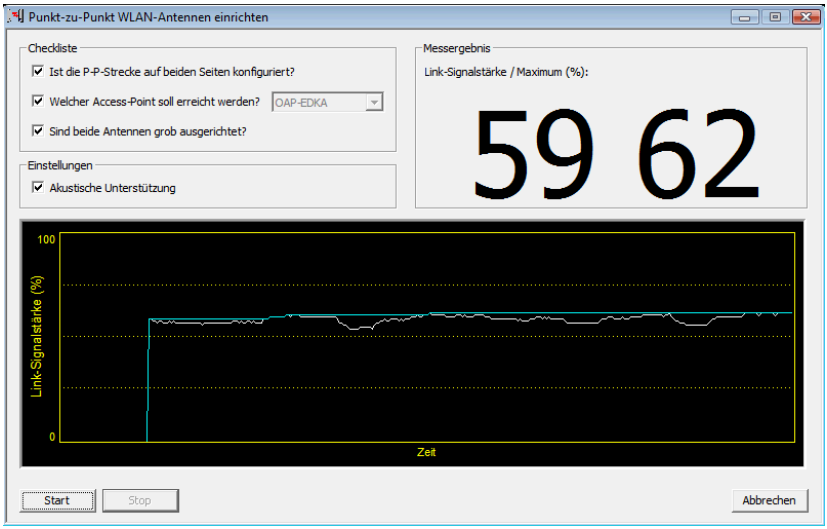
Um die Antennen möglichst gut auszurichten, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden.

Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden. Je schneller die LED blinkt, umso besser ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).

Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2PVerbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert (gegenüberliegende Basisstation mit MAC-Adresse oder Stations- Namen definiert)?
- Welcher Access Point soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitors gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erreichen.

Konfigurieren

Startet LANconfig, um das ausgewählte Gerät zu konfigurieren.

Web-Browser starten

Startet den Standard-Web-Browser, um das ausgewählte Gerät über WEBconfig zu konfigurieren.

Content-Filter-Kategorien anzeigen

Sofern Ihr Gerät über ein aktiviertes Content-Filter-Modul verfügt, rufen Sie über diesen Menüpunkt die Content-Filter-Kategorien auf.

Unter dem Menüpunkt **Content-Filter-Kategorien** finden Sie folgende Funktionen:

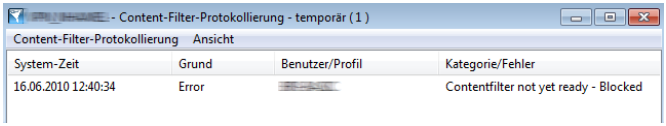
- **Zurücksetzen**: Löscht die angezeigten Informationen und setzt alle Zähler auf Null zurück.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Kategorien-Informationen speichern**: Speichert die angezeigten Kategorien-Informationen an einem Ort Ihrer Wahl in einem geeigneten Dateiformat (*.acc).
- **Kategorien-Informationen laden**: Lädt gespeicherte Kategorien-Informationen aus einer Datei.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.
- **Content-Filter-Kategorien (Aktuell)**: Zeigt den aktuellen Status der Content-Filter-Kategorien.
- **Content-Filter-Kategorien (Last-Snapshot)**: Zeigt den Status der Content-Filter-Kategorien beim letzten Schnappschuss.

Content-Filter-Protokollierung anzeigen

Sofern Ihr Gerät über ein aktiviertes Content-Filter-Modul verfügt, sehen Sie über diesen Menüpunkt die Content-Filter-Protokollierung ein.



Unter dem Menüpunkt **Content-Filter-Protokollierung** finden Sie folgende Funktionen:

- **Zurücksetzen**: Löscht die angezeigten Informationen.
- **Aktualisieren**: Aktualisiert die angezeigten Angaben.
- **Schließen**: Schließt dieses Informationsfenster.

Unter dem Menüpunkt **Ansicht** finden Sie folgende Funktionen:

- **Immer im Vordergrund**: Das Fenster ist immer im Vordergrund.

Eigenschaften

Über diesen Menüpunkt öffnen Sie den Eigenschaften-Dialog des markierten Gerätes, in dem sich auf verschiedenen Seiten teils globale, teils gerätespezifische Einstellungen vornehmen oder einsehen lassen.

Hinweis: Die verfügbaren Seiten des Dialogs sind weitgehend identisch mit denen unter **Datei** > **Gerät hinzufügen**. Dieser Abschnitt behandelt daher nur jene Seiten, die ausschließlich im Eigenschaften-Dialog erscheinen. Für alle übrigen Seiten, siehe

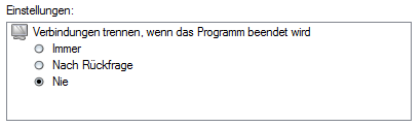
- *Allgemein* auf Seite 317
- *Protokolle & Logins* auf Seite 319
- *Ansicht* auf Seite 319
- *Protokollierung* auf Seite 319

Information

Auf dieser Seite finden Sie weitere Informationen zu Gerät und Hersteller.

Erweitert

Auf dieser Seite finden Sie erweiterte Einstellungen.



Unter **Verbindungen trennen, wenn das Programm beendet wird** stellen Sie ein, ob LANmonitor bestehende Verbindungen des Gerätes zu Gegenstellen beim Beenden trennen soll.

- **Immer**: LANmonitor trennt die Verbindungen stets ohne Rückfrage.
- **Nach Rückfrage**: LANmonitor trennt Verbindungen nur nach vorangehender Bestätigung durch den Benutzer.
- **Nie**: LANmonitor trennt die Verbindungen nicht. Die Verbindungen bleiben bestehen.

Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANmonitor-Bedienoberfläche an.

Immer im Vordergrund

Wenn Sie diese Einstellung aktivieren, wird das Fenster stets im Vordergrund angezeigt.

Zustand im Systray anzeigen

Wenn Sie diese Einstellung aktivieren, zeigt LANmonitor den Zustand der Geräte (Fehler) im Systray an.

LANmonitor in den Systray minimieren

Wenn Sie diese Einstellung aktivieren, wird LANmonitor beim Minimieren im Systray anstelle der Taskleiste abgelegt.

Symbolleiste

Blendet die Symbolleiste aus bzw. ein. Lesen Sie hierzu auch *Die Symbolleiste im LANmonitor* auf Seite 343.

Anzeigen

Unter diesem Menüpunkt stellen Sie folgende Anzeige-Optionen ein oder aus:

- Fehlermeldungen
- Diagnosemeldungen
- System-Informationen

Hinweis: Viele wichtige Details zum Status eines Gerätes werden erst angezeigt, wenn die Anzeige der System-Informationen aktiviert ist. Dazu gehören beispielsweise die Schnittstellen und das Gebührenmanagement. Wir empfehlen daher interessierten Benutzern, die Anzeige der System-Informationen einzuschalten.

Extras

Unter diesem Menüpunkt lesen Sie die gespeicherten Informationen ausgewählter Informationsfenster ein (z. B. gespeicherte Syslog- oder Accounting-Protokolle) und starten andere Programmbestandteile von LCMS.

LANmonitor (temporär) starten

Öffnet ein neues Fenster von LANmonitor zur temporären Überwachung von Geräten. Nach dem Schließen von LANmonitor gehen die Einstellungen des temporären LANmonitor-Fensters verloren.

WLANmonitor starten

Startet den WLANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *WLANmonitor - WLAN-Geräte überwachen* auf Seite 349.

LANconfig starten

Startet LANconfig. Mehr Informationen dazu erhalten Sie im Kapitel *LANconfig - Geräte konfigurieren* auf Seite 208.

Geräteprotokoll-Datei anzeigen

Öffnet die Sicherung eines Aktivitäten-Protokolls zur Ansicht. Lesen Sie dazu auch *Geräteaktivitäten anzeigen* auf Seite 324.

Accounting-Datei anzeigen

Hier können Sie eine Accounting-Datei laden. Lesen Sie dazu auch *Accounting-Informationen anzeigen* auf Seite 331.

Syslog-Datei anzeigen

Hier können Sie eine Syslog-Datei laden. Lesen Sie dazu auch *Syslog anzeigen* auf Seite 326.

Trace-Ausgabe analysieren

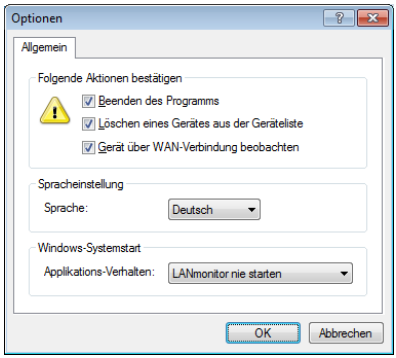
Startet LANtracer. Mehr Informationen dazu erhalten Sie im Kapitel *LANtracer - Tracen mit LANconfig und LANmonitor* auf Seite 372.

Ping

Hier können Sie einen Ping-Test durchführen. Lesen Sie dazu auch *Ping* auf Seite 333.

Optionen

Hier können Sie die Einstellungen zum Bestätigen von Aktionen, zur Spracheinstellung und zum Verhalten der Applikation beim Windows-Systemstart bearbeiten.



- **Folgende Aktionen bestätigen**: Geben Sie an, welche Aktionen durch den Nuter bestätigt werden müssen.
- **Spracheinstellung**: Wählen Sie hier die Sprache der grafischen Programmoberfläche (Deutsch, Englisch oder Spanisch).
- **Windows-Systemstart**: Wählen Sie hier, wie LANmonitor sich beim Starten von Windows verhalten soll.

Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.2.5 Die Symbolleiste im LANmonitor

Die Symbolleiste im LANmonitor beinhaltet die folgenden Funktionen:

- Gerät hinzufügen
- Geräte suchen
- Gerät entfernen
- Geräte reduzieren
- Geräte erweitern
- Accounting-Informationen anzeigen
- IPv4-Firewall-Ereignisse anzeigen
- VPN-Verbindungen anzeigen
- Geräteaktivitäten anzeigen
- Ping
- Trace-Ausgabe erstellen
- Spectral Scan anzeigen
- LANmonitor (temporär) starten
- WLANmonitor starten
- Alle Fenster in den Systray minimieren
- QuickFinder

Hinweis: Unter **Ansicht** > **Symbolleiste** blenden Sie die Symbolleiste ein- oder aus.

3.2.6 Das Kontextmenü im LANmonitor

Das Kontextmenü zu jedem hinzugefügten Gerät in der LANmonitor-Ansicht zeigt dieselben Funktionen wie das Menü **Gerät** in der Menüleiste. Zusätzlich ist die Funktion **Löschen** enthalten, um das Gerät aus der LANmonitor-Ansicht zu entfernen.

3.2.7 LANmonitor Tastaturbefehle

Einfg	Gerät hinzufügen
Entf	Gerät entfernen
F3	Geräte suchen
F5	Alle Geräte aktualisieren
Alt+F4	Beenden
Pfeil hoch	Einen Eintrag in der Geräteliste aufwärts springen
Pfeil runter	Einen Eintrag in der Geräteliste abwärts springen
Pfeil links, ENTER	Menübaum in der Geräteliste reduzieren
Pfeil rechts, ENTER	Menübaum in der Geräteliste erweitern
Strg+F5	Aktualisieren
Space	Gerät > Optionen
F7	Extras > Optionen
F1	Hilfethemen

3.2.8 Anwendungskonzepte für LANmonitor

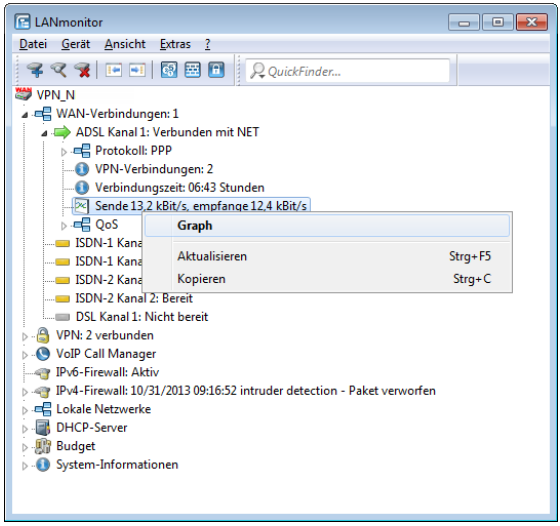
In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANmonitor.

Performance Monitoring im LANmonitor

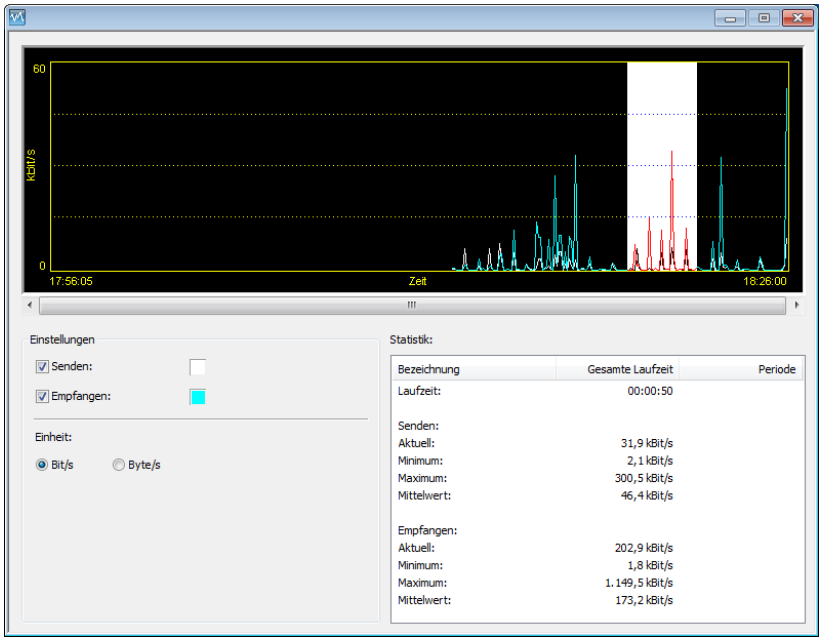
LANmonitor ist dazu in der Lage, verschiedene Kenngrößen eines Gerätes aufzuzeichnen und diese in Form einer Verlaufskurve graphisch darzustellen. Hierzu gehören u. a.:

- Sende- und Empfangsrate für WAN-Verbindungen
- Sende- und Empfangsrate für Point-to-Point-Verbindungen
- Empfangssignalstärke für Point-to-Point-Verbindungen
- Linksignalstärke für Point-to-Point-Verbindungen
- Durchsatz für Point-to-Point-Verbindungen
- CPU-Last
- Freier Speicher
- Temperatur (nicht für alle Modelle verfügbar)

Die aktuellen Werte einer Kenngröße zeigt LANmonitor direkt im entsprechenden Gruppenzweig der Geräteübersicht an. Um die graphische Aufzeichnung zu starten, öffnen Sie auf einer Kenngröße das Kontextmenü und wählen den Eintrag **Graph**.



Daraufhin öffnet sich ein weiteres Fenster, welches den zeitlichen Verlauf der Kenngröße dargestellt.



Indem Sie mit der linken Maustaste im aktuellen Graph eine Periode markieren, bekommen Sie deren Werte in der Statistik separat angezeigt.

Hinweis: Bitte beachten Sie, dass die angezeigte Werte gelöscht werden, sobald der Dialog geschlossen wird. Für eine längere Überwachung lassen Sie das Fenster dauerhaft geöffnet. Der Dialog stellt maximal die Werte der letzen 24 Stunden dar.

Internet-Verbindung kontrollieren

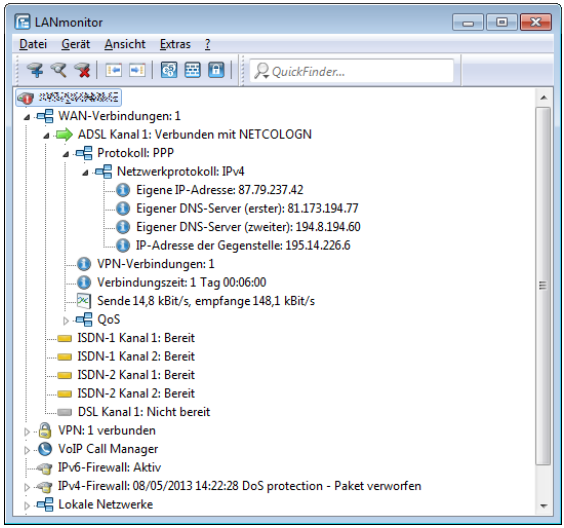
Als Beispiel für die Funktionen von LANmonitor wird in diesem Abschnitt gezeigt, welche Informationen LANmonitor über den Verbindungsaufbau zu Ihrem Internet-Provider bereitstellt

1. Starten Sie LANmonitor, z. B. mit einem Doppelklick auf das Desktop-Symbol.
2. Legen Sie über **Datei** > **Gerät hinzufügen** ein neues Gerät an und geben im sich öffnenden Fenster die IP-Adresse für das Gerät an, das Sie über-

wachen wollen. Falls die Konfiguration des Gerätes mit einem Passwort gesichert ist, geben Sie dieses gleich mit ein. LANmonitor legt automatisch einen neuen Eintrag in der Geräteliste an und zeigt zunächst den Zustand der Übertragungskanäle.

3. Starten Sie Ihren Web-Browser und geben Sie eine beliebige Webseite ein.
4. Wechseln Sie zurück zu LANmonitor und öffnen Sie den Zweig **WAN-Verbindungen** des Gerätes. Unter **ADLS Kanal x: Verbunden mit …** zeigt Ihnen LANmonitor nun an, wie auf einem Kanal eine Verbindung aufgebaut und welche Gegenstelle dabei gerufen wird.

Sobald die Verbindung hergestellt ist, zeigt der Kommunikationskanal durch das Pluszeichen vor dem Eintrag an, dass zu diesem Kanal weitere Informationen vorliegen. Durch Klicken auf das Pluszeichen oder Doppelklick auf einen entsprechenden Eintrag öffnen Sie eine baumartige Struktur, in der Sie verschiedene Informationen ablesen können.

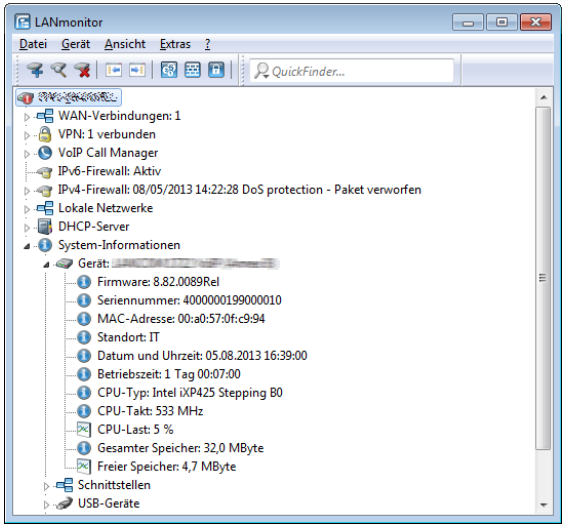


- In diesem Beispiel können Sie aus den Protokoll-Informationen zum PPP ablesen, welche IP-Adresse der Provider Ihrem Router für die Dauer der Verbindung zugewiesen hat und welche Adressen für DNS- und NBNS-Server übermittelt wurden.
- Unter den allgemeinen Informationen können Sie beobachten, mit welchen Übertragungsraten aktuell Daten mit dem Internet ausgetauscht werden.

- Durch einen Klick mit der rechten Maustaste auf den aktiven Kanal können Sie die Verbindung manuell trennen. Dazu benötigen Sie ggf. das Konfigurationspasswort.
- Wenn Sie ein Protokoll der LANmonitor-Ausgaben in Form einer Datei wünschen, starten Sie das Aktivitätsprotokoll (siehe auch *Geräteaktivitäten anzeigen* auf Seite 324).

Abfrage der CPU- und Speicherauslastung über SNMP

LANmonitor bietet Ihnen die Möglichkeit, die CPU- und Speicherauslastung eines Gerätes über SNMP abzufragen und anzuzeigen. Öffnen Sie dazu den Menübaum eines Gerätes, wechseln Sie in die **System-Informationen** und öffnen den Zweig **Gerät: …**.



Passwortschutz für SNMP-Lesezugriff

Der Lesezugriff auf ein Gerät über SNMP – z. B. über LANmonitor – kann über ein Passwort geschützt werden. Dabei werden die gleichen Benutzerdaten verwendet wie beim Zugriff auf LANconfig. Wenn der SNMP-Zugriff passwortgeschützt ist, können nur bei der Eingabe der entsprechenden Benutzerdaten Informationen über den Gerätezustand etc. über SNMP ausgelesen werden.

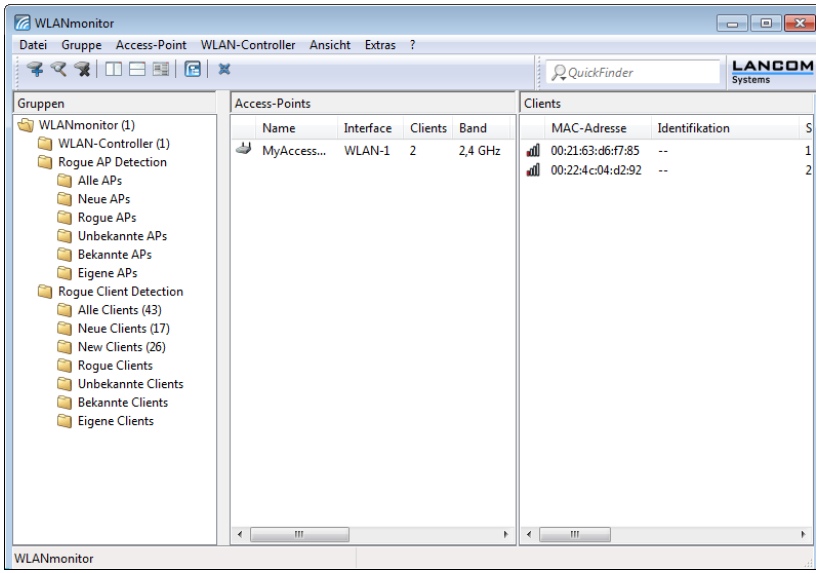
Die Benutzerinformationen können im LANmonitor für jedes Gerät getrennt eingetragen werden. Klicken Sie dazu mit der rechten Maustaste auf das gewünschte Gerät, wählen Sie im Kontextmenü den Eintrag **Optionen** und tragen Sie Ihre Benutzerdaten ein.

Hinweis: Die Zugriffsrechte im LANmonitor sind abhängig von den Rechten des Benutzers.

3.3 WLANmonitor - WLAN-Geräte überwachen

Der WLANmonitor ist ein separater Bestandteil von LANmonitor. Mit dem ihm überwachen Sie zentral den Status eines drahtlosen Netzwerkes (WLAN). Dabei können Sie sowohl Informationen über das gesamte Netzwerk als auch Detailinformationen zu einzelnen WLAN-Controllern, Access Points und eingeloggten Clients abrufen. Ebenso unterstützt Sie das Programm beim Aufspüren netzfremder Access Points (*Rogue AP Detection*).

Zudem bietet der WLANmonitor die Möglichkeit, Access Points zu Gruppen zusammenzufassen. Solche Gruppen können z. B. Etagen, Abteilungen oder Standorte umfassen. Dies erleichtert gerade bei großen WLAN-Infrastrukturen den Überblick über das gesamte Netzwerk.



Die Programmoberfläche von WLANmonitor ist in drei Spalten unterteilt:

In der linken Spalte (**Gruppen**) finden Sie eine Reihe vordefinierter die Gruppen-Ordner, in die WLANmonitor die verschiedenen Gerätetypen automatisch kategorisiert. Sie können diese Gruppen nach belieben umbenennen oder durch zusätzliche Gruppen erweitern.

In der mittleren Spalte (**Access-Points**) listet WLANmonitor die gefundenen Access Points auf. Zusätzlich erscheinen hier die wichtigsten Basisinformationen über die einzelnen Access Points:

- Name des Access Points
- Aktive physikalische Schnittstelle(n) (Interfaces)

  Hinweis: Geräte mit mehreren WLAN-Modulen tauchen mehrfach in der Liste auf. Jedes WLAN-Modul enthält dabei einen separaten Eintrag.

- Anzahl der auf ihm angemeldeten Clients
- Das verwendete Frequenzband
- Der verwendete Funkkanal
- Die vom Gerät ermittelte Sendeleistung

- Der vom Gerät ermittelte Rauschpegel
- Die derzeitige Auslastung des verwendeten Kanals (Kanallast)
- IP-Adresse des Access Point
- Der Aktivierungsstatus des *Background-Scans*

In der rechten Spalte (**Clients**) werden die auf dem ausgewählten Access Point eingeloggten Clients aufgelistet. Zu jedem Client werden folgende Informationen angezeigt:

- Verbindungsqualität in Form eines Balkendiagramms
- MAC-Adresse des WLAN-Clients
- Identifikation bzw. Name der eingeloggten Clients, sofern diese in der Access-Liste oder in einem RADIUS-Server eingetragen sind
- Signalstärke der Verbindung
- Name des Access-Points, auf dem der Client eingeloggt ist
- Bezeichnung des WLAN-Netzes (SSID)
- Für die Funkverbindung verwendetes Verschlüsselungsverfahren
- WPA-Version (WPA-1 oder WPA-2)
- Übertragungsrate beim Senden (TX-Rate)
- Übertragungsrate beim Empfangen (RX-Rate)
- Letzter Fehler, der im Zusammenhang mit dem Client aufgetreten ist
- IP-Adresse des WLAN-Clients

Sofern Sie keinen Access Point angewählt haben oder der betreffende Access Point über keinerlei Clients verfügt, zeigt Ihnen LANmonitor in der Client-Übersicht stattdessen sämtliche vorhandenen Clients an.

3.3.1 WLANmonitor starten

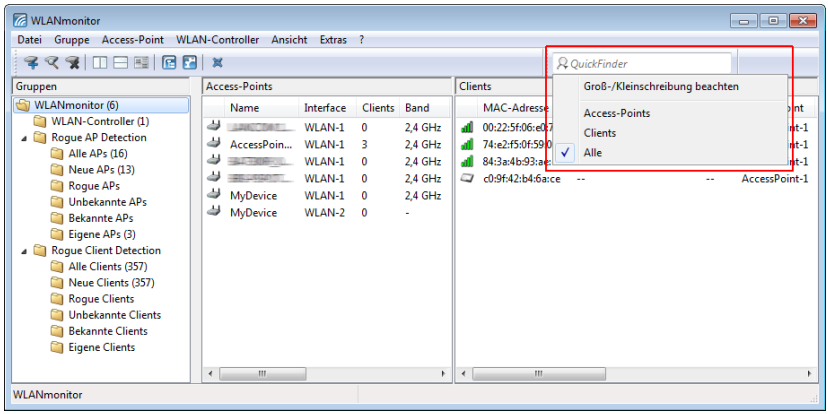
Der WLANmonitor ist Bestandteil des LANmonitor. Starten Sie den WLANmonitor aus dem LANmonitor über den Menüpunkt **Extras** > **WLANmonitor starten**; über die entsprechende Schaltfläche in der LANmonitor-Symbolleiste oder direkt über z. B. das Desktop-Symbol.

Hinweis: Alternativ kann der WLANmonitor von der Konsole aus mit folgendem Befehl gestartet werden: `[Installationspfad]lanmon -wlan`

Wenn Sie LANconfig geöffnet haben, können Sie auch mit der rechten Maustaste auf ein WLAN-Gerät klicken und **WLAN Gerät überwachen** wählen; dann startet der WLANmonitor ebenfalls.

3.3.2 QuickFinder im WLANmonitor

Der WLANmonitor erfasst sowohl Access Points als auch WLAN-Clients. Mit einem Klick auf die Lupe am linken Rand des Suchfensters öffnen Sie ein Kontextmenü zur Auswahl des Suchumfangs. Wählen Sie je nach Anwendung nur die Access Points, nur die Clients oder alle Einträge aus.



3.3.3 Rogue-Detection-Funktion

WLANmonitor bietet Ihnen die Möglichkeit, sogenannte "Rogue Access Points (APs)" und "Rogue Clients" in Ihrem Netz aufzuspüren. Als "Rogue" bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als Access Point oder Client Teilnehmer in einem WLAN zu werden.

- **Rogue Clients** sind Rechner mit WLAN-Adapter in Reichweite des eigenen WLANs, die sich bei einem der Access Points einzubuchen versuchen, um z. B. die Internetverbindung mit zu nutzen oder Zugang zu geschützten Bereichen des Netzwerks zu erhalten.
- **Rogue APs** sind Access Points, die z. B. von den Mitarbeitern einer Firma ohne Kenntnis und Erlaubnis der System-Administratoren an das Netzwerk angeschlossen werden und so über ungesicherte WLAN-Zugänge bewusst oder unbewusst Tür und Tor für potentielle Angreifer öffnen. Nicht ganz so gefährlich, aber zumindest störend, sind z B. Access Points in Reich-

weite des eigenen WLAN, die zu fremden Netzwerken gehören. Verwenden solche Geräte z. B. die gleiche SSID und den gleichen Kanal wie die eigenen APs (Default-Einstellungen), können die eigenen WLAN-Clients versuchen, sich beim fremden Netzwerk einzubuchen.

Da alle unbekannten Clients und Access Points in Reichweite des eigenen Netzwerks eine mögliche Bedrohung und Sicherleitslücke – oder zumindest aber eine Störung – darstellen, müssen diese Geräte erkannt werden, um ggf. weitere Maßnahmen zur Sicherung des eigenen Netzwerks einzuleiten. Die Informationen über die Clients in der Reichweite des eigenen Netzwerks werden automatisch in den internen Tabellen der Access Points gespeichert. Mit der Aktivierung des **Background Scans** werden auch die benachbarten Access Points erfasst und in der Scan-Tabelle gespeichert. Lesen Sie dazu auch das Kapitel *Background Scan für Access Points aktivieren* auf Seite 370.

Mit dem WLANmonitor lassen sich diese Informationen sehr komfortabel auswerten, indem das Programm solche Access Points und Clients in Kategorien wie z. B. 'Bekannt', 'Unbekannt' oder 'Rogue' einteilt.

Die Gruppe "Rogue AP Detection"

Für die Organisation der Rogue Access Points nutzt WLANmonitor die folgenden vordefinierten (Unter-)Gruppen:

- **Alle APs**: Enthält die Übersicht der APs aller gescannten WLANs und stellt damit die Obermenge aller nachfolgenden Gruppen dar. Die APs sind entsprechend ihrer Gruppenzugehörigkeit eingefärbt.
- **Neue APs**: Enthält neue unbekannte und unkonfigurierte WLANs. Die zugehörigen APs sind gelb eingefärbt.
- **Rogue APs**: Enthält WLANs, die als Rogue erkannt wurden und dringend zu beobachten sind. Die zugehörigen APs sind rot eingefärbt.
- **Unbekannte APs**: Enthält WLANs, bei denen weitere Untersuchungen notwendig sind. Die zugehörigen APs sind grau eingefärbt.
- **Bekannte APs**: Enthält WLANs, welche keine Gefahr darstellen. Die zugehörigen APs sind grau eingefärbt.
- **Eigene APs**: Enthält neue eigene WLANs von APs, die der WLANmonitor beobachtet. Die zugehörigen APs sind grün eingefärbt.

Hinweis: Wenn sich bei einem AP ein Parameter ändert (z. B. die Sicherheitseinstellung), dann wird er wieder als neu gefundener AP angezeigt.

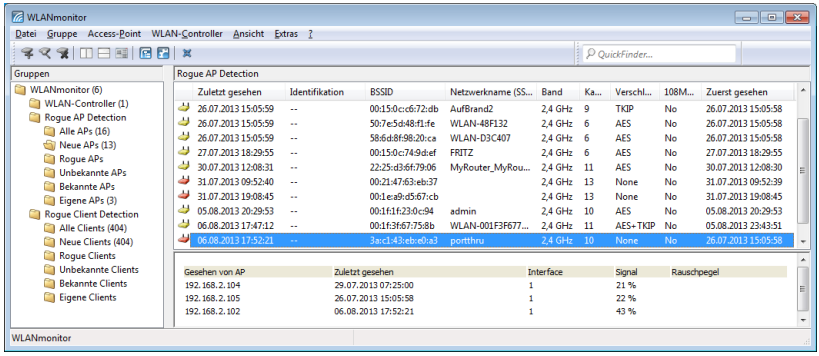
Innerhalb der einzelnen Gruppen zeigt WLANmonitor die folgenden Informationen zu den Rogue APs an:

- Zeitpunkt der ersten und letzten Erkennung
- Name des APs (Identifikation)
- MAC-Adresse des AP für dieses WLAN (BSSID)
- Bezeichnung des WLANss (SSID)
- Das verwendete Frequenzband
- Der verwendete Funkkanal
- Für die Funkverbindung verwendetes Verschlüsselungsverfahren
- Verwendung des 108 Mbps-Modus

Wenn Sie einen Listeneintrag anklicken, zeigt Ihnen WLANmonitor die folgenden Detailinformationen an:

- IP-Adressen der APs, die das betreffende WLAN gescannt haben
- Zeitpunkt der letzten Entdeckung bzw. des letzten Scans
- WLAN-Interface, auf dem der Scan durchgeführt wurde
- Signalstärke, mit welcher die APs das WLAN empfangen haben
- Rauschpegel

Sie haben die Möglichkeit, die gefundenen WLANs je nach Status in eine entsprechenden Gruppe verschieben. Innerhalb der einzelnen Gruppen legen Sie über das Kontextmenü (rechte Maustaste) eigene Gruppen an, mit Ausnahme der Gruppe **Alle APs**.



Die Gruppe "Rogue Client Detection"

Für die Organisation der Rogue Clients nutzt WLANmonitor die folgenden vordefinierten (Unter-)Gruppen:

- **Alle Clients**: Enthält die Übersicht aller gesehener Clients und stellt damit die Obermenge aller nachfolgenden Gruppen dar. Die Clients sind entsprechend ihrer Gruppenzugehörigkeit eingefärbt.
- **Neue Clients**: Enthält neue unbekannte Clients. Die zugehörigen Clients sind gelb eingefärbt.
- **Rogue Clients**: Enthält Clients, die als Rogue erkannt wurden und dringend zu beobachten sind. Die zugehörigen Clients sind rot eingefärbt.
- **Unbekannte Clients**: Enthält Clients, bei denen weitere Untersuchungen notwendig sind. Die zugehörigen Clients sind grau eingefärbt.
- **Bekannte Clients**: Enthält Clients, welche keine Gefahr darstellen. Die zugehörigen Clients sind grau eingefärbt.
- **Eigene Clients**: Enthält neue eigene Clients, die bei Access Points assoziiert sind, welche der WLANmonitor beobachtet. Die zugehörigen Clients sind grün eingefärbt.

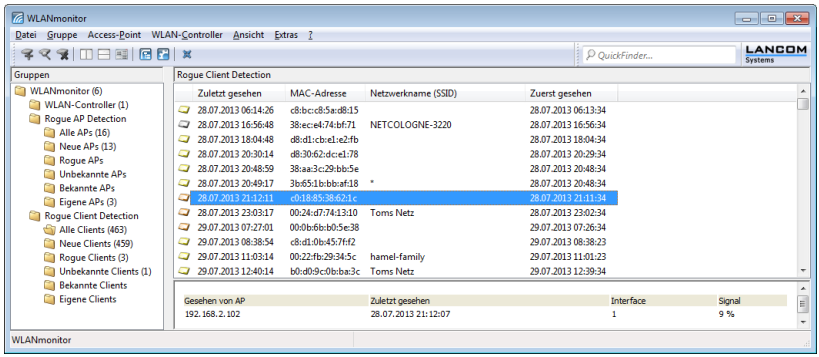
Innerhalb der einzelnen Gruppen zeigt WLANmonitor die folgenden Informationen zu den Rogue Clients an:

- Zeitpunkt der ersten und letzten Erkennung
- MAC-Adresse des Clients
- Bezeichnung des WLAN-Netzes (SSID)

Wenn Sie einen Listeneintrag anklicken, zeigt Ihnen WLANmonitor die folgenden Detailinformationen an:

- IP-Adressen der Access Points, die den betreffende Client gesehen haben
- Zeitpunkt der letzten Entdeckung
- WLAN-Interface, auf dem der Client entdeckt wurde
- Signalstärke, mit welcher die APs das WLAN-Netz empfangen haben

Sie können die gefundenen Clients je nach Status in eine entsprechenden Gruppe verschieben. Innerhalb der einzelnen Gruppen können Sie über das Kontextmenü (rechte Maustaste) eigene Gruppen anlegen, mit Ausnahme der Gruppe **Alle Clients**.



3.3.4 Die Menüstruktur im WLANmonitor

Über die Menüleiste verwalten Sie WLAN-Geräte und deren Konfigurationen, und passen sowohl das Aussehen als auch die Funktionsweise von WLANmonitor an.

Datei

Unter diesem Menüpunkt beenden Sie LANmonitor.

Beenden

Schließt und beendet WLANmonitor.

Gruppe

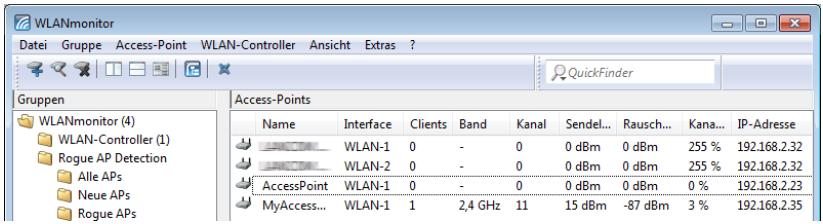
Die Bearbeitung von Gruppen umfasst die folgenden Funktionen:

- Gruppe hinzufügen
- Gruppe entfernen
- Gruppe umbenennen

WLANmonitor bietet Ihnen die Möglichkeit, alle verfügbaren Access Points unabhängig von ihren physikalischen Standorten anzuordnen. Das erleichtert den Überblick im Netzwerk und hilft bei der Lokalisierung von evtl. auftretenden Problemen. Zudem lassen sich WLAN-Informationen gruppenweise abrufen.

Sie können Ihre Access Points z. B. nach Abteilungen, Standorten oder Ihrem Verwendungszweck (z. B. öffentlicher Hotspot) gruppieren.

In der linken Spalte des WLANmonitors (Gruppen-Baum) werden die Gruppen angezeigt. Von der obersten Gruppe 'WLANmonitor' ausgehend können Sie über den Menüpunkt **Datei** > **Gruppe** hinzufügen neue Untergruppen anlegen und so eine Struktur aufbauen. Die bei der Suche gefundenen Access-Points befinden sich jeweils in der aktuell ausgewählten Gruppe im Gruppen-Baum.



Hinweis: Die bereits erkannten Access Points können Sie per Drag and Drop in die gewünschte Gruppe ziehen.

Um die Zuordnung von Access-Points und Clients zu erleichtern, können Sie ein Gerät mit der Maus markieren. Das jeweilige Pendant wird dann in den entsprechend verknüpften Listen ebenfalls markiert:

- Wenn in der Access-Point-Liste ein Access Point markiert wird, werden alle auf diesem Gerät eingeloggten Clients in der Client-Liste ebenfalls markiert.
- Wenn in der Client-Liste ein Client markiert wird, wird in der Access-Point-Liste der Access Point markiert, auf dem der gewählte Client eingeloggt ist.

Gruppe hinzufügen

Fügt eine Gruppe hinzu.

Gruppe entfernen

Entfernt eine Gruppe.

Gruppe umbenennen

Hier können Sie den Namen einer Gruppe ändern.

Access-Point

Unter diesem Menüpunkt verwalten Sie sämtliche Access Points.

Access-Point hinzufügen

Wählen Sie diesen Menüpunkt, um einen Access Point zur Liste hinzuzufügen, den WLANmonitor nicht automatisch erkannt hat. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 261).

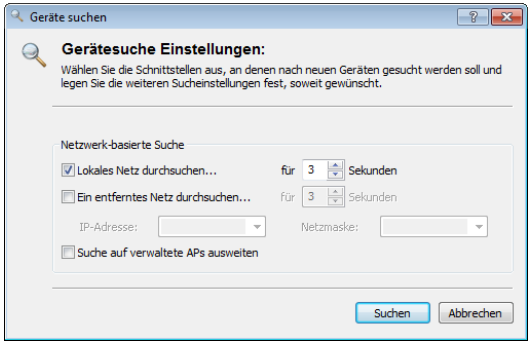
Hinweis: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

Access Point entfernen

Entfernt den markierten Access Point aus der Liste.

Access Point suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach verfügbaren Access Points im Netz.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz
- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Hinweis: Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle Access Points aktualisieren

Aktualisiert die Liste aller Access Points.

Aktualisieren

Aktualisiert die Anzeige des markierten Access Points.

Eigenschaften

Hier können Sie sich die Eigenschaften des ausgewählten Access Points anzeigen lassen. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 261). Zudem erhalten Sie hier Informationen zum Gerät und zum Hersteller.

Hinweis: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

WLAN-Controller

Unter diesem Menüpunkt verwalten Sie die WLAN-Controller Ihres Netzes.

WLAN-Controller hinzufügen

Klicken Sie unter **Gruppen** auf den Ordner **WLAN-Controller** und wählen Sie dann in der Menüleiste den Menüpunkt **WLAN-Controller hinzufügen**, um einen WLAN-Controller zur Liste hinzuzufügen, den WLANmonitor nicht automatisch erkannt hat. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 261).

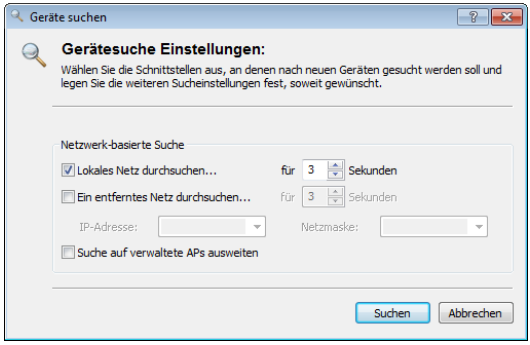
Hinweis: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

WLAN-Controller entfernen

Entfernt den markierten WLAN-Controller.

WLAN-Controller suchen

Über diesen Menüpunkt starten Sie die automatische Suche nach verfügbaren WLAN-Controllern im Netz.



Wählen Sie aus, wo nach Geräten gesucht werden soll:

- Im lokalen Netz

- In einem entfernten Netz

  Wenn Sie ein entferntes Netz durchsuchen wollen, müssen Sie die Adresse des Netzwerkes und die zugehörige Netzmaske angeben.

- Sie können die Suche bei Bedarf auch auf verwaltete Access Points (APs) ausweiten.

Klicken Sie auf **Suchen**, um die Suche zu starten. Die gefundenen Geräte werden automatisch der Liste hinzugefügt.

Hinweis: Wenn ein Gerät gefunden wird, das bereits in der Liste vorhanden ist, wird es nicht ein zweites Mal der Liste hinzugefügt. Daher kann es sein, dass weniger Geräte neu hinzukommen, als während des Suchvorgangs gemeldet werden.

Alle WLAN-Controller aktualisieren

Aktualisiert die Liste aller WLAN-Controller.

Aktualisieren

Aktualisiert die Anzeige des markierten WLAN-Controllers.

Eigenschaften

Hier können Sie sich die Eigenschaften des ausgewählten WLAN-Controllers anzeigen lassen. Die dazugehörigen Einstellungsmöglichkeiten sind mit denen von LANmonitor unter **Datei** > **Gerät hinzufügen** > **Allgemein** identisch (siehe *Allgemein* auf Seite 261). Zudem erhalten Sie hier Informationen zum Gerät und zum Hersteller.

Hinweis: Wenn Sie Benutzernamen und Passwort dauerhaft speichern, erhält jeder Nutzer Zugang zu dem Gerät, der auch WLANmonitor ausführen darf.

Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der WLANmonitor-Bedienoberfläche an.

Symbol im Systray anzeigen

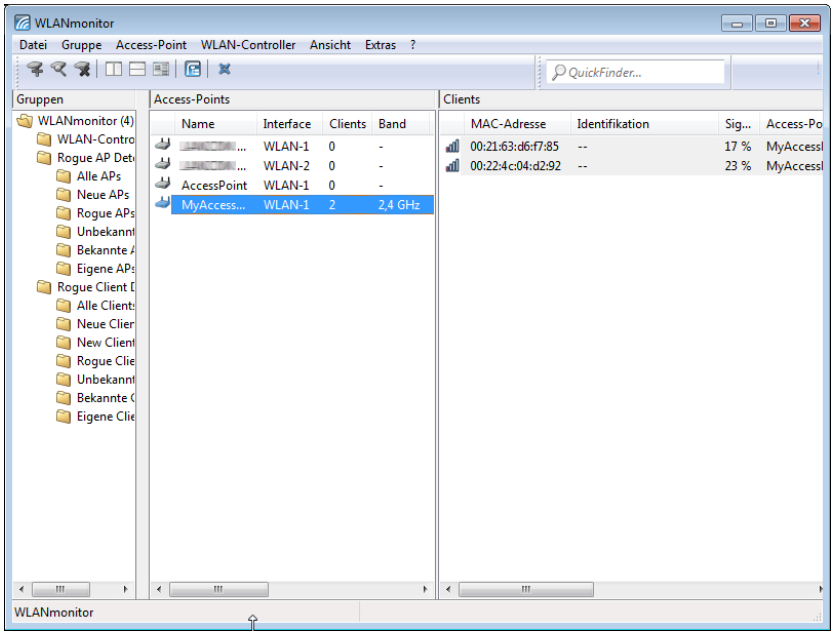
Zeigt das Symbol im Systray an.

WLANmonitor in den Systray minimieren

Wenn Sie diese Einstellung aktivieren, wird WLANmonitor beim Minimieren im Systray anstelle der Taskleiste abgelegt.

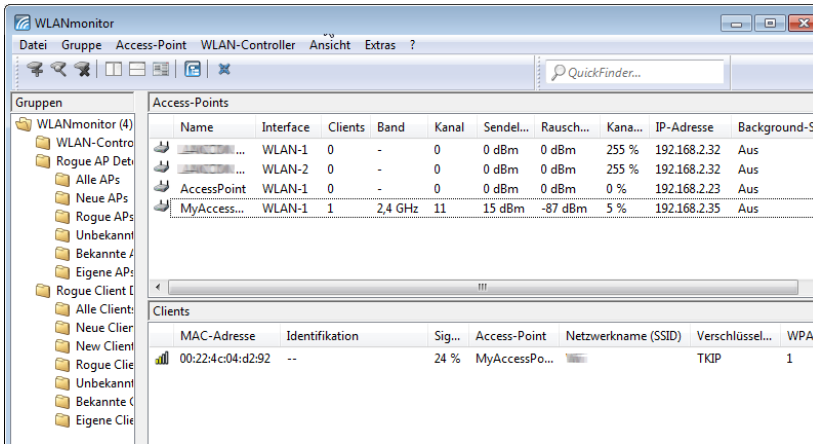
Fenster vertikal ausrichten

Richtet das Fenster vertikal aus, d. h. die Listen für Access Points und Clients werden nebeneinander dargestellt.



Fenster horizontal ausrichten

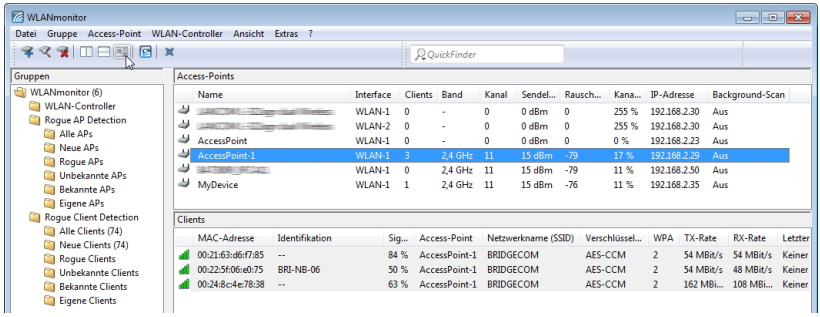
Richtet das Fenster horizontal aus, d. h. die Listen für Access Points und Clients werden untereinander dargestellt.



Zeilen markieren/ filtern

Mit dieser Option filtern Sie die Liste der angezeigten Access Points oder Clients.

- Markieren Sie eine Access Point und rufen Sie die Option **Ansicht** > **Zeilen markieren/Filtern** auf. Die Liste der Clients zeigt dann nur noch die Clients, die beim gewählten Access Point angemeldet sind.
- Markieren Sie eine Client und rufen Sie die Option **Ansicht** > **Zeilen markieren/Filtern** auf. Die Liste der Access Points zeigt dann nur noch den Access Point, bei dem der gewählte Client angemeldet ist.



Symbolleiste

Blendet die Symbolleiste aus bzw. ein. Lesen Sie hierzu auch *Die Symbolleiste im LANmonitor* auf Seite 343.

Statusleiste

Blendet die Statusleiste aus bzw. ein.

Extras

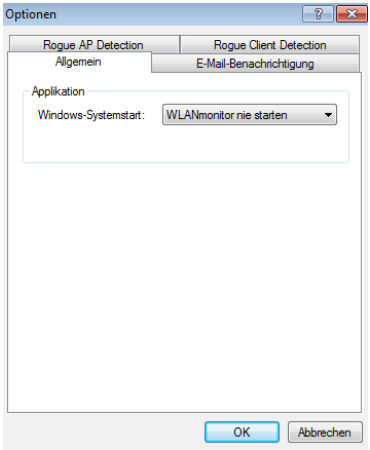
Unter diesem Menüpunkt starten Sie weitere Bestandteile von LCMS und konfigurieren z. B. das Verhalten von WLANmonitor bei Entdecken unbekannter oder unkonfigurierter Access Points.

Optionen

Unter diesem Menüpunkt nehmen Sie die programmbezogenen Einstellungen für WLANmonitor vor.

Allgemein

In diesem Dialog nehmen Sie die allgemeinen Einstellungen zum Programm vor.



Windows-Systemstart

WLANmonitor kann beim Start des Betriebssystems automatisch geladen werden. Folgende **Windows-Systemstart**-Arten stehen Ihnen zur Verfügung:

- **WLANmonitor nie starten**

  Die Anwendung startet nicht automatisch mit dem Betriebssystem, sondern muss manuell gestartet werden.

- **WLANmonitor immer starten**

  Die Anwendung startet immer automatisch nach dem erfolgreichen Start des Betriebssystems.

- **WLANmonitor wie zuvor starten**

  Die Anwendung startet in dem Zustand, in dem Sie sich beim Herunterfahren des Betriebssystems befand. War die Anwendung aktiv, wird sie wieder gestartet; war sie nicht aktiv, wird sie auch nicht automatisch gestartet.

Hinweis: Beim Wechsel auf eine Einstellung, die ein automatisches Starten der Anwendung ermöglicht, wird ein Eintrag in der Registry des Betriebssystems vorgenommen. Firewall-Applikationen auf dem Rechner oder die Betriebssysteme selbst (Windows XP, Windows Vista oder Windows 7) können diesen Eintrag ggf. als Angriff deuten und eine Warnung ausgeben bzw. den Eintrag verhindern. Um das gewünschte Startverhalten zu ermöglichen, ignorieren Sie diese Warnungen bzw. lassen Sie die durchzuführenden Aktionen zu.

Dialog-Sprache

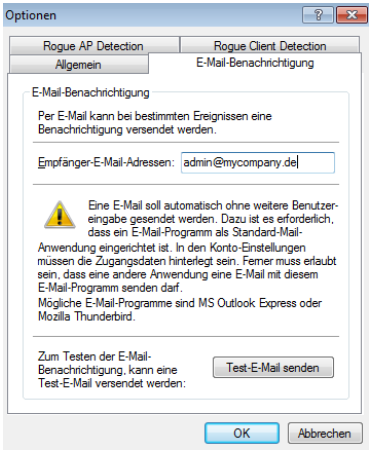
Hierüber ändern Sie die Sprache des Benutzer-Interfaces (GUI). Die Auswahl der Sprache erfolgt normalerweise automatisch anhand der Sprache des Betriebssystems.

Hinweis: Damit die Änderung der Spracheinstellung wirksam wird, ist ein Neustart der Anwendung erforderlich.

Hinweis: Diese Einstellung ist nur in Windows-Versionen bis XP vorhanden. Ab Vista übernimmt WLANmonitor die Spracheinstellungen aus LANconfig.

E-Mail-Benachrichtigung

In diesem Dialog nehmen Sie Einstellungen zur Alarmierungsfunktion im WLANmonitor vor.



Der WLANmonitor kann den Administrator automatisch per E-Mail informieren, wenn ein unbekannter oder unkonfigurierter Access Point entdeckt wird. Aktivieren Sie diese Option, wenn der WLANmonitor unbekannte oder unkonfigurierte Access Points per E-Mail melden soll.

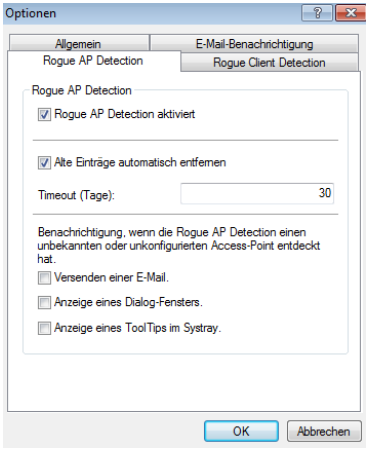
- **Empfänger-E-Mail-Adressen**: Geben Sie hier die E-Mail-Adresse(n) des Administrators an, der über die Rogue AP Detection informiert werden soll. Mehrere E-Mail-Adressen werden durch Kommata getrennt.

Hinweis: Für die Alarmierung per E-Mail muss auf dem Rechner, auf dem der WLANmonitor läuft, ein Mail-Client (z. B. MS Outlook Express oder Mozilla Thunderbird) als Standard-Mail-Client eingerichtet sein, der den automatischen Mail-Versand erlaubt.

- **Test-E-Mail senden**: Manche Mail-Clients erfordern vor dem Versand durch Dritt-Anwendungen eine Bestätigung durch den Benutzer. Testen Sie die Alarmierungsfunktion mit dieser Schaltfläche.

Rogue AP Detection

In diesem Dialog nehmen Sie Einstellungen zur "Rogue AP Detection" vor. Weitere Informationen zu dieser Funktion finden Sie im Kapitel *Rogue-Detection-Funktion* auf Seite 352.



Der Dialog bietet Ihnen folgende Einstellungsmöglichkeiten:

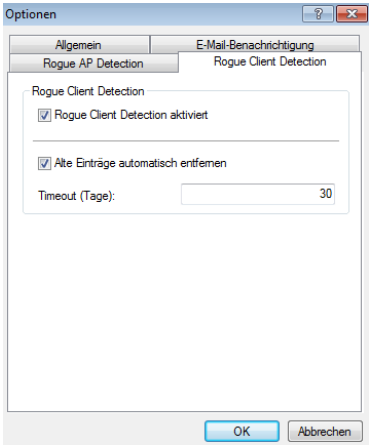
- **Rogue AP Detection aktiviert**: Aktiviert die automatische Suche nach Rogue Access Points.
- **Alte Einträge automatisch entfernen**: Wenn aktiviert, entfernt WLANmonitor automatisch Einträge zu Access Points aus den Gruppen, deren Sichtung länger zurückliegt als die unter **Timeout** angegebenen Tage.

Zudem haben Sie die Möglichkeit, festzulegen, auf welche Art und Weise WLANmonitor Sie bei Entdecken eines unbekannten oder unkonfigurierten Access Points benachrichtigt.

- **Versenden einer E-Mail**: Versendet eine Mitteilung an die unter **E-Mail-Benachrichtigung** hinterlegte(n) Empfänger-Adresse(n).
- **Anzeige eines Dialog-Fensters**: Öffnet ein Popup-Fenster.
- **Anzeige eines ToolTips im Systray**: Zeigt einen ToolTip im Systray an.

Rogue Client Detection

In diesem Dialog nehmen Sie Einstellungen zur "Rogue Client Detection" vor. Weitere Informationen zu dieser Funktion finden Sie im Kapitel *Rogue-Detection-Funktion* auf Seite 352.



Der Dialog bietet Ihnen folgende Einstellungsmöglichkeiten:

- **Rogue Client Detection aktiviert**: Aktiviert die automatische Suche nach Rogue Client.
- **Alte Einträge automatisch entfernen**: Wenn aktiviert, entfernt WLANmonitor automatisch Einträge zu Access Points aus den Gruppen, deren Sichtung länger zurückliegt als die unter **Timeout** angegebenen Tage.

LANmonitor starten

Startet LANmonitor. Mehr Informationen dazu erhalten Sie im Kapitel *LANmonitor - Geräte im LAN überwachen* auf Seite 313.

LANconfig starten

Startet LANconfig. Mehr Informationen dazu erhalten Sie im Kapitel *LANconfig - Geräte konfigurieren* auf Seite 208.

Hilfe

Unter diesem Menüpunkt finden Sie weitere Hilfe zum Programm und lassen sich Informationen zur Software anzeigen.

Hilfethemen

Über diesen Menüpunkt gelangen Sie zu den Hilfethemen. Alternativ können Sie auch F1 drücken.

Info

Unter diesem Menüpunkt werden Ihnen die Version und das Builddatum der Software angezeigt.

3.3.5 Die Symbolleiste im WLANmonitor

Die Symbolleiste im WLANmonitor beinhaltet die folgenden Funktionen:

- Gerät hinzufügen
- Geräte suchen
- Gerät entfernen
- Fenster vertikal ausrichten
- Fenster horizontal ausrichten
- Zeilen markieren/ filtern
- LANmonitor starten
- Fenster in den Systray minimieren
- QuickFinder

Hinweis: Unter **Ansicht** > **Symbolleiste** blenden Sie die Symbolleiste ein- oder aus.

3.3.6 Das Kontextmenü im WLANmonitor

Wenn Sie mit der rechten Maustaste auf eine Gerät im WLANmonitor klicken, dann öffnet sich das Kontextmenü.

Der Inhalt des Kontextmenüs hängt vom Typ des gewählten Gerätes ab: Im Falle eines markierten Access Points gleicht es dem Menü **Access Point**, im Falle eines markierten WLAN-Controllers dem Menü **WLAN-Controller**.

3.3.7 WLANmonitor Tastaturbefehle

Alt+F4	Beenden
Einfg	Gruppe hinzufügen
Entf	Gruppe entfernen
F2	Gruppe umbenennen
Einfg	Access Point hinzufügen
Entf	Access Point entfernen
F3	Access-Points suchen
F5	Alle Access-Points aktualisieren
Strg+F5	Aktualisieren
Space	Access Point > Optionen
Einfg	WLAN-Controller hinzufügen
Entf	WLAN-Controller entfernen
F3	WLAN-Controller suchen
Space	WLAN-Controller > Optionen
F7	Extras > Optionen
F1	Hilfethemen

3.3.8 Anwendungskonzepte für den WLANmonitor

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für WLANmonitor.

Background Scan für Access Points aktivieren

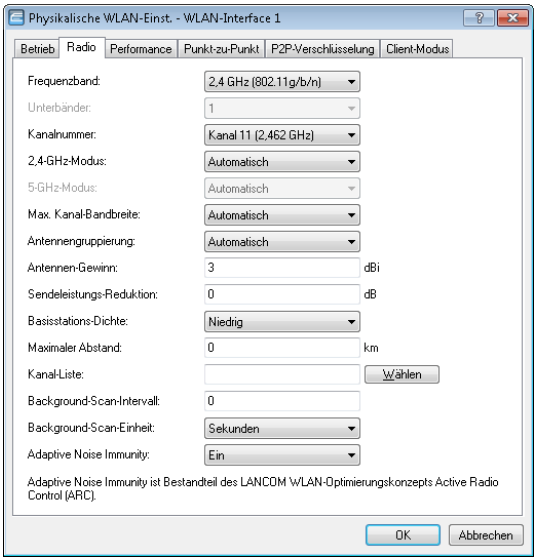
Zur Erkennung anderer Access Points in der eigenen Funkreichweite können Acess Points und Wireless Router die empfangenen Beacons (Management-Frames) aufzeichnen und in der Scan-Tabelle speichern. Da diese Aufzeichnung im Hintergrund neben der 'normalen' Funktätigkeit der Access Points abläuft, wird diese Funktion auch als "Background Scan" bezeichnet. Für

Wireless-Router im Access Point-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue-AP-Detection eingesetzt. Ohne die Aktivierung des Background Scans ist z. B. die Rogue Detection im WLANmonitor auf die Erkennung von Rogue Clients beschränkt.

Zur Konfiguration des Background Scans definieren Sie eine Zeit, innerhalb der alle verfügbaren WLAN-Kanäle einmal auf die empfangenen Beacons hin gescannt werden. Das nachfolgende Tutorial beschreibt, wie Sie diese Zeit setzen.

1. Starten Sie LANconfig und öffnen Sie die manuelle Konfiguration für Ihr Gerät.
2. Öffnen Sie den Dialog **Wireless-LAN** > **Allgemein** und wählen Sie unter **Physikalische WLAN-Einst.** das WLAN-Interface, für das die Background Scanning aktivieren wollen.
3. Wechseln Sie im sich öffnenden Dialogfenster zum Reiter **Radio**.
4. Wählen Sie aus der Auswahlliste **Background-Scan-Einheit** eine Zeiteinheit aus und geben Sie im Eingabefeld **Background-Scan-Intervall** eine dazugehörige Dauer ein.

   Das Scan-Intervall sollte der Zeitspanne entsprechen, innerhalb derer unbefugte Access Points erkannt werden sollen, z. B. `3600 Sekunden`. Der kleinste sinnvolle Wert sowohl im 2,4-GHz- als auch 5-GHz-Band beträgt `260 Sekunden`. Dieser Wert führt bei möglichen 13 Kanälen dazu, dass alle 20 Sekunden ein weiterer Kanal gescannt wird (Intervall / Anzahl Kanäle).



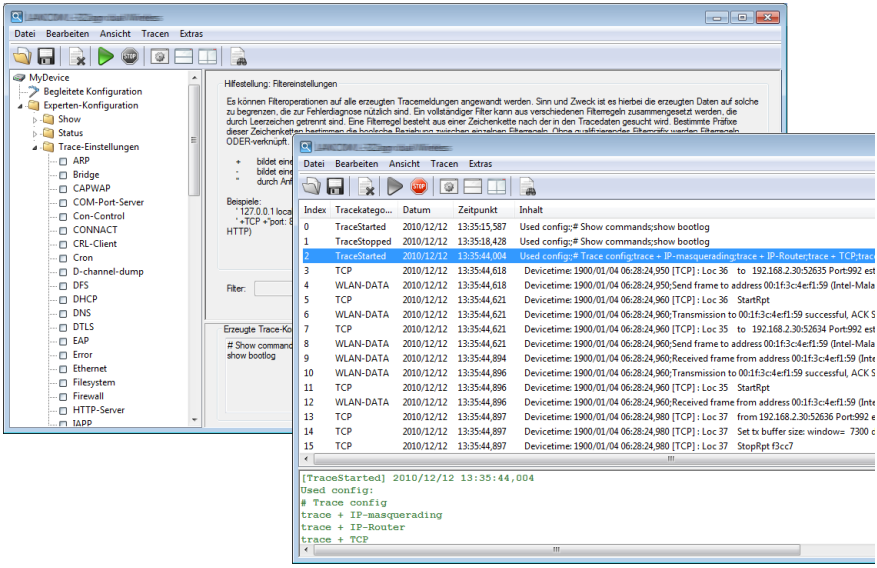
5. Schließen Sie alle Dialoge und laden Sie die Konfiguration auf Ihr Gerät zurück.

Fertig! Fortan sucht Ihr WLAN-Gerät innerhalb des angegebenen Scan-Intervalls zyklisch die aktuell ungenutzen Frequenzen des aktiven Bandes nach erreichbaren Access Points ab.

3.4 LANtracer - Tracen mit LANconfig und LANmonitor

Mit der Trace-Funktion in LANconfig und LANmonitor können Sie über die normalen Trace-Funktionen hinaus, wie sie von der Kommandozeilen-Oberfläche bekannt sind, weitere Funktionen nutzen, die eine Erstellung und Auswertung der Traces erleichtern. So lässt sich z. B. die aktuelle Trace-Konfiguration, mit der die benötigten Trace-Befehle aktiviert werden, in einer Konfigurationsdatei speichern. Ein erfahrener Service-Techniker kann eine solche Trace-Konfiguration vorbereiten und einem weniger erfahrenen Anwender zur Verfügung stellen, der damit die gewünschte Trace-Ausgabe eines Gerätes erzeugt. Auch Trace-Ergebnisse lassen sich komfortabel in

einer Datei speichern, um sie an den Techniker zur Auswertung zurückzugeben.



3.4.1 LANtracer starten

Die Ausgabe von Traces kann sehr komfortabel über LANconfig oder LANmonitor vorgenommen werden. Um das Trace-Fenster für ein Gerät zu öffnen, klicken Sie mit der rechten Maustaste auf den Eintrag des Gerätes und wählen im Kontext-Menü den Eintrag **Trace-Ausgabe erstellen**.

Hinweis: Zur Abfrage von Traces über LANconfig oder LANmonitor muss ein (bestenfalls SSL-verschlüsselter) Telnet-Zugriff auf das Gerät erlaubt sein. Beim Starten des Trace-Dialogs versuchen LANconfig oder LANmonitor, zunächst eine SSL-verschlüsselte Telnet-Verbindung zum Gerät aufzubauen. Falls das Gerät keine SSL-Verbindungen unterstützt, wechseln LANconfig oder LANmonitor automatisch auf unverschlüsseltes Telnet. Wenn der Konfigurationszugriff auf das Gerät passwortgeschützt ist, sind zudem die Zugangsdaten für einen Administrator mit Trace-Rechten erforderlich.

Um nachfolgende Analysen durch detaillierte Trace-Daten zu vereinfachen, können Sie den Assistenten für die **Begleitete Konfiguration** starten. Der

Assistent führt Sie durch mehrere Dialoge, in denen Sie bequem Trace-Parameter zur Analyse bestimmter Probleme auswählen. Nach Abschluss der Eingaben aktiviert der Assistent automatische die entsprechende Trace-Konfiguration.

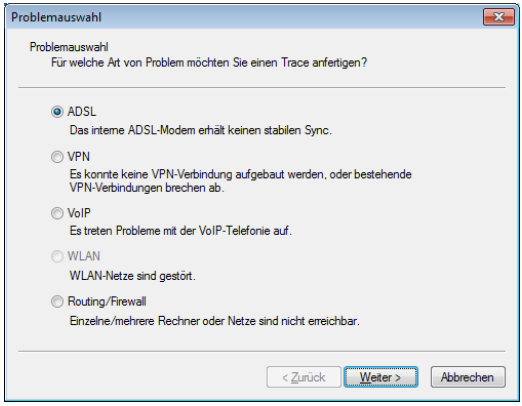
3.4.2 Arbeiten mit LANtracer

Das nachfolgende Kapitel beschreibt allgemein, wie Sie bestimmte Funktionalitäten von LANtracer für die Ausgabe und Sicherung von Traces nutzen.

Begleitete Konfiguration der Trace-Ausgaben

Als Alternative zur Experten-Konfiguration der Trace-Ausgaben bietet LANtracer Ihnen auch die Möglichkeit einer begleiteten (assistierten) Konfiguration. Dieser Assistent vereinfacht die Erstellung von Trace-Ausgaben, indem er Ihnen eine Auswahl möglicher Probleme anzeigt, für die Sie Diagnose-Informationen benötigen. Der Assistent setzt daraufhin für Sie die notwendigen Parameter bzw. Einstellungen in der Experten-Konfiguration.

Zum Starten des Assistenten klicken Sie im linken Fensterteil von LANtracer auf **Begleitete Konfiguration** > **Assistent starten** und navigieren weiter zur **Problemauswahl**.



Experten-Konfiguration der Trace-Ausgaben

Über die Einstellungen des Assistenten **Begleitete Konfiguration** hinaus können Sie – mit Hilfe der Experten-Konfiguration – die Traces und weitere Anzeigen genauer einstellen. Die Experten-Konfiguration unterteilt sich in drei Bereiche: ***Show***, ***Status*** und ***Trace-Einstellungen***.

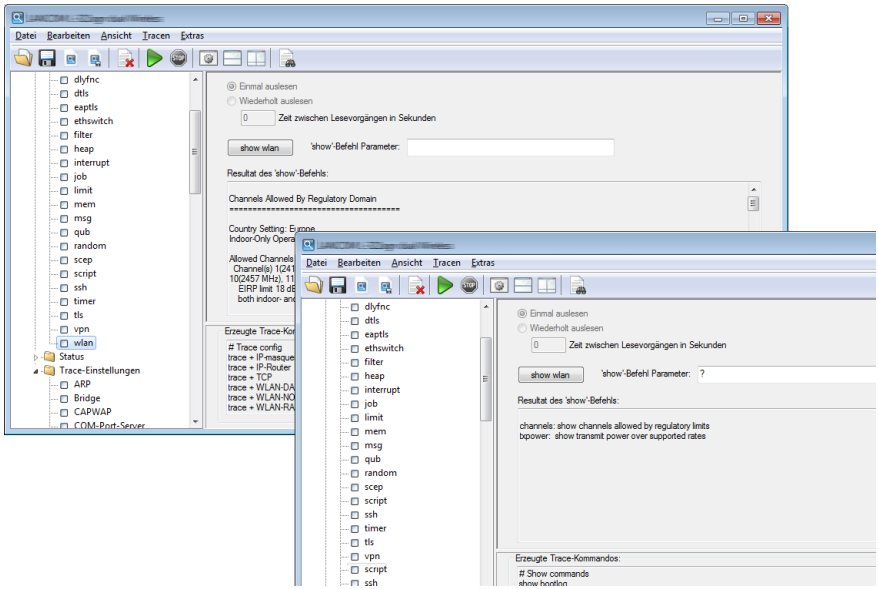
Show

Für jeden Gerätetyp können Sie bestimmte Informationen mit einem Show-Kommando aufrufen – üblicherweise werden die Show-Kommandos auf der Kommandozeile (Telnet) angewendet. In der Experten-Konfiguration des Traces kann der Aufruf dieser Show-Kommandos sehr bequem über die grafische Windows-Oberfläche erfolgen.

- Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Show-Kommandos (z. B. **Show** > **wlan**) und dann den show-Button (z. B. **show wlan**), um die aktuelle Ausgabe des Show-Kommandos aufzurufen.
- Je nach gewähltem Eintrag können bzw. müssen noch ergänzende Parameter angegeben werden. Um eine Übersicht der möglichen Parameter zu erhalten, geben Sie in das Eingabefeld ein Fragezeichen ('?') ein und klicken den show-Button.

Um die Ausgabe eines Show-Kommandos in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen. Für jedes aktivierte Show-Kommando ist separat einstellbar, ob es nur einmal beim Start des Traces oder in regelmäßigen Intervallen (in Sekunden) ausgeführt wird.

Hinweis: Die Einstellungen der Show-Kommandos werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert.



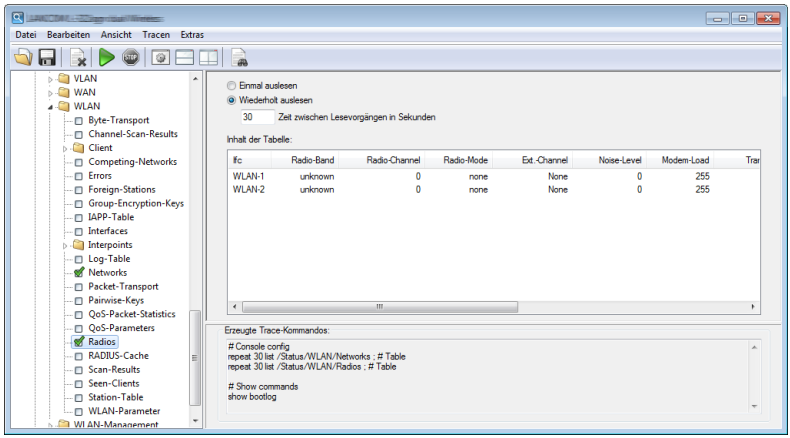
Status

Über die Kommandozeile (Telnet) oder über WEBconfig können Sie umfangreiche Statusinformationen und Statistiken über ein Gerät abfragen. Alle verfügbaren Status-Informationen lassen sich aber auch über den Trace-Dialog einsehen.

- Klicken Sie im linken Bereich des Trace-Dialogs auf den Namen eines Status-Eintrags, um den aktuellen Inhalt der Tabelle bzw. des Wertes anzuzeigen.

Um die Ausgabe des Status-Eintrags in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen. Für jeden aktivierten Status-Eintrag ist separat einstellbar, ob er nur einmal beim Start des Traces oder in regelmäßigen Intervallen (in Sekunden) ausgelesen wird.

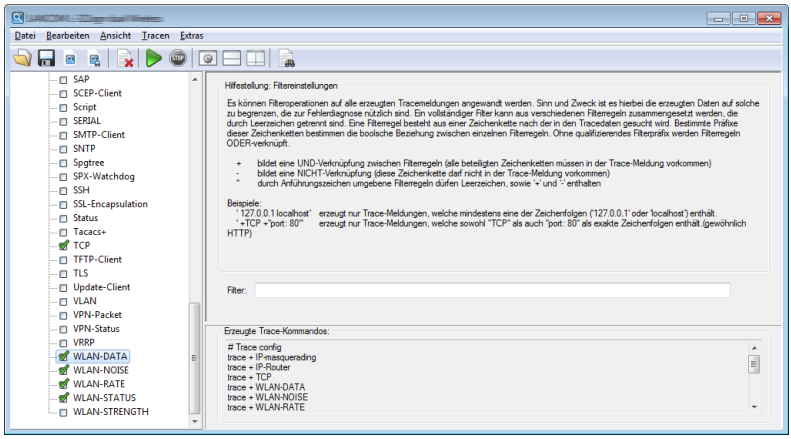
Hinweis: Die Einstellungen der Status-Informationen werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert. Äquivalent dazu wird die Ausgabe der Status-Informationen zusammen mit den eigentlichen Trace-Daten gespeichert.



Trace-Einstellungen

Im Bereich der Trace-Einstellungen können Sie jene Traces aktivieren, die für das aktuelle Gerät ausgegeben werden sollen. Um die Trace-Kommandos in die Trace-Ergebnisse zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dessen Namen.

Zu jedem Trace können Sie außerdem einen Filter eingeben. Um z. B. nur die IP-Adresse einer bestimmten Workstation anzuzeigen, geben Sie die entsprechende IP-Adresse als Filter des IP-Router-Traces ein. Um mehr über die Filterfunktion zu erfahren, lesen Sie das Kapitel *Trace-Ausgabe filtern* auf Seite 378.



Trace-Ausgabe filtern

Die Ausgabe von Traces an der Kommadozeile oder im Trace-Dialog von LCMS ist in vielen Fällen sehr umfangreich, weil der Trace in kurzer zeitlicher Abfolge Informationen aus dem Gerät empfängt. Um die Ausgabe der Traces übersichtlicher zu gestalten, können Sie geeignete Filter anwenden. Die Filter basieren auf einer Suchfunktion, welche die Trace-Ausgaben nach relevanten Informationen untersucht und nur die gewünschten Aspekte darstellt.

Im folgenden Beispiel aktiviert der Administrator einen einfachen IP-Router-Trace auf einem Gerät mit drei Internetanbindungen und verschickt Pings an verschiedene Ziele. Die ungefilterte Trace-Ausgabe zeigt alle Pakete, die der IP-Router des Gerätes verarbeitet:

```
root@MyDevice:/
> trace # ip-router
IP-Router ON

root@MyDevice:/

>[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cde
Route: WAN Tx (INTERNET3)
```

```
[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1ccf
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1ccf
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:06,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cde
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1cea
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:06,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1cea
Route: LAN-1 Tx (INTRANET2):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cd0
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (LAN-1, INTRANET3, RtgTag: 3):
DstIP: 4.4.4.1, SrcIP: 192.168.3.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0015, seq: 0x1cdf
Route: WAN Tx (INTERNET3)

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cd0
```

```
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:07,430
IP-Router Rx (INTERNET3, RtgTag: 3):
DstIP: 192.168.3.100, SrcIP: 4.4.4.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0015, seq: 0x1cdf
Route: LAN-1 Tx (INTRANET3):

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (LAN-1, INTRANET2, RtgTag: 2):
DstIP: 3.3.3.1, SrcIP: 192.168.2.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0014, seq: 0x1ceb
Route: WAN Tx (INTERNET2)

[IP-Router] 2010/12/20 17:11:07,600
IP-Router Rx (INTERNET2, RtgTag: 2):
DstIP: 192.168.2.100, SrcIP: 3.3.3.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0014, seq: 0x1ceb
Route: LAN-1 Tx (INTRANET2):
```

Die Ausgabe von nur 2 Sekunden reicht schon aus, um eine recht große Menge an Daten zu erzeugen. Um die Ausgabe übersichtlicher zu gestalten, fügen Sie nach dem Trace-Kommando einen Filter an. Die Filter beginnen mit dem @-Zeichen und geben ein Suchkriterium an. In diesem Beispiel reduzieren Sie den Filter auf alle Ausgaben, in denen das Suchkriterium "Internet1" vorkommt, um nur die Pakete dieser Gegenstelle auszugeben.

Hinweis: Die Filter unterscheiden nicht zwischen Groß- und Kleinschreibung.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1

IP-Router ON @ INTERNET1

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfb
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:50,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
```

```
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfb
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (LAN-1, INTRANET1, RtgTag: 1):
DstIP: 11.11.11.1, SrcIP: 192.168.1.100, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo request, id: 0x0016, seq: 0x1cfc
Route: WAN Tx (INTERNET1)

[IP-Router] 2010/12/20 17:11:51,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1cfc
Route: LAN-1 Tx (INTRANET1):
```

Wieder beträgt der Zeitrahmen des Traces zwei Sekunden, die Menge an Daten wurde aber schon deutlich reduziert. Lediglich die Daten zur Gegenstelle "INTERNET1" werden angezeigt. Es können aber auch noch weitere Filterkriterien angegeben werden indem einfach ein Leerzeichen zwischen dem ersten und zweiten Kriterium gesetzt werden. Zusätzlich zum Leerzeichen können sowohl "+" als auch "-" als Operatoren verwendet werden. Hierbei gilt, bei einem "+" müssen beide Kriterien erfüllt sein, bei einem "-" darf das Kriterium nicht erfüllt sein und bei einem Leerzeichen muss eines der verknüpften Kriterien erfüllt sein. Die Möglichkeit Strings, die Operatoren enthalten auch als Filter zu nutzen wird durch Anführungszeichen umgesetzt.

Wenn Sie mehrere Suchbegriffe verwenden möchten, trennen Sie die einzelnen Begriffe durch die folgenden Operatoren:

- Leerzeichen: Ein Leerzeichen vor einem Suchbegriff stellt eine logische ODER-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie eine der so markierten Zeichenketten enthält.
- +: Ein Pluszeichen vor einem Suchbegriff stellt eine logische UND-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie alle der so markierten Zeichenketten enthält.
- -: Ein Minuszeichen vor einem Suchbegriff stellt eine logische NICHT-Verknüpfung dar. Die Trace-Ausgabe wird nur dann angezeigt, wenn sie keine der so markierten Zeichenketten enthält.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 -"echo request"
```

```
IP-Router ON @ INTERNET1 -"echo request"

[IP-Router] 2010/12/20 17:12:06,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0b
Route: LAN-1 Tx (INTRANET1):

[IP-Router] 2010/12/20 17:12:07,430
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0016, seq: 0x1d0c
Route: LAN-1 Tx (INTRANET1):
```

Jetzt zeigt der Trace nur noch die Einträge an, welche die Gegenstelle 'INTERNET1' enthalten, die aber **nicht** die Zeichenkette 'echo request' enthalten. So reduzieren Sie die Anzeige auf die Antworten eines Pings, die von der entsprechenden Gegenstelle stammen.

Sie können zeitgleich mehrere Traces verwenden und nach unterschiedlichen Kriterien filtern. Im folgenden Beispiel läuft neben dem IP-Router Trace auch ein Ethernet Trace, um sich das zum Ping zugehörige Paket auf dem Ethernet anzuschauen.

```
root@MyDevice:/
> trace # ip-router @ INTERNET1 +"echo reply"
IP-Router ON @ INTERNET1 +"echo reply"

root@MyDevice:/
> trace # eth @ ICMP +"echo reply"
Ethernet ON @ icmp +"echo reply"

[IP-Router] 2010/12/21 14:17:21,000
IP-Router Rx (INTERNET1, RtgTag: 1):
DstIP: 192.168.1.100, SrcIP: 11.11.11.1, Len: 84, DSCP/TOS: 0x00
Prot.: ICMP (1), echo reply, id: 0x0002, seq: 0x2654
Route: LAN-1 Tx (INTRANET1):

[Ethernet] 2010/12/21 14:17:21,000
Sent 98 byte Ethernet packet via LAN-1:
HW Switch Port : ETH-1
-->IEEE 802.3 Header
Dest : 00:a0:57:12:a9:21 (Hirschmann 12:a9:21)
Source : 00:a0:57:12:f7:81 (Hirschmann 12:f7:81)
Type : IPv4
```

```
-->IPv4 Header
Version : 4
Header Length : 20
Type of service : (0x00) Precedence 0
Total length : 84
ID : 18080
Fragment : Offset 0
TTL : 59
Protocol : ICMP
Checksum : 24817 (OK)
Src Address : 11.11.11.1
Dest Address : 192.168.1.100
-->ICMP Header
Msg : echo reply
Checksum : 18796 (OK)
Body : 00 00 00 02 00 00 26 54 ......
 7e c9 6d 8c 00 00 00 00 ~.m.....
 00 01 02 03 04 05 06 07 ........
 08 09 0a 0b 0c 0d 0e 0f ........
 10 11 12 13 14 15 16 17 ........
 18 19 1a 1b 1c 1d 1e 1f ........
 20 21 22 23 24 25 26 27 !"#$%
```

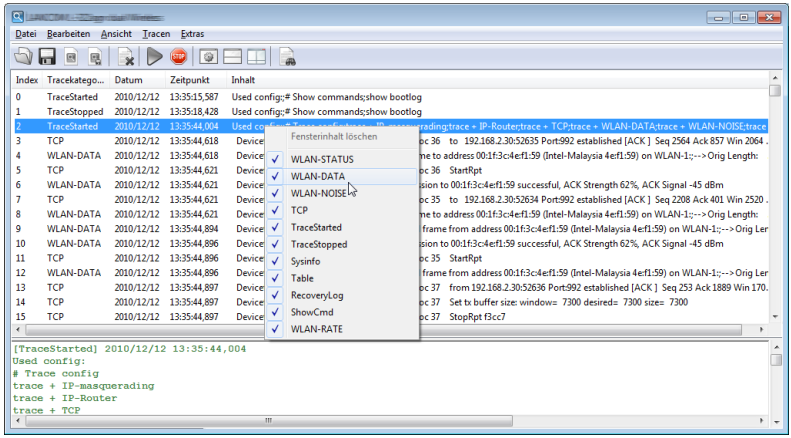
Anzeige der Trace-Ergebnisse

Um die Ausgabe der Trace-Daten zu starten, klicken Sie auf den Start-Button (▶) und wechseln so von der Konfigurationsansicht in die Ergebnisansicht von LANtracer. In dieser Ansicht werden die laufenden Trace-Ausgaben angezeigt:

- Der obere Bereich listet die Ergebnisse für die ausgeführten Trace-Kommandos chronologisch in jeweils einer Zeile auf.
- Der untere Bereich stellt die Ergebnisse für das im oberen Bereich ausgewählte Trace-Kommando ausführlich dar. Hier sind alle aktiven Trace-, Status- und Show-Einträge mit den jeweiligen Filtern und Parametern aufgelistet. Die Ausgabe erfolgt mehrzeilig, da die Ergebnisse für ein einzelnes Trace-Kommando sehr umfangreich sein können.

Mit einem rechten Mausklick auf ein Trace-Ereignis öffnen Sie das Kontextmenü, über das Sie die einzelnen Trace-Kategorien ein- oder ausblenden können, um die angezeigten Ergebnisse grob zu filtern.

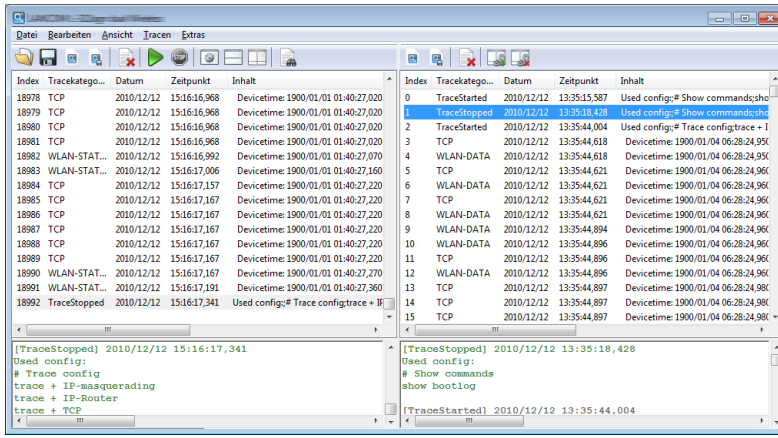
Hinweis: Die Trace-Daten werden erfasst, solange die Trace-Ausgabe aktiv ist. Um eine Überlastung des Arbeitsspeichers auf der Workstation mit LANconfig oder LANmonitor zu vermeiden, werden die Trace-Daten automatisch in eine Backup-Datei gespeichert. Die zeitlichen Intervalle und die maximale Größe einer Sicherungsdatei stellen Sie im LANtracer unter **Extras** > **Sonstige Einstellungen** > **Traceeinstellungen** ein.



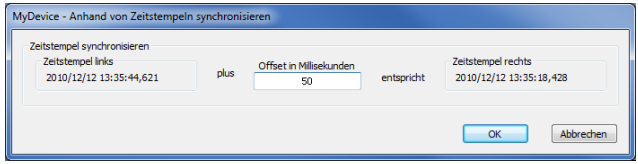
Trace-Daten vergleichen

Um die Ergebnisse eines Traces mit anderen (in einer Backup abgespeicherten) Tracedaten zu vergleichen, können Sie in der geteilten Trace-Ansicht zwei Traces nebeneinander darstellen.

1. Stoppen Sie dazu den aktuell laufenden Trace und wählen Sie im Menü **Ansicht** > **Trace-Erg. Doppelansicht**.
2. Laden Sie in den noch leeren Ansichtsbereich die Datei mit den aktuell oder zu einem früheren Zeitpunkt erfassten Trace-Daten.

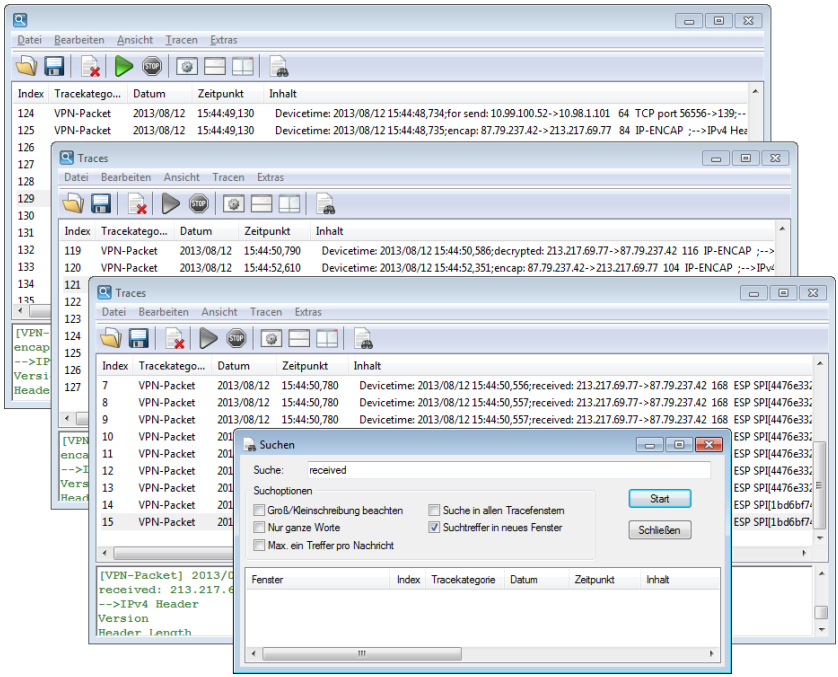


3. Starten Sie die Synchronisation der beiden Traces anhand des Zeitstempels mit der Schaltfläche . Geben Sie im folgenden Fenster einen geeigneten Wert für den Offset in Millisekunden ein und starten Sie die Synchronisation.



Mehrstufige Suche

Sie haben die Möglichkeit, durch intelligentes Verschachteln von Suchanfragen eine mehrstufige (kaskadierte) Suche innerhalb der Trace-Ergebnisse durchzuführen. Aktivieren Sie dazu *vor* dem Beginn der ersten Suche die Option **Suchtreffer in neues Fenster** und lassen Sie die Option für alle weiteren Suchanfragen aktiviert. Suchen Sie anschließend sukzessiv nach verschiedenen Schlüsselbegriffen im jeweils der zuletzt geöffneten Fester, um die Trefferliste immer weiter zu verfeinern.



Um eine Suchanfrage wieder zu verallgemeinern bzw. einen Suchschritt zurückzugehen, schließen Sie einfach die jeweils zuletzt geöffnete Ergebnisansicht und kehren so zur vorangehenden Ergebnisansicht zurück.

Mehr zu den Einstellungsmöglichkeiten im **Suchen**-Dialog finden Sie im Kapitel *Suchen* auf Seite 389.

Backup-Einstellungen für die Traces

Beim Starten eines Traces über LANconfig oder LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Mehr zu den entsprechenden Einstellungsmöglichkeiten finden Sie im Abschnitt *Traceeinstellungen* auf Seite 392.

Sichern und Wiederherstellen der Trace-Daten

Auch die eigentlichen Trace-Daten können Sie zur späteren Bearbeitung oder Weitergabe an einen anderen Benutzer über **Datei** > **Tracedaten/Support-Konfigurationsdatei speichern** auf einen Datenträger schreiben und über **Datei** > **Tracedaten laden** wieder öffnen.

Alternativ können Sie auch die Schaltflächen zum Laden und zum Speichern der Trace-Daten verwenden.

Sichern und Wiederherstellen der Trace-Konfiguration

Zur späteren Wiederverwendung oder Weitergabe an einen anderen Benutzer können Sie die komplette Konfiguration der Trace-Ausgabe über **Datei** > **Tracekonfiguration speichern** auf einen Datenträger schreiben und später mit **Datei** > **Tracekonfiguration laden** wieder öffnen.

Hinweis: Trace-Konfigurationen selbst sind geräteunspezifisch, lassen sich prinzipiell also in Kombination mit jedem Gerät verwenden. Nicht importierbare – weil auf dem Zielgerät nicht vorhandene Optionen, Status-Werte oder Show-Befehle – werden beim Ladevorgang übersprungen. LANtracer gibt Ihnen allerdings eine Warnmeldung aus, welche die vom Zielgerät nicht unterstützten Bestandteile einer Tracekonfiguration auflistet.

Konfigurationsdatei für den Support ausspielen

LANtracer bietet Ihnen die Möglichkeit, eine spezielle Konfigurationsdatei zu erstellen, um Sie zur Fehlerdiagnose oder weiteren Unterstützung an den Support weiterzugeben. Diese Datei beinhaltet die aktuelle Konfiguration sowie zusätzliche Informationen zum Gerät, welche den Support-Mitarbeitern die Fehlersuche ggf. erleichtern.

Falls Sie bestimmte Informationen nicht weitergeben möchten, bietet Ihnen LANtracer die Option, sicherheitsrelevante Informationen beim Speichern auszublenden. Mehr zu den entsprechenden Einstellungsmöglichkeiten finden Sie im Abschnitt *Support-Konfigurationsdatei* auf Seite 393.

3.4.3 Die Menüstruktur im LANtracer

Über die Menüleiste laden und speichern Sie Trace-Konfigurationen und -Daten, starten und stoppen Traces, und passen sowohl das Aussehen als auch die Funktionsweise von LANtracer an.

Datei

Unter diesem Menüpunkt speichern und laden Sie Trace-Konfigurationen/-Daten und beenden LANtracer.

Tracedaten laden

Über diesem Menüpunkt laden Sie die in einer *.lct-Datei abgespeicherten Trace-Daten in die Ergebnisansicht.

Tracedaten/Support-Konfigurationsdatei speichern

Über diesem Menüpunkt speichern Sie nach einem Trace die aufgezeichneten Trace-Daten in eine *.lct-Datei. Parallel dazu wird in das selbe Verzeichnis eine Support-Konfigurationsdatei abgelegt. Diese Datei ist mit der im Abschnitt *Support-Konfigurationsdatei speichern* auf Seite 389 beschriebenen Datei identisch.

Tracekonfiguration laden

Über diesem Menüpunkt laden Sie die in einer *.lcg-Datei abgespeicherte Trace-Konfiguration in die Konfigurationsansicht.

Hinweis: Trace-Konfigurationen selbst sind geräteunspezifisch, lassen sich prinzipiell also in Kombination mit jedem Gerät verwenden. Nicht importierbare – weil auf dem Zielgerät nicht vorhandene Optionen, Status-Werte oder Show-Befehle – werden beim Ladevorgang übersprungen. LANtracer gibt Ihnen allerdings eine Warnmeldung aus, welche die vom Zielgerät nicht unterstützten Bestandteile einer Tracekonfiguration auflistet.

Tracekonfiguration speichern

Über diesem Menüpunkt speichern Sie die in der Konfigurationsansicht getätigten Einstellungen in eine geräteunabhängige *.lcg-Datei.

Tracedaten importieren

Über diesem Menüpunkt importieren Sie die in einer *.lct-Datei abgespeicherten Trace-Daten in die Ergebnisansicht. Auf diese Weise haben Sie die Möglichkeit, Tracedaten grafisch aufzubereiten, die Sie über die Kommandozeile (z. B. mit Telnet oder PuTTy) erstellt haben.

Support-Konfigurationsdatei speichern

Über diesem Menüpunkt speichern Sie die in der Konfigurationsansicht getätigten Einstellungen in eine gerätespezifische *.spf-Datei.

Eine Support-Konfigurationsdatei beeinhaltet die aktuelle Konfiguration und zusätzliche Informationen über das Gerät. Da diese Datei für den technischen Support bestimmt ist und somit Ihre Hände verlässt, können Sie in den *Einstellungen für die Support-Konfigurationsdatei* bei Bedarf sensible Bereiche der Konfiguration ausblenden.

Schließen

Schließt und beendet LANtracer.

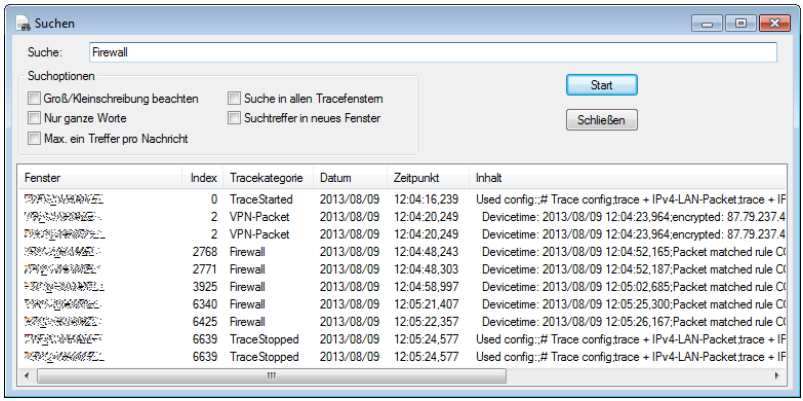
Bearbeiten

Unter diesem Menüpunkt durchsuchen oder löschen Sie die angezeigten Traces.

Suchen

Über diesem Menüpunkt öffnen Sie den Such-Dialog, der es Ihnen ermöglicht, die aufgezeigneten oder geladenen Trace-Daten gezielt nach bestimmten Begriffen zu durchsuchen. Sofern Sie keine weiteren Suchoptionen ausgewählt haben, führt die Funktion anhand des eingegeben Suchbegriffs eine Wildcard-Suche in allen existierenden Spalten durch; d. h. im Ergebnisfenster werden alle Treffer gelistet, die den eingegebenen Suchbegriff enthalten.

Um also gezielt nach Trace-Einträgen zu einer bestimmten Rubrik oder mit einem bestimmten Datum zu suchen, geben Sie z. B. `Firewall` oder `2013/08/09` ein und klicken **Start**.



Ferner haben Sie die Möglichkeit, folgende Suchoptionen zur Begrenzung der Suche zu aktivieren:

- **Groß/Kleinschreibung beachten**: Aktiviert die case-sensitive Suche.
- **Nur ganze Worte**: Aktiviert die Suche nach ganzen Wörtern bzw. deaktiviert die Suche nach Teil-Strings. In diesem Fall zeigt die Suche nach z. B. `VPN` nur Einträge an, in denen der Begriff als solcher vorkommt. Begriffe wie `VPN-Packet` fallen nicht ins Suchmuster.
- **Max. ein Treffer pro Nachricht**: Fasst mehrere Treffer zu einem Begriff innerhalb eines Trace-Eintrags zu einem einzigen Suchtreffer zusammen.
- **Suche in allen Tracefenstern**: Weitet die Suche auf alle geöffneten Ergebnisansichten aus. Andernfalls bleibt die Suche auf jene Ergebnisansicht beschränkt, auf die sie sich zuletzt bezog. Lesen Sie dazu auch das Kapitel *Mehrstufige Suche* auf Seite 385.
- **Suchtreffer in neues Fenster**: Zeigt die gefundenen Treffer in einer neuen Ergebnisansicht an.

Fensterinhalt löschen

Über diesem Menüpunkt löschen Sie die in der aktuellen Ergebnisansicht angezeigten Trace-Daten.

Ansicht

Unter diesem Menüpunkt passen Sie das Verhalten der LANtracer-Bedienoberfläche an.

Trace-Ergebnisse

Wechselt in den Modus zur Anzeige der Trace-Ergebnisse

Trace-Erg. Doppelansicht

Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht).

Konfiguration

Wechselt in den Modus zur Konfiguration der Trace-Ausgabe.

Tracen

Unter diesem Menüpunkt starten und stoppen Sie die Trace-Ausgabe.

Trace starten

Über diesen Menüpunkt starten Sie die Trace-Ausgabe.

Trace starten

Über diesen Menüpunkt stoppen Sie die Trace-Ausgabe.

Extras

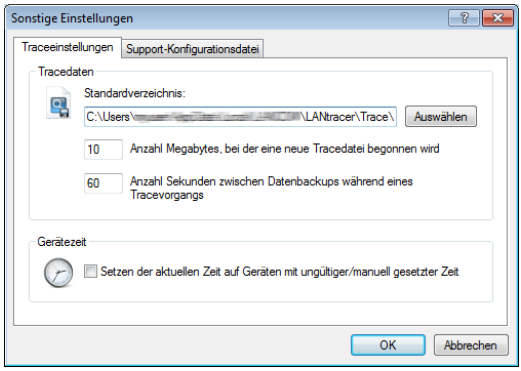
Unter diesem Menüpunkt finden Sie die programmbezogenen Einstellungsmöglichkeiten für LANtracer, z. B. zur automatischen Protokollierung der Trace-Ausgabe oder zur Definition der Support-Konfigurationsdatei.

Sonstige Einstellungen

Unter diesem Menüpunkt nehmen Sie die programmbezogenen Einstellungen für LANtracer vor.

Traceeinstellungen

Unter diesem Menüpunkt nehmen Sie die Einstellungen zu den Tracedaten und zur Gerätezeit vor.



Tracedaten

Beim Starten eines Traces über LANconfig oder LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Die Einstellungen für das Trace-Backup nehmen Sie im Abschnitt **Tracedaten** vor. Geben Sie

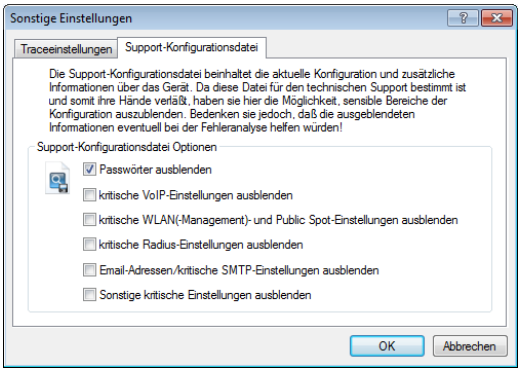
- … die maximale Größe einer Trace-Backup-Datei (in Megabyte) an. Wenn diese Größe mit einem aktiven Trace erreicht wird, wird automatisch eine weitere Trace-Backup-Datei angelegt. eine Ausgabegröße (in Megabyte) an, ab der LANtracer automatisch eine Trace-Datei erzeugt.
- … ein Intervall (in Sekunden) an, in dem LANtracer die Trace-Ausgabe in die erzeugte Datei speichert.
- … ein Verzeichnis an, in welchem LANtracer die Trace-Dateien standardmäßig ablegt.

Gerätezeit

Um eine zeitlich genaue Trace-Ausgabe zu erhalten, kann LANtracer außerdem vor einem Trace die Gerätezeit auf Gültigkeit prüfen und bei Geräten mit ungültiger/manuell gesetzter Zeit automatisch korrigieren, wenn Sie die betreffende Option aktivieren.

Support-Konfigurationsdatei

Unter diesem Menüpunkt legen Sie fest, welche Inhalte beim Speichern einer Support-Konfigurationsdatei automatisch entfernt werden. Die hierbei erstellte Support-Datei enthält alle Informationen im Klartext. Sie können die Datei daher in einem Editor öffnen und auf ggf. noch vorhandene sensible Einträge prüfen.



Folgende Inhalte und Einstellungen werden durch Anwählen der einzelnen Optionen ausgeblendet. Benutzen Sie in LANconfig den Quickfinder, um bequem zu den einzelnen Bezeichnern zu gelangen:

- Ausblenden von Passwörtern

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Kommunikation > **RADIUS**	**CLIP-Passwort**	2.2.22.7
VPN > **…** > **IKE-Schlüssel & Identitäten**	**Preshared-Key**	2.19.5.3.3
VPN > **…** > **IKE-Schlüssel & Identitäten**	–	2.19.5.3.4
Public Spot > **…** > **Benutzer-Liste**	**Passwort**	2.24.2.2
Public Spot > **…** > **Anmelde-Server**	**Auth.-Server Schlüssel**	2.24.3.4
Public Spot > **…** > **Anmelde-Server**	**Acc.-Server Schlüssel**	2.24.3.7

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
RADIUS-Server > **…** > **Benutzerkonten**	**Passwort**	2.25.10.7.2
Meldungen > **SMTP-Konto**	**Passwort**	2.27.6
WLAN-Controller > **…** > **Stationen**	**WPA-Passphrase**	2.37.20.4
Zertifikate > **…** > **Challenge-Tabelle**	**Challenge**	2.39.2.5.3.4

- Ausblenden von kritischen VoIP-Einstellungen

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
VoIP-Call-Manager > **…** > **SIP-Benutzer**	**Passwort**	2.33.3.1.1.3
VoIP-Call-Manager > **…** > **ISDN-Benutzer**	**Passwort**	2.33.3.2.2.6
VoIP-Call-Manager > **…** > **Analog-Benutzer**	**Passwort**	2.33.3.3.2.5
VoIP-Call-Manager > **…** > **SIP-Leitungen**	**Passwort**	2.33.4.1.1.6
VoIP-Call-Manager > **…** > **SIP-PBX-Leitungen**	**Passwort**	2.33.4.2.1.4

- Ausblenden von kritischen WLAN(-Management)- und Public Spot-Einstellungen

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Wireless LAN > **…** > **WLAN-Verschlüsselungs-Einstellungen**	**Schlüssel 1/Passphrase**	2.23.20.3.6
Wireless LAN > **…** > **WEP-Gruppen-Schlüssel**	**Schlüssel 2**	2.23.20.4.3
Wireless LAN > **…** > **WEP-Gruppen-Schlüssel**	**Schlüssel 3**	2.23.20.4.4
Wireless LAN > **…** > **WEP-Gruppen-Schlüssel**	**Schlüssel 4**	2.23.20.4.5
Public Spot > **…** > **Benutzer-Liste**	**Passwort**	2.24.2.2
Public Spot > **…** > **Anmelde-Server**	**Auth.-Server Schlüssel**	2.24.3.4
Public Spot > **…** > **Anmelde-Server**	**Acc.-Server Schlüssel**	2.24.3.7
Wireless-LAN > **…** > **RADIUS-Server**	**Schlüssel (Shared-Secret)**	2.30.3.4
WLAN-Controller > **Optionen**	**E-Mail Empfänger**	2.37.10.3
WLAN-Controller > **…** > **Stationen**	**WPA-Passphrase**	2.37.20.4

- Ausblenden von kritischen Radius-Einstellungen

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Kommunikation > **RADIUS**	**Schlüssel (Shared-Secret)**	2.2.22.4

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Kommunikation > **RADIUS**	**CLIP-Passwort**	2.2.22.7
RADIUS-Server > **…** > **Weiterleitungs-Server**	Auth.-Server: **Schlüssel (Secret)**	2.25.10.3.4
RADIUS-Server > **…** > **Weiterleitungs-Server**	Acc.-Server: **Schlüssel (Secret)**	2.25.10.3.10
RADIUS-Server > **…** > **Benutzerkonten**	**Passwort**	2.25.10.7.2
Wireless-LAN > **…** > **RADIUS-Server**	**Schlüssel (Shared-Secret)**	2.30.3.4

- Ausblenden von E-Mail-Adressen und kritischen SMTP-Einstellungen

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Firewall/QoS > **Allgemein**	**Administrator E-Mail**	2.8.10.10
Meldungen > **SMTP-Konto**	**Passwort**	2.27.6
WLAN-Controller > **Optionen**	**E-Mail Empfänger**	2.37.10.3

- Ausblenden von sonstigen kritischen Einstellungen

Dialog oder Tabelle	*Bezeichner*	*SNMP-ID*
Kommunikation > **…** > **PPP-Liste**	**Passwort**	2.2.5.3
Kommunikation > **…** > **Aktions-Tabelle**	**Gegenstelle**	2.2.25.3
Kommunikation > **…** > **Aktions-Tabelle**	**Aktion**	2.2.25.6
Management > **…** > **Weitere Administratoren**	**Passwort**	2.11.21.2

Hinweis: Bedenken Sie, dass das Ausblenden von sensiblen Bereichen der Konfiguration die Fehleranalyse durch den Support erschweren kann.

3.4.4 Die Symbolleiste im LANtracer

Das Trace-Modul bietet die folgenden Schaltflächen zur Bedienung:

Lädt eine Datei mit Trace-Daten

Speichert die aktuellen Trace-Daten, um diese an einen Anwender weiterzugeben.

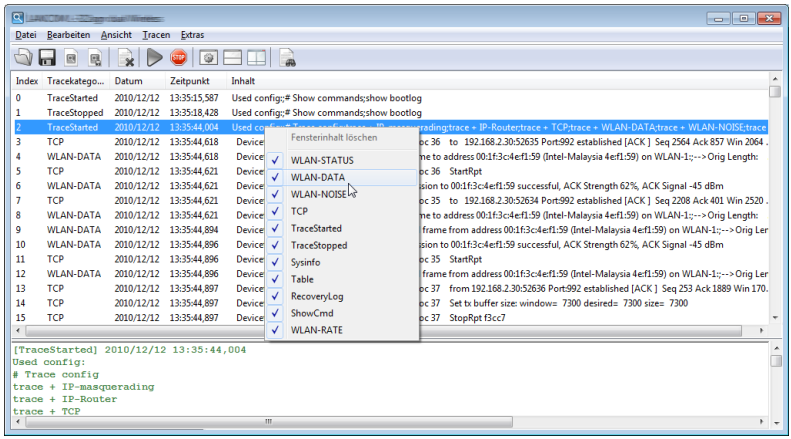
Löscht die aktuelle Anzeige der Trace-Ergebnisse

	Startet die Ausgabe der Trace-Ergebnisse gemäß der aktuellen Konfiguration und wechselt automatisch in den Anzeige-Modus der Trace-Ergebnisse. Solange die Ausgabe der Trace-Ergebnisse läuft, sind alle anderen Schaltflächen deaktiviert.
	Hält die Ausgabe der Trace-Ergebnisse an
	Wechselt in den Modus zur Konfiguration der Trace-Ausgabe
	Wechselt in den Modus zur Anzeige der Trace-Ergebnisse
	Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht)
	Startet die Synchronisation der beiden Traces in der geteilten Anzeige anhand des Zeitstempels
	Beendet die Synchronisation der beiden Traces in der geteilten Anzeige
	Öffnet das Fenster zur Suche in den Trace-Ergebnissen

Tabelle 20: Bedeutung der Symbole

3.4.5 Das Kontextmenü in LANtracer

Das Kontextmenü ist nur in der Ergebnisansicht verfügbar. Darin haben Sie die Möglichkeit, einzelne Trace-Kategorien auszublenden und so die angezeigten Ergebnisse grob zu filtern, oder den Fensterinhalt komplett zu leeren.



3.4.6 LANtracer Tastaturbefehle

Alt+L	Tracedaten laden
Alt+I	Tracedaten importieren
Alt+S	Tracedaten/Support-Konfigurationsdatei speichern
Strg+L	Tracekonfiguration laden
Strg+S	Tracekonfiguration speichern
Strg+F	Öffnet das Fenster zur Suche in den Trace-Ergebnissen
Alt+D	Löscht die aktuelle Anzeige der Trace-Ergebnisse
Strg+R	Wechselt in den Modus zur Anzeige der Trace-Ergebnisse
Strg+T	Wechselt in den Modus zur geteilten Anzeige der Trace-Ergebnisse in zwei parallelen Fenstern (Doppelansicht)
Strg+K	Wechselt in den Modus zur Konfiguration der Trace-Ausgabe
Leertaste, Enter	Makiert Auswahlkästchen in der Experten-Konfiguration
Alt+C	Schließt LANtracer

4 Diagnose

4.1 Trace-Ausgaben – Infos für Profis

Zur Kontrolle der internen Abläufe im Router während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Durch einen solchen Trace werden z. B. die einzelnen Schritte bei der Verhandlung des PPPs angezeigt. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Besonders positiv: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Router als auch bei der Gegenseite zu finden sein.

Hinweis: Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

4.1.1 So starten Sie einen Trace

Trace-Ausgaben starten Sie in einer Telnet-Sitzung. Stellen Sie zunächst eine Telnet-Verbindung zu Ihrem Gerät her. Der Trace-Aufruf erfolgt dann mit dieser Syntax:

▶ `trace [Schlüssel] [Parameter]`

Der Befehl Trace, der Schlüssel, die Parameter und die Kombinationsbefehle werden jeweils durch Leerzeichen voneinander getrennt.

4.1.2 Übersicht der Schlüssel

Dieser Schlüssel ...	*... ruft in Verbindung mit Trace die folgende Reaktion hervor:*
?	zeigt einen Hilfetext an
+	schaltet eine Trace-Ausgabe ein

Dieser Schlüssel ...	*... ruft in Verbindung mit Trace die folgende Reaktion hervor:*
-	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen den verschiedenen Trace-Ausgaben um (Toggle)
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

4.1.3 Übersicht der Parameter im trace-Befehl

Hinweis: Die jeweils für ein bestimmtes Modell verfügbaren Traces können über die Eingabe von `trace` ohne Argumente auf der Kommandozeile angezeigt werden.

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`Status`	Status-Meldungen der Verbindungen
`Fehler`	Fehler-Meldungen der Verbindungen
`PPP`	Verhandlung des PPP-Protokolls
`LCR`	Least-Cost-Router
`Script`	Script-Verhandlung
`Firewall`	Zeigt die Aktionen der Firewall
`RIP`	IP Routing Information Protocol
`ARP`	Address Resolution Protocol
`ICMP`	Internet Control Message Protocol
`IP-Masquerading`	Vorgänge im Masquerading-Modul
`DHCP`	Dynamic Host Configuration Protocol
`NetBIOS`	NetBIOS-Verwaltung
`DNS`	Domain Name Service Protocol
`Paket-Dump`	Anzeige der ersten 64 Bytes eines Pakets in hexadezimaler Darstellung
`ATM-Cell`	ATM-Paketebene
`ATM-Error`	ATM-Fehler
`SMTP-Client`	E-Mail-Verarbeitung des integrierten Mail-Clients
`Mail-Client`	E-Mail-Verarbeitung des integrierten Mail-Clients
`SNTP`	Simple Network Time Protokoll
`NTP`	Timeserver Trace

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`Connact`	Meldungen aus dem Aktivitätsprotokoll
`Cron`	Aktivitäten der Zeitautomatik (Cron-Tabelle)
`RADIUS`	RADIUS-Trace
`Serial`	Informationen über den Zustand der seriellen Schnittstelle
`USB`	Informationen über den Zustand der USB-Schnittstelle
`Load-Balancer`	Informationen zum Load Balancing
`VRRP`	Informationen über das Virtual Router Redundancy Protocol
`Ethernet`	Informationen über die Ethernet-Schnittstellen
`VLAN`	Informationen über virtuelle Netzwerke
`IGMP`	Informationen über das Internet Group Management Protocol
`WLAN`	Informationen über die Aktivitäten in den Funknetzwerken
`WLAN-ACL`	Status-Meldungen über MAC-Filterregeln. **Hinweis:** Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.
`IAPP`	Trace zum Inter Access Point Protocol, zeigt Informationen über das WLAN-Roaming.
`DFS`	Trace zur Dynamic Frequency Selection, der automatischen Kanalwahl im 5-GHz-WLAN-Band
`Bridge`	Informationen über die WLAN-Bridge
`EAP`	Trace zum EAP, dem bei WPA/802.11i und 802.1x verwendeten Protokoll zur Schlüsselaushandlung
`Spgtree`	Informationen zum Spanning Tree Protokoll
`LANAUTH`	LAN-Authentifizierung (z. B. Public Spot)
`SIP-Packet`	SIP-Informationen, die zwischen einem VoIP Router und einem SIP-Provider bzw. einer übergeordneten SIP-TK-Anlage ausgetauscht werden
`VPN-Status`	IPSec und IKE Verhandlungen
`VPN-Packet`	IPSec und IKE Pakete
`GRE`	Meldungen zu GRE-Tunneln
`XML-Interface-PbSpot`	Meldungen des Public-Spot-XML-Interfaces
`hnat`	Informationen zum Hardware-NAT
`IPv6-Config`	Informationen über die IPv6-Konfiguration

Dieser Parameter ...	*... ruft beim Trace die folgende Anzeige hervor:*
`IPv6-Firewall`	Ereignisse der IPv6-Firewall
`IPv6-Interfaces`	Informationen der IPv6-Schnittstellen
`IPv6-LAN-Packet`	Datenpakete über die IPv6-LAN-Verbindung
`IPv6-Router`	Informationen über das IPv6-Routing
`IPv6-WAN-Packet`	Datenpakete über die IPv6-WAN-Verbindung

Tabelle 21: Übersicht aller durchführbaren Traces

Erweiterte WLAN-Traces

Zur Unterstützung einer besseren Diagnose im WLAN-Bereich lassen sich unter **Setup** > **WLAN** einige Trace-Parameter gezielt anpassen.

Trace-Daten-Pakete

Die Ausgabe der Tracemeldungen lässt sich auf bestimmte Datenpakete eingrenzen.

Mögliche Werte:

normal

NULL

andere

Default:

normal

NULL

andere

Trace-MAC

Für den WLAN-Data-Trace lässt sich die Ausgabe von Tracemeldungen auf einen bestimmten Client mit der hier eingetragenen WLAN-MAC-Adresse einstellen.

Mögliche Werte:

max. 12 hexadezimale Zeichen aus

0123456789abcdef

Default:

000000000000

Besondere Werte:

000000000000: Deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

Hinweis: Dieser Filter wirkt für die Traces WLAN-DATA, WLAN-STRENGTH und WLAN-AGGREGATION, jedoch nicht für WLAN-STATUS.

Trace-Mgmt-Packete

Mit dieser Auswahl lässt sich einstellen, welche Klassen von Management-Frames im WLAN-DATA-Trace auftauchen sollen.

Mögliche Werte:

Assoziierung: (Re)Association Request/Response, Disassociate

Authentisierung: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Andere: alle restlichen Management-Frametypen

Default:

Assoziierung

Authentisierung

Probes

Action

Andere

Trace-Pakete

Ähnlich wie bei der Trace-MAC und der Trace-Stufe lassen sich die Ausgaben im WLAN-DATA-Traces anhand des Typs der empfangenen bzw. gesendeten Pakete einschränken, z. B. Management (Authenticate,

Association, Action, Probe-Request/Response), Control (z. B. Powersave-Poll), EAPOL (802.1x-Verhandlung, WPA-Key-Handshake).

Mögliche Werte:

Management

Control

Daten

EAPOL

Alle

Default:

Alle

Trace-Stufe

Für den WLAN-Data-Trace lässt sich die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränken. Der hier eingetragene Wert schränkt die Pakete im WLAN-DATA-Trace bis zur entsprechenden Stufe ein.

Mögliche Werte:

0 bis 255

Besondere Werte:

0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde

1: zusätzlich die physikalischen Parameter der Pakete (Datenrate, Signalstärke etc.)

2: zusätzlich der MAC-Header

3: zusätzlich der Layer3-Header (z. B. IP/IPX)

4: zusätzlich der Layer4-Header (TCP, UDP...)

5: zusätzlich die TCP/UDP-Payload

255: keine Beschränkung des Inhalts. Der Trace gibt die kompletten Pakete aus.

Default:

255

4.1.4 Kombinationsbefehle

Dieser Kombinations-Befehl ...	*... ruft beim Trace die folgende Anzeige hervor:*
Display	Status- und Error-Ausgaben
Protocol	PPP- und Script-Ausgaben
TCP-IP	IP-Routing-, IP-RIP-, ICMP- und ARP-Ausgaben
IPX-SPX	IPX-Routing-, RIP-, SAP-, IPX-Wd.-, SPX-Wd.-, und NetBIOS-Ausgaben

Die angehängten Parameter werden dabei von links nach rechts abgearbeitet. Dadurch kann ein zunächst aufgerufener Parameter anschließend auch wieder eingeschränkt werden.

4.1.5 Filter für Traces

Manche Traces wie der IP-Router-Trace oder die VPN-Traces erzeugen eine große Anzahl von Ausgaben. Damit wird die Ausgabe schnell unübersichtlich. Mit den Trace-Filtern haben Sie die Möglichkeit, nur die für Sie wichtigen Informationen aus den gesamten Traces herauszufiltern.

Zum Einschalten eines Trace-Filters wird das Trace-Kommando um den Parameter „@“ erweitert, der die folgende Filterbeschreibung einleitet. In der Filterbeschreibung gelten folgende Operatoren:

Operator	*Beschreibung*
(Leerzeichen)	ODER-Verknüpfung: Der Filter passt dann, wenn einer der Operanden in der Trace-Ausgabe vorkommt
+	UND-Verknüpfung: Der Filter passt dann, wenn der Operand in der Trace-Ausgabe vorkommt
-	Nicht-Verknüpfung: Der Filter passt dann, wenn der Operand nicht in der Trace-Ausgabe vorkommt
"	die Ausgabe muss exakt dem Suchmuster entsprechen

Als Operanden können beliebige Zeichenketten eingetragen werden, z. B. die Namen von Gegenstellen, Protokollen oder Ports. Der Trace-Filter verarbeitet diese Angaben dann nach den Regeln der verwendeten Operatoren so wie z. B. die Suchmaschinen im Internet.

4.1.6 Beispiele für die Traces

Dieser Schlüssel ...	*... ruft in Verbindung mit Trace die folgende Reaktion hervor:*
trace	zeigt alle Protokolle an, die während der Konfiguration Ausgaben erzeugen können, und den Zustand der jeweiligen Ausgaben (ON oder OFF)
trace + protocol display	schaltet die Ausgabe aller Verbindungsprotokolle und der Status- und Fehlermeldungen ein
trace - icmp	schaltet alle Trace-Ausgaben mit Ausnahme des ICMP-Protokolls ein
trace ppp	zeigt den Zustand des PPPs an
trace # ipx-rt display	schaltet die Trace-Ausgaben des IPX-Routers und der Display-Ausgaben um
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B -ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen, die nicht ICMP verwenden
trace + ip-router @ GEGENSTELLE-A GEGENSTELLE-B +ICMP	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die sich auf die Gegenstellen A oder B beziehen und die ICMP verwenden
trace + ip-router @+TCP +"port: 80"	schaltet die Ausgaben des IP-Routers an für alle Ausgaben, die TCP/IP und den Port 80 verwenden. “port: 80” steht in Anführungszeichen, um auch das Leerzeichen als Teil der Zeichenkette einzubeziehen.

4.1.7 Traces aufzeichnen

Um einen Trace komfortabel mit einem Windows-System aufzuzeichnen (z. B. als Unterstützung für den Support), empfehlen wir Ihnen folgende Vorgehensweise:

Öffnen Sie bitte HyperTerminal unter **Start** / **Programme** / **Zubehör** / **Kommunikation** / **Hyper Terminal**. Als Name geben Sie einen beliebigen Namen ein.

Wählen Sie im Fenster 'Verbinden mit' im Pulldown-Menü 'Verbindung herstellen über' den Eintrag 'TCP/IP'. Geben Sie anschließend als 'Hostadresse' die lokale/öffentliche IP-Adresse oder den FQDN des Gerätes ein. Nach der Bestätigung erscheint im HyperTerminal eine Login Aufforderung. Geben Sie nun das Konfigurationspasswort ein.

Zum Aufzeichnen des Traces klicken Sie in der Menüleiste auf **Übertragen** / **Text aufzeichnen**. Geben Sie den Pfad an, in dem die Textdatei gespeichert werden soll. Wechseln Sie nun wieder in das Dialogfenster und geben den entsprechenden Trace-Befehl ein.

Um den Trace wieder zu stoppen, klicken Sie im HyperTerminal in der oberen Menüleiste auf **Übertragen** / **Text aufzeichnen beenden**.

4.2 Tracen mit dem LANmonitor

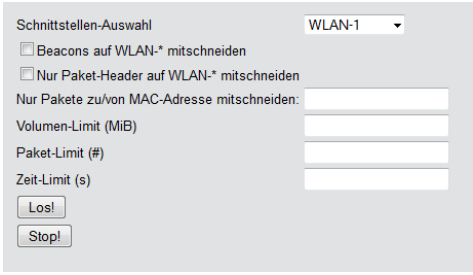
Informationen zu diesem Thema finden Sie im Kapitel *LANtracer - Tracen mit LANconfig und LANmonitor* auf Seite 372.

4.3 Paket-Capturing

Um Datenpakete zwecks Analyse von Störungen oder Problemen aufzuzeichnen, besteht die Möglichkeit, über ein Kommandozeilen-Tool den Befehl `lcoscap` auszuführen. Dieser Befehl aktiviert die Aufzeichnung der Pakete und schreibt die Ergebnisse in eine Datei, die Sie mit einem Tool wie z. B. “Wireshark” öffnen und analysieren können.

HiLCOS bietet Ihnen eine zusätzliche, deutlich komfortablere Methode zur Verfügung: Wählen Sie in WEBconfig unter **Setup** > **WLAN** > **Paket-Capture** > **WLAN-Capture-Format** ein Datenformat aus, in dem das Gerät Datenpakete ausgewählter Schnittstellen aufzeichnet und in eine Ergebnisdatei speichert.

Nach dem Festlegen der Parameter starten Sie unter **Extras** > **Paket-Capturing** mit einem Klick auf **Los!** das Paket-Capturing. Die erzeugte Datei können Sie anschließend z. B. mit “Wireshark” öffnen.



Diese Methode bietet Ihnen mehrere Vorteile:

- Sie sind auf keine spezielle Software angewiesen, da Sie Webconfig auf beliebigen Web-Browsern ausführen können.
- Die Eingabe von Kommandozeilenbefehlen entfällt. Stattdessen stehen Ihnen komfortable Menü-Elemente zur Verfügung.
- Wenn Sie Webconfig über HTTPS betreiben, ist die Vertraulichkeit und Sicherheit des aufgezeichneten Datenverkehrs gewährleistet.

Das Paket-Capturing funktioniert sowohl mit IPv4- als auch mit IPv6-Verbindungen.

4.4 Datenpakete aufzeichnen und analysieren

Sie haben mit HiLCOS zwei Möglichkeiten, Datenpakete zwecks Analyse von Störungen oder Problemen aufzuzeichnen.

Zum einen besteht die Möglichkeit, über ein Kommandozeilen-Tool den Befehl **lcoscap** auszuführen. Dieser Befehl aktiviert die Aufzeichnung der Pakete und schreibt die Ergebnisse in eine Datei, die Sie mit einem Tool wie “Wireshark” öffnen und analysieren können.

Zum anderen können Sie die deutlich komfortablere Methode über WEBconfig nutzen. Hierbei können Sie unterschiedliche Parameter definieren und auf diese Weise Datenpakete ausgewählter Schnittstellen aufzeichnen, um Sie für eine anschließende Analyse in einer Ergebnisdatei zu schreiben.

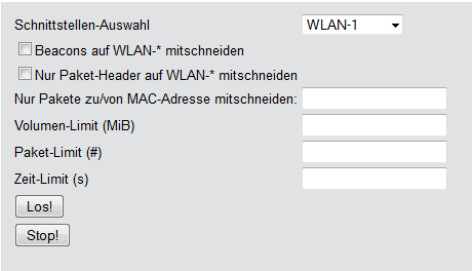
Diese Methode bietet Ihnen mehrere Vorteile:

- Sie sind auf keine spezielle Software angewiesen, da Sie Webconfig auf beliebigen Web-Browsern ausführen können.
- Die Eingabe von Kommandozeilenbefehlen entfällt. Stattdessen stehen Ihnen komfortable Menü-Elemente zur Verfügung.
- Wenn Sie WEBconfig über HTTPS betreiben, ist die Vertraulichkeit und Sicherheit des aufgezeichneten Datenverkehrs gewährleistet.

Der LCOScap-Client kann sich somit sowohl über IPv4 als auch über IPv6 mit dem Gerät verbinden.

4.4.1 Capture-Daten via Paket-Capturing erstellen

Der Dialog **Extras** > **Paket-Capturing** im WEBConfig bietet Ihnen eine einfache Möglichkeit, Datenpakete von unterschiedlichen Schnittstellen aufzuzeichnen und anschließend mit einer geeigneten Software (z. B. Wireshark) zu analysieren.



Für die Spezifizierung der Ausgabe-Datei stehen Ihnen folgende allgemeine Menüpunkte zur Verfügung:

Schnittstellen-Auswahl

Mit diesem Auswahlmenü bestimmen Sie die Schnittstelle, deren Datenpakete aufgezeichnet werden.

Beacons auf WLAN-* mitschneiden

Aktivieren Sie diese Option, um neben den Datenpakete auch die Beacon-Informationen aufzuzeichnen, wenn die ausgewählte Schnittstelle eine WLAN-Schnittstelle ist.

Nur Paket-Header auf WLAN-* mitschneiden

Aktivieren Sie diese Option, um die Aufzeichnung der Datenpakete auf den Paket-Header zu beschränken, wenn die ausgewählte Schnittstelle eine WLAN-Schnittstelle ist.

Nur Pakete zu/von MAC-Adresse mitschneiden

Wenn Sie nur Datenpakete einer bestimmten physikalischen Adresse innerhalb der ausgewählten Schnittstelle aufzeichnen wollen, können Sie diese hier festlegen.

Volumen-Limit (MiB)

Geben Sie hier das maximale Volumen der aufgezeichneten Pakete in Mebibytes an.

Paket-Limit (#)

Hier können Sie eine maximale Anzahl aufzuzeichnender Pakete festlegen.

Zeit-Limit (s)

Geben Sie hier eine maximale Zeit in Sekunden an, nach welcher die Aufzeichnung endet.

Nach dem Festlegen der Parameter und einem Klick auf **Los!** erzeugen Sie eine extern zu speichernde Datei, die Sie z. B. mit Wireshark öffnen können. Nach einiger Zeit – abhängig von der Verbindungsgeschwindigkeit – öffnet sich ein Dialog, der Sie zum Speichern der erzeugten Datei auffordert. Sie können die Datei mit der Endung *.cap jetzt lokal speichern. Standardmäßig erhält die Datei einen Namen, welcher die Bezeichnung und die zugehörige Schnittstelle des Gerätes enthält, dessen Datenpakete Sie aufgezeichnet haben (z. B. MyDevice-LAN-2.cap). Sie können den voreingestellten Dateinamen jedoch während des Speichervorgangs oder auch nachträglich ändern.

Eine laufende Aufzeichnung lässt sich jederzeit durch einen Klick auf **Stop!** beenden. Dies ist beispielsweise dann sinnvoll, um zunächst eingegebene Parameter zu korrigieren bzw. anzupassen.

Note: Wenn Sie Aufzeichnung ohne Angabe von Limits starten, zeichnet das Gerät die Pakete solange auf, bis Sie den Vorgang mit einem Klick auf **Stop** manuell beenden!

Flexibles WLAN Capture-Format

Ihnen stehen für das Paket-Capturing im WLAN verschiedene Formate zur Auswahl, unter denen das Gerät die aufgezeichnete Paketdaten speichern kann.

`Setup : WLAN : Paket-Capture`

4.4.2 Capture-Daten via LCOSCAP erstellen

Mit "LCOSCAP" haben Sie die Möglichkeit, den Datenverkehr aufzuzeichnen und in einem Wireshark kompatiblen Format abszupeichern. Sie bedienen "LCOSCAP" über die Kommandozeile, indem Sie die entsprechenden Parameter anhängen.

Sie steuern LCOSCAP über die folgenden Parameter:

-o

Zieldatei, welche den Mitschnitt enthält.

-p

Passwort des Gerätes, auf dem LCOSCAP den Datenverkehr aufnimmt.

-i

Interface des Gerätes, dessen Daten LCOSCAP erfasst.

Note: Wenn sie den Parameter -i auslassen, gibt LCOSCAP die Interface-Liste des Gerätes aus.

-b

Schalter, der die Beacons des Datenverkehrs mit einbezieht (ausschließlich für WLAN).

-h

Schalter, der die 802.11-Header mit einbezieht, allerdings ohne Payload (ausschließlich für WLAN).

-l

Gibt die maximale Größe der Capture-Datei an. Tritt der angegebene Wert ein, erzeugt LCOSCAP eine neue Datei. Die erstellten Dateien erhalten fortlaufende Nummern.

-n

Gibt die Anzahl der Dateien an, die LCOSCAP erzeugt. Wenn die maximale Anzahl der Dateien eintritt, überschreibt LCOSCAP die 1. Datei.

--h

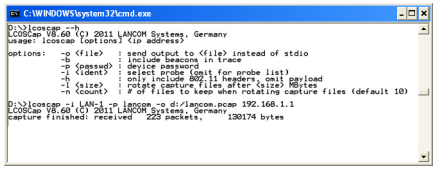
Mit `LCOSCAP --h` rufen Sie die LCOSCAP-Hilfe auf.

Um den Datenverkehr eines Gerätes aufzuzeichnen, geben Sie folgenden Befehl ein:

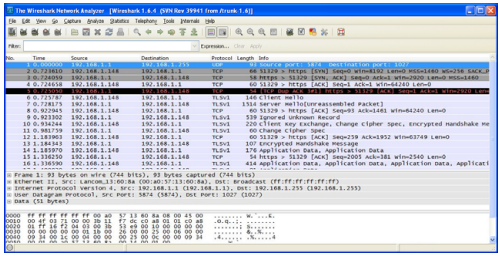
```
LCOSCAP -i LAN-1 -p lancom -o d:/lancom.pcap 192.168.1.1
```

- Das Gerät besitzt in diesem Beispiel die IP-Adresse "192.168.1.1".
- Das Passwort lautet "lancom".
- Sie zeichnen den Datenverkehr am Interface "LAN-1" auf.
- Speicherort und Name der Datei lauten `d:/lancom.pcap`

Mit der Tastenkombination **Strg + C** stoppen Sie die Aufzeichnung



Zur Analyse öffnen Sie die von LCOSCAP erzeugte Datei mit "Wireshark".



4.5 Das SYSLOG-Modul

Mit dem SYSLOG-Modul besteht die Möglichkeit, Zugriffe auf das Gerät protokollieren zu lassen. Diese Funktion ist insbesondere für Systemadministra-

toren interessant, da sie die Möglichkeit bietet, eine lückenlose Historie aller Aktivitäten aufzeichnen zu lassen.

Um die SYSLOG-Nachrichten empfangen zu können, benötigen Sie einen entsprechenden SYSLOG-Client bzw. -Dämon. Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Dämon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei.

Unter Linux wird in der Datei `/etc/syslog.conf` angegeben, welche Facilities (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Dämons, ob auf Netzwerkverbindungen explizit gehört wird.

Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Dämons erfüllt.

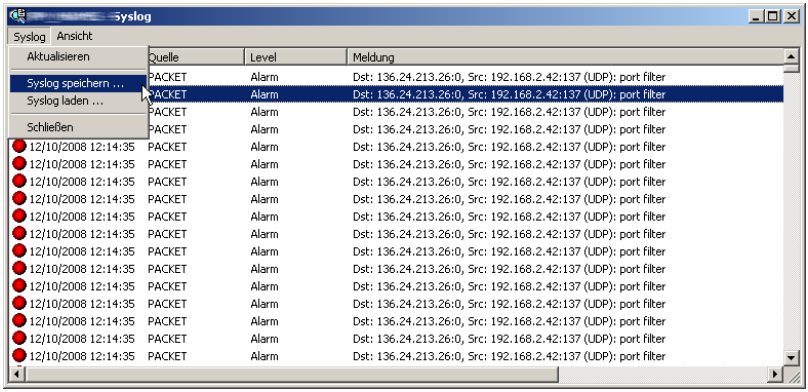
4.5.1 Einleitung

Über das SYSLOG-Protokoll werden die Aktivitäten eines Geräts protokolliert. Diese Funktion ist insbesondere für Systemadministratoren interessant, da sie eine lückenlose Historie aller Aktivitäten im Gerät aufzeichnet. Die über das SYSLOG-Protokoll erfassten Informationen können auf verschiedenen Wegen eingesehen werden:

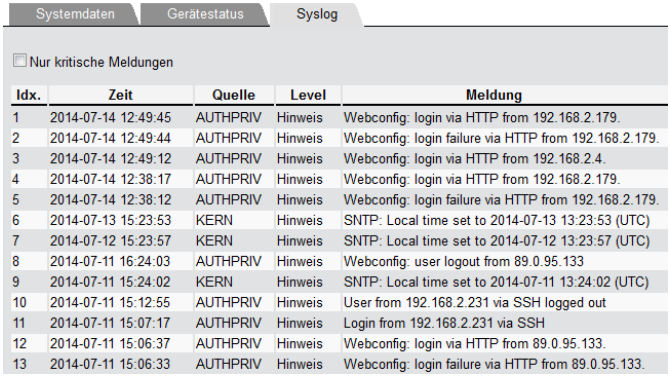
- Die SYSLOG-Meldungen können an eine zentrale “Sammelstelle” für SYSLOG geschickt werden, einen so genannten SYSLOG-Client oder SYSLOG-Daemon. Diese Variante bietet sich z. B. an, wenn die Nachrichten vieler Geräte gemeinsam protokolliert werden sollen.
  - Unter UNIX/Linux erfolgt die Protokollierung durch den in der Regel standardmäßig eingerichteten SYSLOG-Daemon. Dieser meldet sich entweder direkt über die Konsole oder schreibt das Protokoll in eine entsprechende SYSLOG-Datei. In der Datei `/etc/syslog.conf` wird angegeben, welche Facilities (zu diesem Begriff später mehr) in welche Logdatei geschrieben werden sollen. Überprüfen Sie in der Konfiguration des Daemons, ob auf Netzwerkverbindungen explizit gehört wird.
  - Windows stellt keine entsprechende Systemfunktion bereit. Sie benötigen spezielle Software, die die Funktion eines SYSLOG-Daemons erfüllt.
  - Syslog im Speicher der Geräte.

- Als Erweiterung zur Ausgabe der SYSLOG-Informationen über einen entsprechenden SYSLOG-Client werden je nach Speicherausstattung des Gerätes zwischen 100 und 2048 SYSLOG-Meldungen im RAM gespeichert. Diese internen SYSLOGs können an verschiedenen Stellen eingesehen werden:
  - In der Statistik der Geräte auf der Kommandozeite, z. B. per Telnet
  - In WEBconfig unter /Systeminformation/Syslog
  - In LANmonitor hier haben Sie zusätzlich die Möglichkeit, das Syslog aus dem Gerät zu exportieren und in einer Datei zu speichern. Klicken Sie dazu mit der rechten Maustaste auf den Namen des Gerätes und wählen Sie im Kontextmenü den Eintrag **Syslog anzeigen**. Die Ansicht ist jeweils ein aktueller Schnappschuss. Mit **Aktualisieren** wird eine Kopie des derzeitigen SYSLOGs vom Gerät exportiert und in der Ansicht dargestellt. **Syslog speichern...** speichert die aktuelle Anzeige in eine Datei. Gespeicherte SYSLOGs können mit **Syslog laden...** wieder zur Ansicht geöffnet werden.

Hinweis: Die SYSLOG-Meldungen werden nur dann in den geräteinternen Speicher geschrieben, wenn das Gerät als SYSLOG-Client mit der Loopback-Adresse 127.0.0.1 eingetragen wurde.



Alternativ können Sie die aktuellen SYSLOG-Meldungen auf der Startseite von WEBconfig auf der Registerkarte **Syslog** einsehen:



Systemdaten | Gerätestatus | Syslog

Nur kritische Meldungen

Idx.	Zeit	Quelle	Level	Meldung
1	2014-07-14 12:49:45	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
2	2014-07-14 12:49:44	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
3	2014-07-14 12:49:12	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.4.
4	2014-07-14 12:38:17	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 192.168.2.179.
5	2014-07-14 12:38:12	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 192.168.2.179.
6	2014-07-13 15:23:53	KERN	Hinweis	SNTP: Local time set to 2014-07-13 13:23:53 (UTC)
7	2014-07-12 15:23:57	KERN	Hinweis	SNTP: Local time set to 2014-07-12 13:23:57 (UTC)
8	2014-07-11 16:24:03	AUTHPRIV	Hinweis	Webconfig: user logout from 89.0.95.133
9	2014-07-11 15:24:02	KERN	Hinweis	SNTP: Local time set to 2014-07-11 13:24:02 (UTC)
10	2014-07-11 15:12:55	AUTHPRIV	Hinweis	User from 192.168.2.231 via SSH logged out
11	2014-07-11 15:07:17	AUTHPRIV	Hinweis	Login from 192.168.2.231 via SSH
12	2014-07-11 15:06:37	AUTHPRIV	Hinweis	Webconfig: login via HTTP from 89.0.95.133.
13	2014-07-11 15:06:33	AUTHPRIV	Hinweis	Webconfig: login failure via HTTP from 89.0.95.133.

4.5.2 Aufbau der SYSLOG-Nachrichten

Die SYSLOG-Nachrichten bestehen aus drei Teilen:

- Priorität
- Header
- Inhalt

Priorität

Die Priorität einer SYSLOG-Meldung enthält Informationen über die Severity (den Schweregrad bzw. die Bedeutung einer Meldung) und die Facility (Dienst oder die Komponente, welche die Nachricht ausgelöst hat).

Die im SYSLOG ursprünglich definierten acht Severity-Sufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen dem Alarmlevel, Bedeutung und SYSLOG-Severities.

Priorität	*Bedeutung*	*SYSLOG-Severity*
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING

Priorität	*Bedeutung*	*SYSLOG-Severity*
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller internen Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die standardmäßige Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an. Diese Zuordnung kann bei Bedarf verändert werden.

Quelle	*Bedeutung*	*Facility*
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Header

Der Header beinhalten den Namen oder die IP-Adresse des Gerätes, von dem die SYSLOG-Nachricht empfangen wurde. Für die Auswertung der Nachrichten ist auch die zeitliche Abfolge sehr wichtig. Um die zeitliche Konsistenz der Meldungen nicht durch unterschiedliche Gerätezeiten zu stören, wird die Zeitinformation erst beim SYSLOG-Client in die Nachrichten eingefügt.

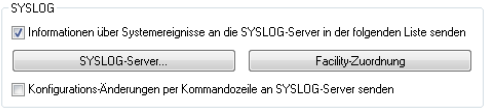
Hinweis: Für die Auswertung der SYSLOG-Meldungen im internen Speicher müssen die Geräte über eine gültige Zeitinformation verfügen.

Inhalt

Der eigentliche Inhalt der SYSLOG-Meldungen beschreibt das Ereignis, also z. B. einen Login-Vorgang, den Aufbau einer WAN-Verbindung oder die Aktivität der Firewall.

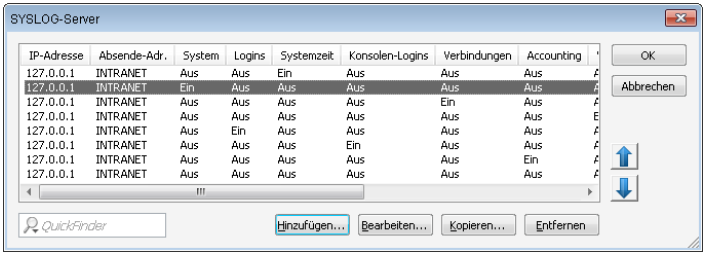
4.5.3 Konfiguration von SYSLOG über LANconfig

Die Parameter zur Konfiguration von SYSLOG finden Sie bei LANconfig im Konfigurationsbereich unter **Meldungen** > **Allgemein** im Abschnitt **SYSLOG**.

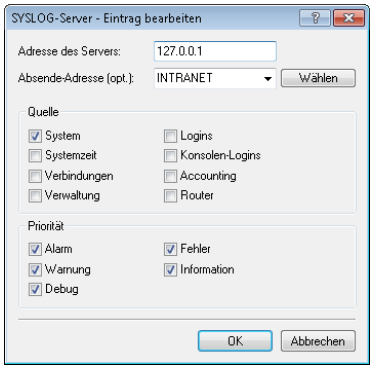


Klicken Sie auf **SYSLOG-Server**, um die vorhandenen SYSLOG-Einträge anzuzeigen.

Die Tabelle der SYSLOG-Einträge ist im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Diese Einstellungen entsprechen den Vorgaben aus der UNIX-Welt, aus der SYSLOG ursprünglich kommt. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Einträge unter LANconfig:



Klicken Sie auf **Hinzufügen** bzw. markieren Sie einen Eintrag und klicken Sie auf **Bearbeiten**.



Adresse des Servers

Legen Sie die IP-Adresse des SYSLOG-Servers fest. Die Angabe ist möglich in Form einer IPv4-/IPv6-Adresse oder eines Hostnamens.

Absende-Adresse (opt.)

Konfigurieren Sie optional eine Absende-Adresse, die der SYSLOG-Client statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Quelle

Die folgende Tabelle gibt eine Übersicht über die Bedeutung aller Nachrichtenquellen, die Sie im Gerät einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die Zuordnung zwischen den internen Quellen des Geräts und den SYSLOG-Facilities an.

Quelle	*Bedeutung*	*Facility*
System	Systemmeldungen (Bootvorgänge, Timersystem etc.)	KERNEL
Logins	Meldungen über Login und Logout eines Users während der PPP-Verhandlung sowie dabei auftretende Fehler	AUTH
Systemzeit	Meldungen über Änderungen der Systemzeit	CRON
Konsolen-Logins	Meldungen über Konsolen-Logins (Telnet, Outband, etc), Logouts und dabei auftretende Fehler	AUTHPRIV
Verbindungen	Meldungen über den Verbindungsauf- und -abbau sowie dabei auftretende Fehler (Display-Trace)	LOCAL0
Accounting	Accounting-Informationen nach dem Abbau einer Verbindung (User, Onlinezeit, Transfervolumen)	LOCAL1

Quelle	*Bedeutung*	*Facility*
Verwaltung	Meldungen über Konfigurationsänderungen, remote ausgeführte Kommandos etc.	LOCAL2
Router	Regelmäßige Statistiken über die am häufigsten genutzten Dienste (nach Portnummern aufgeschlüsselt) sowie Meldungen über gefilterte Pakete, Routing-Fehler etc.	LOCAL3

Priorität

Die im SYSLOG ursprünglich definierten acht Prioritätsstufen sind im Gerät auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen Alarmlevel, Bedeutung und SYSLOG-Prioritäten.

Priorität	*Bedeutung*	*SYSLOG-Priorität*
Alarm	Hierunter werden alle Meldungen zusammengefasst, die der erhöhten Aufmerksamkeit des Administrators bedürfen.	PANIC, ALERT, CRIT
Fehler	Auf diesem Level werden alle Fehlermeldungen übermittelt, die auch im Normalbetrieb auftreten können, ohne dass ein Eingriff des Administrators notwendig wird (z. B. Verbindungsfehler).	ERROR
Warning	Dieser Level übermittelt Fehlermeldungen, die den ordnungsgemäßen Betrieb des Geräts nicht beeinträchtigen.	WARNING
Information	Auf diesem Level werden alle Nachrichten übermittelt, die rein informellen Charakter haben (z. B. Accounting-Informationen).	NOTICE, INFORM
Debug	Übertragung aller Debug-Meldungen. Debug-Meldungen erzeugen ein erhebliches Datenvolumen und beeinträchtigen den ordnungsgemäßen Betrieb des Geräts. Sie sollten daher im Regelbetrieb ausgeschaltet sein und nur zur Fehlersuche verwendet werden.	DEBUG

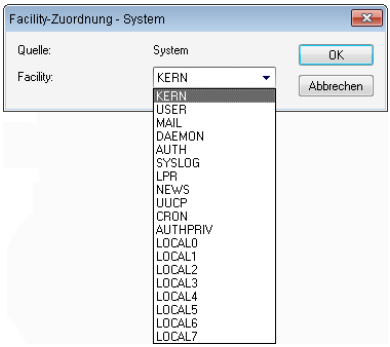
Wenn Sie alle Parameter definiert haben, bestätigen Sie die Eingaben mit **OK**. In der SYSLOG-Tabelle erscheint der SYSLOG-Client mit seinen Parametern.

Zuordnung von geräteinternen Quellen zu SYSLOG-Facilities

Das SYSLOG-Protokoll verwendet bestimmte Bezeichnungen für die Quellen der Nachrichten, die so genannten Facilities. Jede interne Quelle der Geräte, die eine SYSLOG-Nachricht erzeugen kann, muss daher einer SYSLOG-Facility zugeordnet sein.

Die standardmäßige Zuordnung ist bei Bedarf veränderbar. So lassen sich z. B. alle SYSLOG-Meldungen eines Geräts mit einer bestimmten Facility (Local7) versenden. Mit der entsprechenden Konfiguration des SYSLOG-Clients können Sie so alle Meldungen in einer gemeinsamen Log-Datei sammeln.

Über **Meldungen** > **Allgemein** lassen sich im Abschnitt **SYSLOG** unter **Facility-Zuordnung** die internen Quellen den entsprechenden SYSLOG-Facilities zuordnen.



Facilities

Über die Schaltfläche **Facility-Zuordnung** können alle Meldungen vom Gerät einer Facility zugeordnet und dadurch vom SYSLOG-Client ohne zusätzlichen Aufwand in eine spezielle Log-Datei geschrieben werden.

Alle Facilities werden auf 'local7' gesetzt. Unter Linux werden nun in der Datei `/etc/syslog.conf` durch den Eintrag

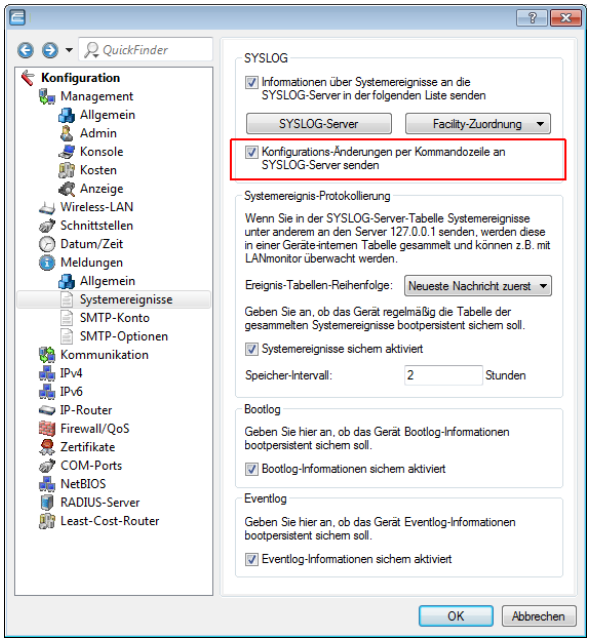
```
local7.* /var/log/hirschmann.log
```

alle Ausgaben des Geräts in die Datei `/var/log/hirschmann.log` geschrieben.

Konfigurationsänderungen per Kommandozeile an SYSLOG-Server senden

Die Einstellung für das Protokollieren der Konfigurationsänderungen über Kommandozeile finden Sie in LANconfig unter **Meldungen** > **Systemereignisse**.

Hinweis: Diese Protokollierung umfasst ausschließlich die an der Kommandozeile ausgeführten Befehle. Konfigurationsänderungen und Aktionen über LANconfig oder Webconfig sind davon nicht erfasst.

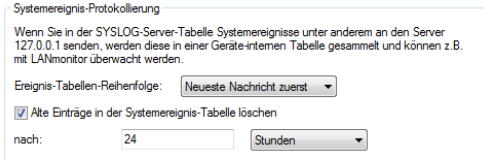


Speicherfrist von Systemereignissen festlegen

Unter **Meldungen** > **Systemereignisse** bestimmen Sie im Abschnitt **Systemereignisse-Protokollierung**, für wie lange das Gerät Systemereignisse speichert. Markieren Sie dazu die Option **Alte Einträge in der Systemereig-**

nis-Tabelle löschen und defnieren Sie eine Zeit (`0`–`9999`) in Stunden, Tagen oder Monaten.

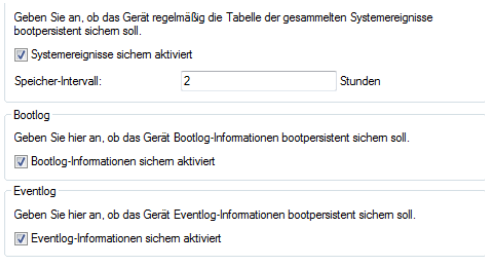
Hinweis: Ein Monat entspricht hierbei 30 Tagen.



SYSLOG, Eventlog und Bootlog bootpersistent

Die Einstellungen für das bootpersistente Speichern von SYSLOG-, Eventlog- und Bootlog-Nachrichten finden Sie (sofern für Ihr Gerät verfügbar) in LANconfig unter **Meldungen** > **Systemereignisse**. Aktivieren Sie dazu die folgenden Optionen:

- SYSLOG: **Systemereignisse sichern aktiviert**
- BOOTLOG: **Bootlog-Informationen sichern aktiviert**
- EVENTLOG: **Eventlog-Informationen sichern aktiviert**



SYSLOG: Erweiterung der Einträge des internen SYSLOG-Servers

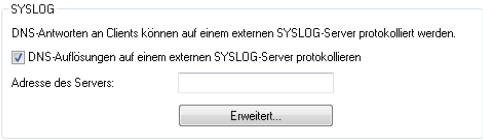
Ab HiLCOS-Version 8.90 kann der interne SYSLOG-Server bestimmter Geräte bis zu 23.000 Einträge speichern.

DNS-Anfragen und -Antworten an externen Syslog-Servern dokumentieren

Der DNS-Server in OpenBAT-Geräten löst DNS-Anfragen von Clients auf. Eine Übersicht darüber, welche Clients welche Namen angefragt und welche Antworten sie erhalten haben, steht im Syslog zur Verfügung.

Hinweis: Das Syslog des Routers/APs selbst kann nicht genutzt werden. Es ist daher erforderlich, einen externen Syslog-Server einzutragen.

Die Konfiguration des DNS-Loggings erfolgt im LANconfig unter **IPv4** > **DNS** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Markieren Sie diese Option, um das DNS-Logging zu aktivieren.

Hinweis: Diese Option ist unabhängig von der Einstellung im Syslog-Modul. Auch bei aktiviertem DNS-Logging und deaktiviertem Syslog-Modul (Einstellung unter **Meldungen** > **Allgemein** im Abschnitt **SYSLOG**) erfolgt das DNS-Logging.

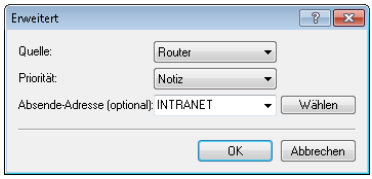
Die entsprechende SYSLOG-Meldung hat den folgenden Aufbau:

```
PACKET_INFO: DNS for <IP-Address>, TID {Hostname}: Ressource-Record
```

Adresse des Servers

Enthält die IP-Adresse oder den DNS-Namen des zu nutzenden SYSLOG-Servers.

Die Einstellungen hinter der Schaltfläche **Erweitert** beeinflussen die Inhalte der SYSLOG-Meldungen.



Quelle

Enthält die Log-Quelle, die in den SYSLOG-Meldungen erscheint.

Priorität

Enthält den Log-Level, der in den SYSLOG-Meldungen erscheint.

Absende-Adresse (optional)

Enthält die Absende-Adresse, die in den SYSLOG-Meldungen erscheint.

4.5.4 Bedeutung von SYSLOG-Meldungen

Dokumentation von Ereignissen auf den xDSL-Schnittstellen

Das Gerät erzeugt bei den folgenden xDSL-Schnittstellen-Ereignissen je einen SYSLOG-Eintrag:

Status	*Bedeutung*	*SYSLOG-Severity*
xDSL: Booting modem: ...	Das Modem startet neu.	NOTICE
xDSL: Set up line to <Leitungsmodus>/<Leitungstyp>	Das xDSL-Modul baut die Verbindung mit dem angegebenen Modus und Typ auf. Folgende Werte sind möglich: ▶ Leitungsmodus: Disabled, Auto sowie alle unter **Setup** > **Schnittstellen** > **ADSL-Interface bzw. VDSL-Interface** konfigurierbaren Modi. ▶ Leitungstyp: POTS, ISDN	INFORM
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:	Das Modem hat die Verbindung erfolgreich mit angegebenen Werten aufgebaut.	NOTICE

Status	*Bedeutung*	*SYSLOG-Severity*
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Dadurch können sich ggf. die Leitungswerte ändern. Nach einer Minute gibt das Modem die aktuellen Leitungswerte aus.	NOTICE
xDSL: Line data update.	Nach einer Synchronisation nehmen Modem und DSLAM eine Optimierung der xDSL-Verbindung vor. Nach einer Minute gibt das Modem diese Meldung aus, wenn sich die Leitungswerte nach der Synchronisation nicht geändert haben.	NOTICE
xDSL: Line disconnected due to	Die Verbindung ist aus dem angegebenem Grund abgebrochen. Folgende Werte sind möglich: ▶ modem reboot ▶ retrain ▶ silence ▶ high line error rate ▶ protocol setting ▶ line type setting ▶ automode line type switch ▶ modem timeout ▶ VC parameter change	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	Der Wert zwischen notwendigem und gemessenem Signal-Rausch-Abstand (SNR) hat sich um mehr als 1dB geändert.	INFORM

4.6 Übersicht der Parameter im ping-Befehl

Das ping-Kommando an der Eingabeaufforderung einer Telnet- oder Terminal-Verbindung sendet ein "ICMP Echo-Request"-Paket an die Zieladresse des zu überprüfenden Hosts. Wenn der Empfänger das Protokoll unterstützt und es nicht in der Firewall gefiltert wird, antwortet der angesprochene Host mit einem "ICMP Echo-Reply". Ist der Zielrechner nicht erreichbar, antwortet das letzte Gerät vor dem Host mit "Network unreachable" (Netzwerk nicht erreichbar) oder "Host unreachable" (Gegenstelle nicht erreichbar).

Die Syntax des Ping-Kommandos lautet wie folgt:

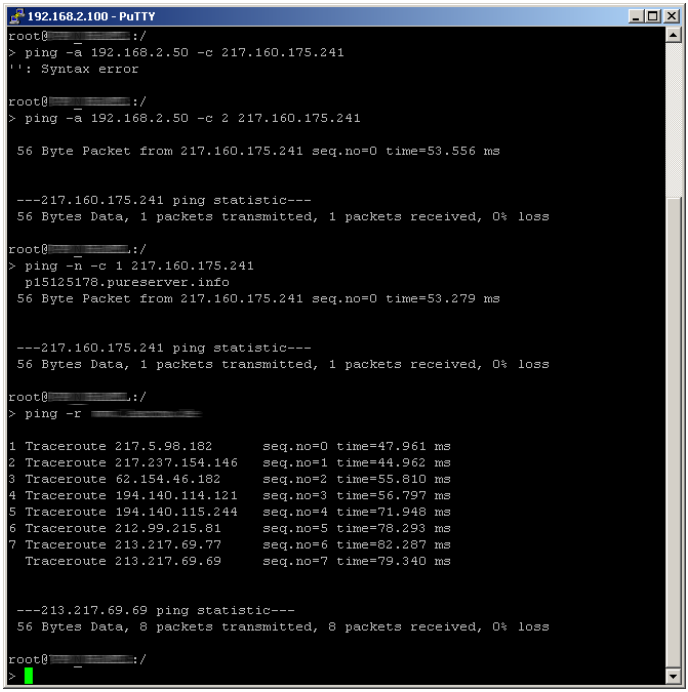
```
ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] Destination
```

Die Bedeutung der optionalen Parameter können Sie der folgenden Tabelle entnehmen:

Parameter	*Bedeutung*
`-a a.b.c.d`	Setzt die Absenderadresse des Pings (Standard: IP-Adresse des Gerätes)
`-a INT`	Setzt die Intranet-Adresse des Gerätes als Absenderadresse
`-a DMZ`	Setzt die DMZ-Adresse des Gerätes als Absenderadresse
`-a LBx`	Setzt eine der 16 Loopback-Adressen im Gerät als Absenderadresse. Gültige Werte für x sind die Hexadezimalen Werte 0-f
`-6 <IPv6-Address>%<Scope>`	Führt ein Ping-Kommando über das mit <Scope> bestimmte Interface auf die Link-Lokale-Adresse aus. Der Parameter-Bereich ist bei IPv6 von zentraler Bedeutung: Da ein IPv6-Gerät sich mit mehreren Schnittstellen (logisch oder physikalisch) pro Schnittstelle eine Link-Lokale-Adresse (fe80::/10) teilt, müssen Sie beim Ping auf eine Link-Lokale-Adresse immer den Bereich (Scope) angeben. Nur so kann das Ping-Kommando die Schnittstelle bestimmen, über die es das Paket senden soll. Den Namen der Schnittstelle trennen Sie durch ein Prozentzeichen (%) von der IPv6-Adresse. **Beispiele:** ▶ `ping -6 fe80::1%INTRANET` Ping auf die Link-Lokale-Adresse "fe80::1", die über die Schnittstelle bzw. das Netz "INTRANET" zu erreichen ist. ▶ `ping -6 2001:db8::1` Ping auf die globale IPv6-Adresse "2001:db8::1".
`-6 <Loopback-Interface>`	Setzt ein IPv6-Loopback-Interface als Absenderadresse.
`-f`	flood ping: Sendet große Anzahl von Ping-Signalen in kurzer Zeit. Kann z. B. zum Testen der Netzwerkbandbreite genutzt werden. ACHTUNG: flood ping kann leicht als DoS Angriff fehlinterpretiert werden.
`-n`	Liefert den Computernamen zu einer eingegebenen IP-Adresse zurück
`-o`	Schickt nach einer Antwort sofort eine weitere Anfrage
`-q`	Ping-Kommando liefert keine Ausgaben auf der Konsole

Parameter	*Bedeutung*
`-r`	Wechselt in Traceroute-Modus: Der Weg der Datenpakete zum Zielcomputer wird mit allen Zwischenstationen angezeigt
`-s n`	Setze Größe der Pakete auf n Byte (max. 65500)
`-i n`	Zeit zwischen den einzelnen Paketen in Sekunden
`-c n`	Sende n Ping-Signale
`Destination`	Adresse oder Hostnamen des Zielcomputers
`stop /<RETURN>`	Die Eingabe von “stop” oder das Drücken der RETURN-Taste beenden das Ping-Kommando

Tabelle 22: Übersicht aller optionalen Parameter im ping-Befehl



4.7 Monitor-Modus am Switch

Die über den Switch der Geräte übertragenen Daten werden zielgerichtet nur auf den Port aufgelegt, an dem der entsprechende Zielrechner angeschlossen ist. An den anderen Ports sind diese Verbindungen daher nicht sichtbar.

Um den Datenverkehr zwischen den einzelnen Ports mithören zu können, können die Ports in den Monitor-Modus geschaltet werden. In diesem Zustand werden auf diesen Ports alle Daten ausgegeben, die zwischen Stationen im LAN und WAN über den Switch des Gerätes ausgetauscht werden.

Bei der Konfiguration mit LANconfig öffnen Sie die Ethernet-Switch-Einstellungen im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'LAN' mit der Schaltfläche **Ethernet-Ports**.

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / Ethernet-Ports

4.8 Kabel-Test

Werden auf Ihren LAN- oder WAN-Verbindungen gar keine Daten übertragen, obwohl die Konfiguration der Geräte keine erkennbaren Fehler aufweist, liegt möglicherweise ein Defekt in der Verkabelung vor.

Mit dem Kabel-Test können Sie aus dem Gerät heraus die Verkabelung testen. Wechseln Sie dazu unter WEBconfig im **HiLCOS-Menübaum** in den Menüpunkt **Status** > **LAN** > **Kabel-Test**. Geben Sie dort die Bezeichnung des Interfaces ein, das Sie testen wollen (z. B. “DSL1” oder “LAN-1”). Achten Sie dabei auf die genaue Schreibweise der Interfaces. Mit einem Klick auf die Schaltfläche **Ausführen** starten Sie den Test für das eingetragene Interface.

Kabel-Test

Hier haben Sie die Möglichkeit, Parameter für das auszuführende Kommando einzugeben:
Parameter LAN-1

Wechseln Sie anschließend in den Menüpunkt **Status** > **LAN** > **Kabel-Test-Ergebnisse**. In der Liste sehen Sie die Ergebnisse, die der Kabel-Test für die einzelnen Interfaces ergeben hat.

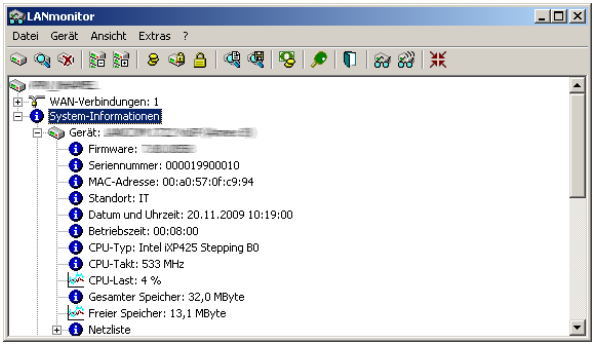
Kabel-Test-Ergebnisse

Ifc	MDI0-Status	MDI0-Distanz	MDI1-Status	MDI1-Distanz	MDI2-Status	MDI2-Distanz	MDI3-Status	MDI3-Distanz
LAN-1	OK		OK		Kurzschluss	4 m	Kurzschluss	4 m

4.9 Mittelwert der CPU-Lastanzeige

4.9.1 Einleitung

Die aktuelle CPU-Last der Geräte wird über verschiedene Ausgabemöglichkeiten angezeigt (LANmonitor, über WEBconfig oder CLI im Status-Bereich, bei einigen Modellen im Display).



4.9.2 Konfiguration

Je nach Bedarf können Sie einstellen, über welchen Zeitraum die angezeigte CPU-Last gemittelt werden soll.

WEBconfig: HiLCOS-Menübaum / Setup / Config

CPU-Last-Intervall

Hier können Sie die den Zeitraum zur Mittelung der CPU-Lastanzeige auswählen. Die Anzeige der CPU-Last im LANmonitor, im Status-Bereich, im Display (sofern vorhanden) sowie in evtl. genutzten SNMP-Tools basiert auf dem hier eingestellten Mittelungszeitraum. Im Status-Bereich unter WEBconfig oder CLI werden zusätzlich die CPU-Lastwerte für alle vier möglichen Mittelungszeiträume angezeigt.

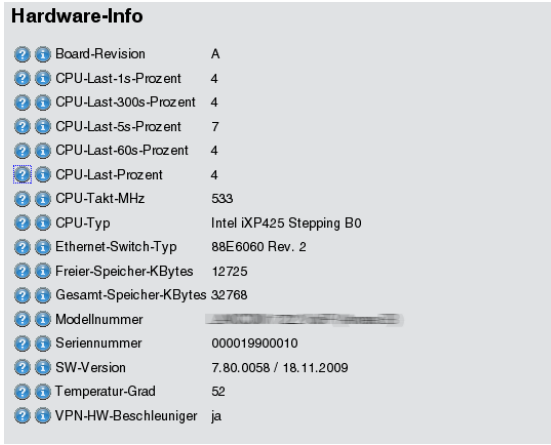
Mögliche Werte:

- 1, 5, 60 oder 300 Sekunden.

Default:

- 60 Sekunden.

Hinweis: Die defaultmäßige Mittelung über 60 Sekunden ist in der HOST-RESOURCES-MIB vorgeschrieben, die von gängigen SNMP-Tools zur Anzeige der CPU-Last in einem Tacho-Display verwendet wird. Bitte beachten Sie diese Vorgabe bei der Anpassung des CPU-Last-Intervalls.



4.10 Versand von Anhängen mit dem mailto-Kommando

Mit dem mailto-Kommando in den Einträgen der Aktionstabelle oder Cron-Tabelle können bei bestimmten Ereignissen automatisch E-Mails mit Informationen über den Zustand der Geräte verschickt werden.

Mit der Erweiterung um Anhänge in den E-Mails können vor dem Versand der Mail beliebige Konsolen-Befehle auf dem Gerät ausgeführt werden, deren Ergebnis dann als Anhang mit der Mail verschickt werden. So lassen sich auch Inhalte von Tabellen oder Menüs (z. B. umfangreiche Statusmeldungen) per Mail versenden.

- Aktion (Aktionstabelle) oder Befehl (Cron-Tabelle) (max. 250 Zeichen)

  Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung bzw. beim Erreichen der definierten Zeit ausgeführt werden soll. In jedem Eintrag darf nur eine Aktion ausgeführt werden.

  Mögliche Werte für die Aktionen (maximal 250 Zeichen):

  – mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus.

  Mögliche Variablen zur Erweiterung der Aktionen:

  – attach=`Konsolen-Befehl`

  Als Konsolen-Befehl können beliebige Befehle auf der Konsole genutzt werden, die zu einer sinnvollen Ausgabe von Informationen führen. Der Konsolen-Befehl wird in Backquotes (auch bekannt als Backticks) eingefasst. Dieses Zeichen wird mit Hilfe der Taste für den “Accent Grave” erzeugt.

  Die Ausgabe des Konsolenbefehls wird in eine Text-Datei geschrieben und an die Mail angehängt. Vor die Ausgaben wird in den angehängten Text automatisch das Kommando und ein Zeit/Datumsstempel eingesetzt.

  Default:

  – leer

  Beispiele:

Mit der folgenden Aktion können Sie den ADSL-Status per E-Mail versenden:

```
mailto:admin@mycompany.de?subject=ADSL-Status?attach=`dir /status/adsl`
```

Mit einer Aktion können auch durchaus mehrere Konsolenbefehle verschickt werden:

```
mailto:admin@mycompany.de?subject=Statusmeldungen?attach=`dir
/status/adsl`?attach=`dir /status/config`
```

Die angehängten Texte werden als 'cmd1.txt', 'cmd2.txt' usw. bezeichnet.

4.11 Erweiterung der Sysinfo

Um Änderungen der Konfiguration feststellen und den Zeitpunkt einer Änderung nachvollziehen zu können, enthält Sysinfo im Feld CONFIG_STATUS zusätzliche Einträge.

Die Geräte speichern den Wert CONFIG_STATUS bei jeder Änderung der Konfiguration (per Kommandozeile, per SNMP oder durch das Laden von Skripten oder kompletten Konfigurationen). Der Wert CONFIG_STATUS besteht aus den folgenden Komponenten:

- Hash-Wert der Gerätekonfiguration als eindeutiges Merkmal eines Konfigurationsstandes.
- Zeitstempel der letzten Konfigurationsänderung im Format HHMMSSddmmyyyy auf Basis der koordinierten Weltzeit UTC. Der Bezug auf UTC garantiert eindeutige Werte ohne Einfluss von Standort oder Sommerzeiteinstellung.
- Zähler für die Konfigurationsänderungen, fortlaufend.

Das Feld CONFIG_STATUS enthält neben einem Wert für Statusschalter der Konfiguration und und einem Wert für den Status zum Flashen der Konfiguration die zusätzlichen Komponenten in der Form <Hash>.<Datum>.<Zähler>.

Sie können die Änderungen an der Konfiguration sowohl in entsprechenden Dateien oder Skripten (z. B. mit LCMS) als auch auf den Geräten direkt vor-

nehmen (Kommandozeile oder WEBconfig). Der Weg der Konfigurationsänderung hat dabei teilweise Einfluss auf den Inhalt des CONFIG_STATUS.

Hash-Wert der Gerätekonfiguration

Nur HiLCOS – das Betriebssystem der Geräte – kann den Hash-Wert berechnen. Der Hash-Wert ist für jeden Konfigurationsstand unterschiedlich, ein veränderter Hash-Wert auf einem Gerät zeigt so eine geänderte Konfiguration an.

Hinweis: HiLCOS speichert den berechneten Hash-Wert während des Flash-Vorgangs in das Gerät.

Zeitstempel der letzten Konfigurationsänderung

Sowohl HiLCOS als auch LCMS können den Zeitstempel setzen, sofern sie über eine gültige Uhrzeit verfügen.

Hinweis: Sofern der gewählte Konfigurationsweg nicht über eine gültige Uhrzeit verfügt, setzt das Gerät den Zeitstempel auf den Wert '00:00:00 0000-00-00'.

Zähler für die Konfigurationsänderungen

Bei der Auslieferung der Geräte enthält der Zähler für die Konfigurationsänderungen den Wert '0'. Danach erhöht jede Konfigurationsänderung diesen Wert um 1. Der Zähler für die Konfigurationsänderungen erlaubt die Ermittlung der aktuellen Konfigurationsversion auch dann, wenn bei der Konfiguration keine gültige Uhrzeit verfügbar war und der Zeitstempel daher den Wert '00:00:00 0000-00-00' enthält.

Hinweis: Ein Konfigurationszähler mit dem Wert '0' nach einer Änderung der Konfiguration deutet auf einen Fehler beim Lesen oder Schreiben des Zählers im Flash hin.

Anzeige des CONFIG_STATUS

Geben Sie zur Anzeige des Wertes CONFIG_STATUS an der Kommandozeile des Gerätes den Befehl `sysinfo` ein.

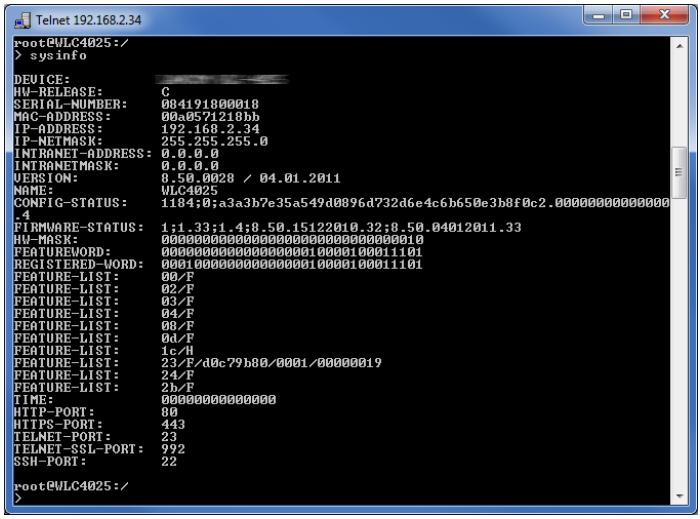


Abbildung 1: Anzeige der Systeminformationen auf der Kommandozeile

4.11.1 Ausgabe zusätzlicher Ports im SYSINFO an der Konsole

Ab HiLCOS-Version 9.00 überträgt der Befehl `sysinfo` auch die Nummern der folgenden Ports:

- HTTP
- HTTPS
- TELNET
- TELNET-SSL
- SSH
- SNMP
- TFTP

4.11.2 Ausgabe des Konfigurations-Datums

Ab HiLCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-date` das Datum und die Uhrzeit der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.20

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Hinweis: Die Werte werden im UTC-Format angezeigt.

4.11.3 Ausgabe des Konfigurations-Hashs

Ab HiLCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-hash` den Hash-Wert der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.21

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Hinweis: Bei dem angezeigten Wert handelt es sich um einen SHA1-Hash.

4.11.4 Ausgabe der Konfigurations-Version

Ab HiLCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-version` die Versionsnummer der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.22

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

5 Sicherheit

Sie mögen es sicher nicht, wenn Außenstehende die Daten auf Ihren Rechnern einsehen oder verändern können. Darüber hinaus sollten Sie die Konfigurationseinstellungen Ihrer Geräte vor unbefugten Änderungen schützen. Dieses Kapitel widmet sich daher einem sehr wichtigen Thema: der Sicherheit. Die Beschreibung der Sicherheitseinstellungen ist in folgende Abschnitte unterteilt:

- Schutz für die Konfiguration
  - Passwortschutz
  - Login-Sperre
  - Zugangskontrolle
- Absichern des ISDN-Einwahlzugangs

Zum Ende des Kapitels finden Sie die wichtigsten Sicherheitseinstellungen in Form einer Checkliste. Damit Sie ganz sicher sein können, dass Ihr Gerät bestens abgesichert ist.

Hinweis: Zur Sicherheit der Daten tragen auch noch einige weitere Funktionen des HiLCOS bei, die in separaten Kapiteln beschrieben sind:

- *Firewall*
- *Router-Funktionen*
- *VLAN*

5.1 Schutz für die Konfiguration

Mit der Konfiguration des Gerätes legen Sie eine Reihe von wichtigen Parametern für den Datenaustausch fest: Die Sicherheit des eigenen Netzes, die Kontrolle der Kosten und die Berechtigung einzelner Netzteilnehmer gehören z. B. dazu.

Die von Ihnen einmal eingestellten Parameter sollen natürlich nicht durch Unbefugte verändert werden. Daher bietet das Gerät die Möglichkeit, die Konfiguration mit verschiedenen Mitteln zu schützen.

5.1.1 Passwortschutz

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Passworts.

Hinweis: Solange Sie kein Passwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Beispielsweise könnten Ihre Internetzugangsdaten eingesehen werden, oder der Router so umkonfiguriert werden, dass alle Schutzmechanismen außer Kraft gesetzt werden.

Hinweis: Hinweis: Unter anderem wird ein nicht gesetztes Passwort auf allen Geräten durch eine blinkende Power-LED signalisiert, sofern ein Konfigurationszugriff über WAN oder WLAN möglich ist.

Tipps für den richtigen Umgang mit Passwörtern

Für den Umgang mit Passwörtern möchten wir Ihnen an dieser Stelle einige Tipps ans Herz legen:

- **Halten Sie ein Passwort so geheim wie möglich.**

  Notieren Sie niemals ein Passwort. Beliebt aber völlig ungeeignet sind beispielsweise: Notizbücher, Brieftaschen und Textdateien im Computer. Es klingt trivial, kann aber nicht häufig genug wiederholt werden: verraten Sie Ihr Passwort nicht weiter. Die sichersten Systeme kapitulieren vor der Geschwätzigkeit.

- **Passwörter nur sicher übertragen.**

  Ein gewähltes Passwort muss der Gegenseite mitgeteilt werden. Wählen Sie dazu ein möglichst sicheres Verfahren. Meiden Sie: Ungeschütztes E-Mail, Brief, Fax. Besser ist die persönliche Übermittlung unter vier Augen. Die höchste Sicherheit erreichen Sie, wenn Sie das Passwort auf beiden Seiten persönlich eingeben.

- **Wählen Sie ein sicheres Passwort.**

Verwenden Sie zufällige Buchstaben- und Ziffernfolgen. Passwörter aus dem allgemeinen Sprachgebrauch sind unsicher. Auch Sonderzeichen wie '&“?#-*+_:;,!°' erschweren es Angreifern, Ihr Passwort zu erraten und erhöhen so die Sicherheit des Passworts.

Hinweis: Groß- und Kleinschreibung werden beim Passwort für die Konfiguration unterschieden.

- **Verwenden Sie ein Passwort niemals doppelt.**

  Wenn Sie dasselbe Passwort für mehrere Zwecke verwenden, mindern Sie seine Sicherheitswirkung. Wenn eine Gegenseite unsicher wird, gefährden Sie mit einem Schlag auch alle anderen Verbindungen, für die Sie dieses Passwort verwenden.

- **Wechseln Sie das Passwort regelmäßig.**

  Passwörter sollen möglichst häufig gewechselt werden. Das ist mit Mühe verbunden, erhöht aber die Sicherheit des Passwortes beträchtlich.

- **Wechseln Sie das Passwort sofort bei Verdacht.**

  Wenn ein Mitarbeiter mit Zugriff auf ein Passwort Ihr Unternehmen verlässt, wird es höchste Zeit, dieses Passwort zu wechseln. Ein Passwort sollte auch immer dann gewechselt werden, wenn der geringste Verdacht einer undichten Stelle auftritt.

Wenn Sie diese einfachen Regeln einhalten, erreichen Sie ein hohes Maß an Sicherheit.

Eingabe des Passwortes

Das Feld zur Eingabe des Passworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. In einer SSH-Sitzung setzen oder ändern Sie das Passwort mit dem Befehl `passwd`.

LANconfig: Management / Admin / Passwort

WEBconfig: Extras / Passwort ändern

Den SNMP-Zugang schützen

Im gleichen Zug sollten Sie auch den SNMP-Lesezugriff mit Passwort schützen. Für SNMP wird das allgemeine Konfigurations-Passwort verwendet.

LANconfig: Management / Admin / SNMP-Lesezugriff nur mit Passwort zulassen

WEBconfig: HiLCOS-Menübaum / Setup / SNMP / Passw.Zwang-fuer-SNMP-Lesezugriff

5.1.2 Die Login-Sperre

Die Konfiguration im Gerät ist durch eine Login-Sperre gegen „Brute-Force-Angriffe“ geschützt. Bei einem Brute-Force-Angriff versucht ein unberechtigter Benutzer, ein Passwort zu knacken, und so Zugang zu einem Netzwerk, einem Rechner oder einem anderen Gerät zu erlangen. Dazu spielt z. B. ein Rechner automatisch alle möglichen Kombinationen aus Buchstaben und Zahlen durch, bis das richtige Passwort gefunden wurde.

Zum Schutz gegen solche Versuche kann die maximal zulässige Anzahl von fehlerhaften Login-Versuchen eingegeben werden. Wird diese Grenze erreicht, wird der Zugang für eine bestimmte Zeit gesperrt.

Die Login-Sperre greift immer nur für die genutzte Zugangsmöglichkeit. Die anderen Zugangsmöglichkeiten können weiterhin genutzt werden.

Hinweis: Technisch bedingt können SSH und Telnet immer nur gemeinsam gesperrt und entsperrt werden.

Zur Konfiguration der Login-Sperre stehen in den Konfigurationstools folgende Einträge zur Verfügung:

- Sperre aktivieren nach (`Anzahl Login-Fehler`)
- Dauer der Sperre (`Sperr-Minuten`)

LANconfig: Management / Admin

Hinweis: Wenn Sie im Feld **Sperre aktivieren nach** den Wert "0" eintragen, wird die Login-Sperre deaktiviert.

WEBconfig: HiLCOS-Menübaum / Setup / Config

Hinweis: Erfolgt die Anmeldung über RADIUS oder TACACS, bleibt die Login-Sperre ohne Funktionalität.

5.1.3 Einschränkung der Zugriffsrechte auf die Konfiguration

Der Zugriff auf die internen Funktionen kann wie folgt nach Interfaces getrennt konfiguriert werden:

- ISDN-Aministrationszugang
- LAN
- Wireless LAN (WLAN)
- WAN (z. B. ISDN, DSL oder ADSL)

Bei den Netzwerk-Konfigurationszugriffen können weitere Einschränkungen vorgenommen werden, z. B. dass nur die Konfiguration von bestimmten IP-Adressen vorgenommen werden darf. Ferner sind die folgenden internen Funktionen getrennt schaltbar:

- LANconfig (TFTP)
- WEBconfig (HTTP, HTTPS)
- SNMP
- Terminal/Telnet

Hinweis: Bei Geräten mit VPN-Unterstützung kann die Nutzung der einzelnen internen Funktionen über WAN-Interfaces auch nur auf VPN-Verbindungen beschränkt werden.

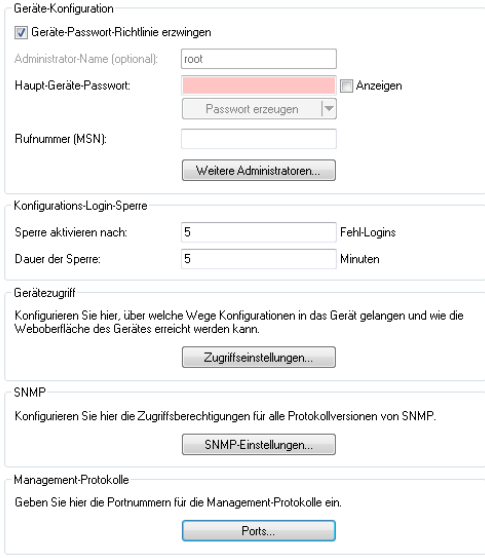
Den ISDN-Administrationszugang einschränken

Nur für Modelle mit ISDN-Schnittstelle.

Solange keine MSN für den Konfigurations-Zugriff eingetragen ist, nimmt ein **unkonfiguriertes** Gerät die Rufe auf alle MSNs an. Sobald die erste Änderung in der Konfiguration gespeichert ist, nimmt das Gerät nur noch die Anrufe auf der Konfigurations-MSN an!

Hinweis: Wenn bei der ersten Konfiguration keine Konfigurations-MSN eingetragen wird, ist die Fernkonfiguration damit ausgeschaltet und das Gerät gegen den Zugriff über die ISDN-Leitung geschützt.

1. Wechseln Sie im Konfigurationsbereich 'Management' auf die Registerkarte 'Admin'.



2. Geben Sie als Rufnummer im Bereich 'Geräte-Konfiguration' eine Rufnummer Ihres Anschlusses ein, die nicht für andere Zwecke verwendet wird.

   Geben Sie alternativ unter Telnet den folgenden Befehl ein:

   ```
   set /setup/config/Fernconfig 123456
   ```

   Hinweis: Der ISDN-Administrationszugang ist als einzige Konfigurationsmethode von den im folgenden beschriebenen Netzwerk-Zugangsbeschränkungen ausgenommen. D.h. alle auf der ADMIN-MSN eingehenden Verbindungen werden nicht über die Zugriffssteuerung von entfernten Netzen eingeschränkt.

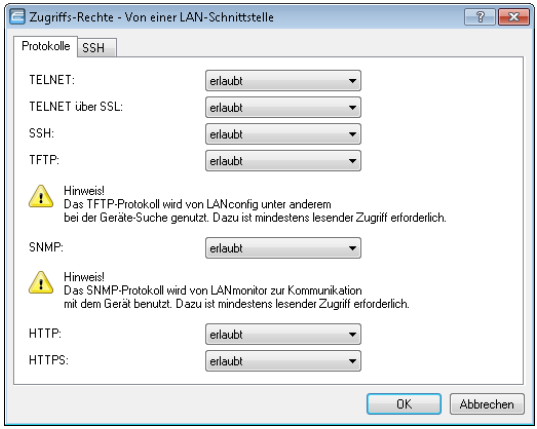
Hinweis: Wenn Sie die ISDN-Fernwartung ganz abschalten wollen, lassen Sie das Feld mit der ADMIN-MSN leer.

Den Netzwerk-Konfigurationszugriff einschränken

Den Zugriff auf die internen Funktionen steuern Sie - getrennt für Zugriffe aus dem lokalen Netz, aus entfernten Netzen oder aus Wireless LANs - für alle Konfigurationsdienste separat.

Dabei ist es möglich, den Konfigurationszugriff generell zu erlauben oder zu verbieten, als reinen Lesezugriff oder - falls Ihr Modell mit VPN ausgerüstet ist - auch nur über VPN zu erlauben.

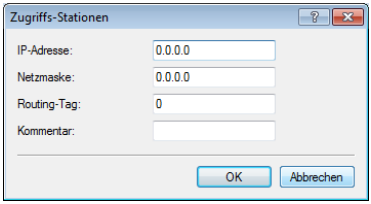
Die Konfigurationsdialoge im LANconfig mit den Zugriffsrechten vom lokalen Netz (LAN), über das WLAN oder über entfernte Netze (WAN) öffnen Sie unter **Management** > **Admin** mit der Schaltfläche **Zugriffseinstellungen**. Wählen Sie anschließend nach einem Klick auf **Zugriffs-Rechte** die entsprechende Schnittstelle aus:



Hinweis: Wenn Sie den Netzwerkzugriff auf den Router über das WAN ganz sperren wollen, stellen Sie den Konfigurationszugriff von einer WAN-Schnittstelle für alle Methoden auf “nicht erlaubt”.

Einschränkung des Netzwerk-Konfigurationszugriffs auf bestimmte IP-Adressen

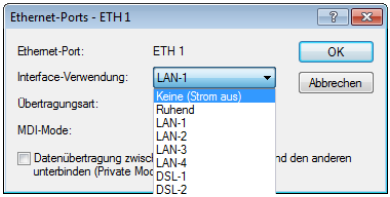
Sie haben die Möglichkeit, über eine spezielle Filterliste den Zugriff auf die internen Funktionen eines Gerätes auf bestimmte IP-Adressen einzuschränken. Sie erreichen den Konfigurationsdialog mit den Zugriffsadressen in LANconfig über die Tabelle **Zugriffs-Stationen** im Dialog **Management** > **Admin**.



Standardmäßig enthält diese Tabelle keine Einträge. Sie sind also dazu in der Lage, über eine beliebige IP-Adresse auf Ihr Gerät zuzugreifen. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske aktivieren Sie den Filter. Danach sind ausschließlich die in diesem Eintrag enthaltenen IP-Adressen dazu berechtigt, die internen Gerätefunktionen zu nutzen. Über zusätzliche Einträge lässt sich der Kreis der Berechtigten erweitern. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze umfassen.

5.1.4 Abschalten von Ethernet-Schnittstellen

Die Ethernet-Schnittstellen von öffentlich zugänglichen Geräten können ggf. von unbefugten Anwendern genutzt werden, um physikalischen Zugang zu einem Netzwerk zu erhalten. Um diesen Versuch zu verhindern, können die Ethernet-Schnittstellen der Geräte ausgeschaltet werden.



LANconfig: Schnittstellen / LAN / Interface-Einstellungen

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen

- **Interface-Verwendung**

  Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

  Mögliche Werte:

  - Keine (Strom aus): Die Schnittstelle ist deaktiviert.
  - Ruhend: Die Schnittstelle ist keiner Verwendung zugeordnet, sie ist allerdings physikalisch aktiv.
  - LAN-1 bis LAN-n: Die Schnittstelle ist einem logischen LAN zugeordnet.
  - DSL-1 bis DSL-n: Die Schnittstelle ist einem DSL-Interface zugeordnet.
  - Monitor: Der Port ist ein Monitor-Port, d.h. es wird alles, was auf den anderen Ports empfangen wird, auf diesem Port wieder ausgegeben. Damit kann an diesem Port z. B. ein Paket-Sniffer (wie Wireshark / Ethereal) angeschlossen werden.

  Default:

  - Abhängig von der jeweiligen Schnittstelle bzw. dem spezifischen Hardware-Modell.

5.2 Den ISDN-Einwahlzugang absichern

Bei einem Gerät mit ISDN-Anschluss kann sich prinzipiell jeder Teilnehmer in Ihr Gerät einwählen. Um unerwünschte Eindringlinge zu vermeiden, müssen Sie deshalb einen besonderen Augenmerk auf die Absicherung des ISDN-Zugangs legen.

Die Absicherungsfunktionen des ISDN-Zugangs können in zwei Gruppen eingeteilt werden:

- Identifikationskontrolle
  - Zugangsschutz mit Name und Passwort
  - Zugangsschutz über die Anruferkennung
- Rückruf an festgelegte Rufnummern

5.2.1 Die Identifikationskontrolle

Zur Identifikationskontrolle kann entweder der Name der Gegenstelle oder die sogenannte Anruferkennung herangezogen werden. Die Anruferkennung ist die Telefonnummer des Anrufers, die bei ISDN normalerweise mit dem Anruf an die Gegenstelle übermittelt wird.

Welcher “Identifier” zur Erkennung des Anrufers verwendet werden soll, wird in folgender Liste eingestellt:

LANconfig: Kommunikation / Ruf-Verwaltung

WEBconfig: HiLCOS-Menübaum / Setup / WAN / Schutz

Zur Auswahl stehen die folgenden Möglichkeiten:

- alle: Anrufe aller Gegenstellen werden angenommen.
- nach Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) in der Nummernliste eingetragen sind.
- nach geprüfter Nummer: Es werden nur Anrufe angenommen, deren Anschlusskennungen (CLIP) einerseits in der Nummernliste eingetragen sind, sowie andererseits von der Vermittlungsstelle für korrekt befunden wurden.

Die Identifizierung setzt natürlich voraus, dass die entsprechende Information vom Anrufer auch übermittelt wird.

Überprüfung des Benutzernamens und des Kennwortes

Bei einer PPP-Einwahl wird zunächst ein Benutzername (und in Verbindung mit PAP, CHAP oder MS-CHAP auch ein Passwort) beim Verbindungsaufbau an die Gegenstelle übertragen. Wählt sich ein Computer in das Gerät ein, so fragt die verwendete Verbindungssoftware, beispielsweise das DFÜ-Netzwerk unter Windows, den zu übermittelnden Benutzernamen und das Passwort in einem Eingabefenster ab.

Baut der Router selber eine Verbindung auf, etwa zu einem Internet Service Provider, so verwendet er seinerseits Benutzername und Passwort aus der PPP-Liste. Ist dort kein Benutzername eingetragen, wird stattdessen der Gerätename verwendet.

LANconfig: Kommunikation / Protokolle / PPP-Liste

WEBconfig: HiLCOS-Menübaum / Setup / WAN / PPP

Außerdem kann beim PPP-Protokoll auch der Anrufer von der Gegenstelle eine Authentifizierung verlangen. Er fordert dann die Gegenstelle zur Übermittlung eines Benutzer- bzw. Gerätenamens und eines Passwortes auf.

Hinweis: Die Sicherungsverfahren PAP, CHAP oder MS-CHAP wenden Sie natürlich nicht an, wenn Sie selber mit dem Gerät z. B. einen Internet Service Provider anwählen. Sie werden den ISP wahrscheinlich nicht dazu bewegen können, eine Anfrage an ihn nach einem Passwort zu beantworten …

Überprüfung der Nummer

Beim Anruf über eine ISDN-Leitung wird in den meisten Fällen über den D-Kanal die Rufnummer des Anrufers übertragen, schon bevor eine Verbindung zustande kommt (CLI – **C**alling **L**ine **I**dentifier).

Wenn die Rufnummer in der Nummernliste vorhanden ist, kann der Zugang zum eigenen Netz gewährt werden, oder der Anrufer wird bei eingeschalteter Rückrufoption zurückgerufen. Ist ein Schutz im Gerät über die Nummer vereinbart, werden alle Anrufe von Gegenstellen mit unbekannten Rufnummern abgelehnt.

Der Schutz mit Hilfe der Rufnummer kann mit allen B-Kanal-Protokollen (Layern) verwendet werden.

5.2.2 Der Rückruf

Eine besondere Variante des Zugriffsschutzes wird mit der Rückruffunktion erreicht: Dazu wird in der Gegenstellenliste für den gewünschten Anrufer die Option 'Rückruf' aktiviert und ggf. die Rufnummer angegeben.

LANconfig: Kommunikation / Gegenstellen / Gegenstellen (ISDN/seriell)

WEBconfig: HiLCOS-Menübaum / Setup / WAN / Einwahl-Gegenstellen

Mit den Einstellungen in Namen- und Nummernliste können Sie das Rückrufverhalten Ihres Routers steuern:

- Der Router kann den Rückruf ablehnen.
- Er kann eine voreingestellte Rufnummer zurückrufen.

- Er kann zunächst den Namen überprüfen und dann eine voreingestellte Rufnummer zurückrufen.
- Die Rufnummer für den Rückruf kann vom Anrufer frei eingegeben werden.

Und ganz nebenbei steuern Sie über die Einstellungen die Verteilung der Kosten für die Verbindung. Ist in der Gegenstellenliste ein Rückruf 'Nach Name' vereinbart, übernimmt der rückrufende Router alle Gebühreneinheiten bis auf die, die für die Namensübermittlung benötigt wird. Ebenfalls fallen Einheiten für den Anrufer an, wenn der Anrufer nicht über CLIP (**C**alling **L**ine **I**dentifier **P**rotocol) identifiziert wird. Ist dagegen eine Identifizierung über die Rufnummer des Anrufers erlaubt und möglich, kommt der Anrufer sogar ganz ohne Kosten weg (Rückruf über den D-Kanal).

Eine besonders effektive Methode des Rückrufs ist das Fast-Call-Back-Verfahren (zum Patent angemeldet). Dieses Verfahren beschleunigt die Rückrufprozedur beträchtlich. Das Verfahren funktioniert nur dann, wenn es von beiden Gegenstellen unterstützt wird. Alle aktuellen Router beherrschen das Fast-Call-Back-Verfahren.

5.3 Standort-Verifikation über ISDN oder GPS

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

5.3.1 GPS-Standort-Verifikation

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten aktiviert das Gerät bei Bedarf automatisch das GPS-Modul und prüft, ob es sich an der „richtigen“ Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet. Nach Abschluss der Standort-Verifikation wird das GPS-Modul automatisch wieder deaktiviert, sofern es nicht manuell eingeschaltet ist.

5.3.2 ISDN-Standort-Verifikation

Mit der ISDN-Standort-Verifikation können Sie den Missbrauch eines Routers verhindern: Der Router überprüft dann nach jedem Einschalten über einen ISDN-Anruf zu sich selbst, ob er am vorgesehenen Standort installiert ist. Erst wenn die Standort-Überprüfung erfolgreich ausgeführt wurde, wird das Router-Modul eingeschaltet.

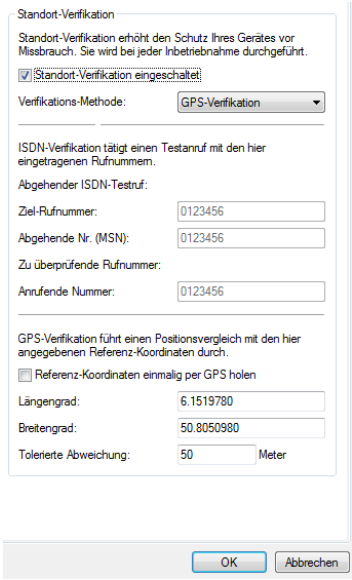
Voraussetzungen für eine erfolgreiche ISDN-Standort-Verifikation:

- Das Gerät muss aus dem öffentlichen ISDN-Netz erreichbar sein.
- Während der Überprüfung mit dem Selbstanruf benötigt das Gerät zwei freie B-Kanäle. Solange nur ein freier Kanal bereitsteht, z. B. weil an einem Mehrgeräteanschluss mit zwei B-Kanälen ein Kanal zum Telefonieren verwendet wird, kann sich das Gerät nicht selbst über ISDN anrufen.

5.3.3 Konfiguration der Standort-Verifikation

Die Parameter für die Standort-Verifikation finden Sie im LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Standort'.

Hinweis: Auf der Registerkarte 'GPS' können Sie das GPS-Modul unabhängig von der Standort-Verifikation einschalten, um z. B. die aktuellen Standortkoordination mit LANmonitor zu überwachen.



- Mit der Option 'Standort-Überprüfung einschalten' aktivieren Sie die Standort-Verifikation.
- Wählen Sie die Methode für die Standort-Überprüfung:
  - 'Selbst-Anruf' für die Überprüfung über ISDN mit einem Rückruf.
  - 'Rufweiterleitungs-Überprüfung' für die Überprüfung über ISDN durch Abfrage der Rufnummer aus der Vermittlungsstelle. Hierbei ist kein Rückruf erforderlich.
  - 'GPS-Verifikation' für die Überprüfung über die Geo-Koordinaten.

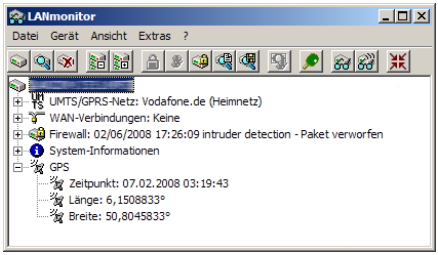
  Hinweis: Für die Standort-Überprüfung über GPS muss eine entsprechende GPS-Antenne an den AUX-Anschluss des Gerätes angeschlossen werden. Zusätzlich muss eine SIM-Karte für den Mobilfunkbetrieb eingelegt werden und das Gerät muss in ein Mobilfunknetz eingebucht sein.

- Tragen Sie für die Standort-Überprüfung über 'Selbst-Anruf' oder 'Rufweiterleitungs-Überprüfung' als 'Ziel-Rufnummer' ein, auf welche Telefonnummer geprüft werden soll.
- Tragen Sie für die Standort-Überprüfung über GPS die Parameter für die GPS-Prüfung ein:

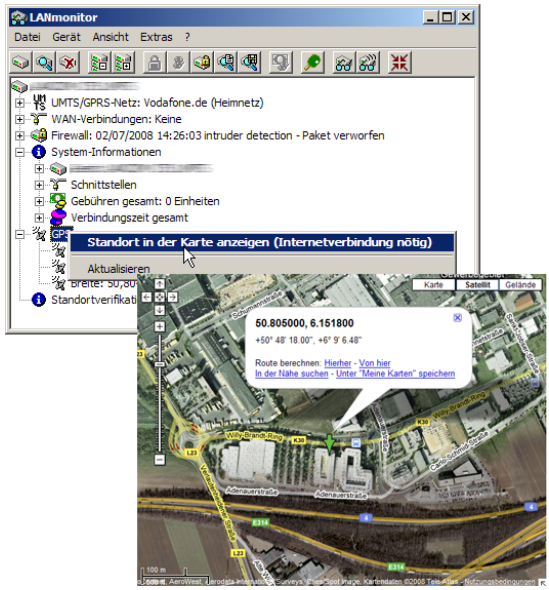
- Längen- und Breitengrad
- Abweichung von der erlaubten Position in Metern

Hinweis: Die Geo-Koordinaten für den aktuellen Standort kann das Gerät selbst ermitteln, indem Sie den Schalter 'Referenz-Koordinaten per GPS holen' aktivieren. Nach dem Rückschreiben der Konfiguration in das Gerät werden automatisch die aktuellen Längen- und Breitengrade eingetragen, wenn die Standortverifikation aktiv ist und gültige GPS-Daten vorliegen. Anschließend wird diese Option selbsttätig wieder deaktiviert.

Alternativ können Sie die Geo-Koordinaten für beliebige Standorte über Tools wie z. B. Google Maps ermitteln.



Hinweis: Wenn im LANmonitor die aktuellen Geo-Koordinaten angezeigt werden, können Sie mit einem rechten Mausklick auf den Eintrag 'GPS' den aktuellen Standort in der Satelliten-Ansicht von Google Maps aufrufen.



LANconfig: Kommunikation / Gegenstellen / Gegenstellen (ISDN/seriell)

WEBconfig: HiLCOS-Menübaum / Setup / Config / Standortverifikation

Experten-Konfiguration
Setup
Config

Standortverifikation

In-Betrieb	nein
Methode	GPS
ISDN-Ifc	S0-1
Zielrufnummer	
Abgehende-Rufnummer	
Erwartete-abgehende-Rufnummer	
Abweichung[m]	50
Laenge[Grad]	0
Breite[Grad]	0
Hole-GPS-Position	nein

Statusabfrage der Standort-Verifikation

Der Status der Standortverifikation kann über den LANmonitor eingesehen werden:

Mit WEBconfig (**Expertenkonfiguration** / **Status** / **Config** / **Standortverifikation**) oder Telnet (`Status/Config/Standortverifikation`) können Sie den Status der Standort-Verifikation einsehen:

Experten-Konfiguration
Status
Config

Standortverifikation

Zustand	Erfolgreich
Abgehender-Ruf-zu	
Erwarte-Ruf-von	
Zuletzt-gesehener-Ruf-von	
Ruf-wurde-angenommen	nein
Ankommender-Ruf	nein
Letzter-Fehler	
Methode	GPS
Position-gueltig	ja
Soll-Laengengrad[Grad]	6.1518583
Ist-Laengengrad[Grad]	6.1518555
Soll-Breitengrad[Grad]	50.8049638
Ist-Breitengrad[Grad]	50.8049638
Abweichung-Laengengrad[m]	1
Abweichung-Breitengrad[m]	0

Erst wenn die Standort-Verifikation im Zustand 'Erfolgreich' ist, kann der Router Daten über die WAN-Interfaces übertragen.

- Eine Standort-Verifikation über ISDN ist dann erfolgreich, wenn die Nummer 'Erwarte-Ruf-von' mit der Nummer der 'Zuletzt-gesehener-Ruf-von' übereinstimmt. Der Anruf wird dabei nicht vom Router angenommen. Der Status zeigt außerdem an, ob der Router überhaupt einen Ruf erkannt hat.

- Eine Standort-Verifikation über GPS ist dann erfolgreich, wenn die GPS-Position gültig ist und innerhalb der zulässigen Abweichung mit der Soll-Position übereinstimmt.

5.4 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Profis alle wichtigen Sicherheitseinstellungen im Überblick. Die meisten Punkte dieser Checkliste sind in einfachen Konfigurationen unbedenklich. In solchen Fällen reichen die Sicherheitseinstellungen aus, die während der Grundkonfiguration oder mit dem Sicherheits-Assistenten gesetzt werden.

Hinweis: Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

Haben Sie das Funknetzwerk durch Verschlüsselung und Zugangskontrolllisten abgesichert?

Mit Hilfe von 802.11i, WPA oder WEP verschlüsseln Sie die Daten im Funknetzwerk mit verschiedenen Verschlüsselungsmethoden wie AES, TKIP oder WEP. Hirschmann empfiehlt die stärkste mögliche Verschlüsselung mit 802.11i und AES. Wenn der eingesetzte WLAN-Client Adapter diese nicht unterstützt, nutzen Sie TKIP oder zumindest WEP. Stellen Sie sicher, dass in Ihrem Gerät bei aktivierter Verschlüsselungs-Funktion mindestens eine Passphrase oder ein WEP-Schlüssel eingetragen und zur Verwendung ausgewählt ist.

Hinweis: Hirschmann rät aus Sicherheitsgründen von der Verwendung von WEP ab! Setzen Sie WEP nur in begründeten Ausnahmefällen ein und ergänzen Sie die WEP-Verschlüsselung nach Möglichkeit mit anderen Schutzmechanismen!

Zur Kontrolle der Einstellungen wählen Sie in LANconfig unter **Wireless LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** die Verschlüsselungseinstellungen für die logischen WLAN-Schnittstellen aus.

Mit der Access Control List (ACL) gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-Netzwerkkarten. Zur Kontrolle der Access Control List wählen Sie in LANconfig im Konfigurationsbereich 'WLAN-Sicherheit' die Registerkarte 'Stationen'.

Mit der Access Control List (ACL) gewähren oder untersagen Sie einzelnen Funk-LAN-Clients den Zugriff auf Ihr Funk-LAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der Funk-Netzwerkkarten. Zur Konfiguration der Access Control List öffnen Sie in LANconfig die **Stationsregeln** unter **Wireless-LAN** > **Stationen**.

Mit der LANCOM Enhanced Passphrase Security (LEPS) ordnen Sie jeder MAC-Adresse in einer zusätzlichen Spalte der ACL eine individuelle Passphrase zu – eine beliebige Folge aus 4 bis 64 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am Access Point und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

Haben Sie ein Kennwort für die Konfiguration vergeben?

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Es ist insbesondere dann unerlässlich, ein Kennwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig unter **Management** > **Admin**. Es ist insbesondere dann unerlässlich, ein Kennwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

Haben Sie die Fernkonfiguration zugelassen?

Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der

Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - von entfernten Netzen' für alle Konfigurationsarten die Option 'nicht erlaubt'.

Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig unter **Management** > **Admin**. Wählen Sie hier im Abschnitt **Konfigurations-Zugriffs-Wege Zugriffs-Rechte** > **Von einer WAN-Schnittstelle** für alle Konfigurationsarten die Option **nicht erlaubt**. Zudem haben Sie die Möglichkeit, den HTTP-Port für die Web Server Dienste zu sperren. Wählen Sie hierfür im Abschnitt **Zugriff auf Web-Server-Dienste** unter **Zugriffs-Rechte** > **Von einer WAN-Schnittstelle** die Option **Deaktiviert**.

Haben Sie die Konfiguration vom Funk-Netzwerk aus zugelassen?

Wenn Sie die Konfiguration vom Funk-Netzwerk aus nicht benötigen, so schalten Sie sie ab. Das Feld zur Abschaltung der Konfiguration vom Funk-Netzwerk aus finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin'. Wählen Sie hier unter 'Zugriffsrechte - Vom Wireless LAN' für alle Konfigurationsarten die Option 'nicht erlaubt'.

Wenn Sie die Konfiguration vom Funk-Netzwerk aus nicht benötigen, so schalten Sie sie ab. Das Feld zur Abschaltung der Konfiguration vom Funk-Netzwerk aus finden Sie ebenfalls in LANconfig unter **Management** > **Admin**. Wählen Sie hier im Abschnitt **Konfigurations-Zugriffs-Wege Zugriffs-Rechte** > **Von einer WLAN-Schnittstelle** für alle Konfigurationsarten die Option **nicht erlaubt**. Zudem haben Sie die Möglichkeit, den HTTP-Port für die Web Server Dienste zu sperren. Wählen Sie hierfür im Abschnitt **Zugriff auf Web-Server-Dienste** unter **Zugriffs-Rechte** > **Von einer WLAN-Schnittstelle** die Option **Deaktiviert**.

Haben Sie die SNMP-Konfiguration mit einem Kennwort versehen?

Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig unter **Management** > **Admin**.

Haben Sie die Firewall aktiviert?

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Allgemein' einschalten.

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter **Firewall/Qos** > **Allgemein** einschalten.

Hinweis: Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Verwenden Sie eine "Deny-All"-Firewall-Strategie?

Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter 'Firewall/QoS' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu findet sich im Referenzhandbuch.

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter **Firewall/Qos** > **Allgemein** einschalten.

Hinweis: Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Verwenden Sie eine “Deny-All” Firewall-Strategie?

Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird “Trojanern” und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** und **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** oder **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln**. Eine Anleitung dazu findet sich im Referenzhandbuch.

Die Stateful-Inspection Firewall der Geräte sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann, wenn Ihr WLAN-Controller als Public Spot eingesetzt wird. Die Firewall können Sie in LANconfig unter **Firewall/Qos** > **Allgemein** einschalten.

Hinweis: Beachten Sie, dass alle Sicherheitsaspekte der Firewall (inkl. IP-Masquerading, Port-Filter und Zugriffs-Liste) nur für Datenverbindungen aktiv sind, die über den IP-Router geführt werden. Direkte Datenverbindungen über die Bridge werden nicht von der Firewall geschützt!

Haben Sie IP-Masquerading aktiviert?

IP-Masquerading heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'IP-Router' auf der Registerkarte 'Routing'.

“IP-Masquerading” heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabellen für IPv4 und

IPv6 finden Sie in LANconfig unter **IP-Router** > **Routing**. Hier haben Sie zusätzlich die Möglichkeit, eine Zeitsteuerung für die Default-Route zu konfigurieren.

Haben Sie kritische Ports über Filter geschlossen?

Die Firewall-Filter des Geräts bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter 'Firewall/QoS' finden Sie die Karteikarte 'Regeln', mit deren Hilfe Filterregeln definiert und verändert werden können.

Die Firewall-Filter des Geräts bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter **Firewall/QoS** > **IPv4-Regeln** > **Regeln** und **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** oder **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Forwarding-Regeln** können Sie Filterregeln definieren und verändern.

Haben Sie bestimmte Stationen von dem Zugriff auf das Gerät ausgeschlossen?

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktio-

nen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf das Gerät gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig unter **Firewall/QoS** > **IPv4-Regeln** und **Firewall/QoS** > **IPv6-Regeln**.

Lagern Sie Ihre abgespeicherte Konfiguration an einem sicheren Ort?

Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

Haben Sie für besonders sensiblen Datenaustausch auf dem Funknetzwerk die Funktionen von IEEE-802.1x eingerichtet?

Wenn Sie auf Ihrem Funk-LAN besonders sensible Daten austauschen, können Sie zur weiteren Absicherung die IEEE-802.1x-Technologie verwenden. Um die IEEE-802.1x-Einstellungen zu kontrollieren oder zu aktivieren, wählen Sie in LANconfig den Konfigurationsbereich '802.1x'.

Wenn Sie auf Ihrem Funk-LAN besonders sensible Daten austauschen, können Sie zur weiteren Absicherung die IEEE-802.1x-Technologie verwenden. Die IEEE-802.1x-Einstellungen zu konfigurieren Sie in LANconfig unter **Wireless-LAN** > **802.1X**.

Haben Sie die Möglichkeiten zum Schutz der WAN-Zugänge bei einem Diebstahl des Gerätes aktiviert?

Nach einem Diebstahl kann ein Gerät theoretisch von Unbefugten an einem anderen Ort betrieben werden. Auch bei einer passwortgeschützten Geräte-Konfiguration könnten so die im Gerät konfigurierten RAS-Zugänge, LAN-Kopplungen oder VPN-Verbindungen unerlaubt genutzt

werden, ein Dieb könnte sich Zugang zu geschützten Netzwerken verschaffen.

Der Betrieb des Gerätes kann jedoch mit verschiedenen Mitteln so geschützt werden, dass es nach dem Wiedereinschalten oder beim Einschalten an einem anderen Ort nicht mehr verwendet werden kann.

Für die GPS-Standort-Verifikation können Sie im Gerät eine erlaubte geografische Position definieren. Nach dem Einschalten prüft das Gerät, ob es sich an der “richtigen” Position befindet – nur bei einer positiven Prüfung wird das Router-Modul eingeschaltet.

Mit den Funktionen des Scripting kann die gesamte Konfiguration des Gerätes nur im RAM gespeichert werden, der beim Booten des Gerätes gelöscht wird. Die Konfiguration wird dabei gezielt nicht in den bootresistenten Flash-Speicher geschrieben. Mit dem Trennen von der Stromversorgung und dem Aufstellen an einem anderen Ort wird damit die gesamte Konfiguration des Gerätes gelöscht (weitere Informationen finden Sie im Referenzhandbuch).

Haben Sie die Speicherung der Konfigurationsdaten Ihren Sicherheitsanforderungen angepasst?

Mit der Funktion des “Autarken Weiterbetriebs” wird die Konfiguration für ein WLAN-Interface, das von einem WLAN-Controller verwaltet wird, nur für eine bestimmte Zeit im Flash bzw. ausschließlich im RAM gespeichert. Die Konfiguration des Geräts wird gelöscht, wenn der Kontakt zum WLAN-Controller oder die Stromversorgung länger als die eingestellte Zeit unterbrochen wird.

Haben Sie den Reset-Taster gegen das unbeabsichtigte Zurücksetzen der Konfiguration gesichert?

Manche Geräte können nicht unter Verschluss aufgestellt werden. Hier besteht die Gefahr, dass die Konfiguration versehentlich gelöscht wird, wenn ein Mitarbeiter den Reset-Taster zu lange gedrückt hält. Mit einer entsprechenden Einstellung kann das Verhalten des Reset-Buttons gesteuert werden, der Reset-Taster wird dann entweder ignoriert oder es wird nur ein Neustart ausgelöst, unabhängig von der gedrückten Dauer.

6 Routing und WAN-Verbindungen

Dieses Kapitel beschreibt die wichtigsten Protokolle und Konfigurationseinträge, die bei WAN-Verbindungen eine Rolle spielen. Es zeigt auch Wege auf, WAN-Verbindungen zu optimieren.

6.1 Allgemeines über WAN-Verbindungen

WAN-Verbindungen werden für folgende Anwendungen verwendet.

- Internet-Zugang
- LAN-LAN-Kopplung
- Remote Access

6.1.1 Brücken für Standard-Protokolle

WAN-Verbindungen unterscheiden sich von direkten Verbindungen (beispielsweise über die LANCAPI) dadurch, dass die Daten im WAN über standardisierte Netzwerk-Protokolle übertragen werden, die auch im LAN Anwendung finden. Direkte Verbindungen arbeiten hingegen mit proprietären Verfahren, die speziell für Punkt-zu-Punkt-Verbindungen entwickelt worden sind.

Über WAN-Verbindungen wird ein LAN erweitert, bei direkten Verbindungen erhält nur ein einzelner PC eine Verbindung zu einem anderen PC. WAN-Verbindungen bilden gewissermaßen Brücken für die Kommunikation zwischen Netzwerken (bzw. für die Anbindung einzelner Rechner an ein LAN).

Welche Protokolle werden auf WAN-Verbindungen eingesetzt?

Auf WAN-Verbindungen über den Highspeed-Anschluss (z. B. DSL-Verbindungen) werden Pakete nach dem IP-Standard übertragen. Geräte mit ISDN-Schnittstelle unterstützen auf der ISDN-Schnittstelle neben IP auch IPX.

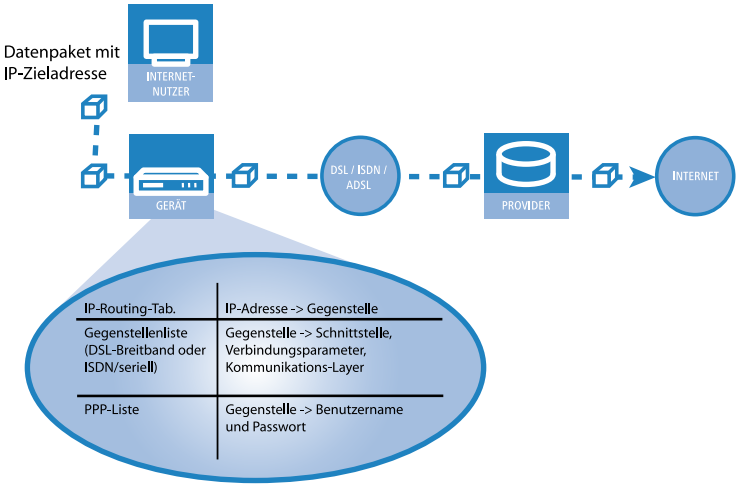
Die enge Zusammenarbeit mit den Router-Modulen

Charakteristisch für WAN-Verbindungen ist die enge Zusammenarbeit mit den Router-Modulen im Gerät. Die Router-Module (IP und IPX) sorgen für die Verbindung von LAN und WAN. Sie bedienen sich der WAN-Module, um Anfragen von PCs aus dem LAN nach externen Ressourcen zu erfüllen.

6.1.2 Was passiert bei einer Anfrage aus dem LAN?

Die Routermodule ermitteln zunächst nur, zu welcher Gegenstelle ein Datenpaket übertragen werden soll. Damit die entsprechende Verbindung ausgewählt und ggf. aufgebaut werden kann, müssen verschiedene Parameter für alle notwendigen Verbindungen vereinbart werden. Diese Parameter sind in unterschiedlichen Listen abgelegt, deren Zusammenspiel die richtigen Verbindungen erlaubt.

Wir wollen diesen Ablauf an einem vereinfachten Beispiel verdeutlichen. Dabei gehen wir davon aus, dass die IP-Adresse des gesuchten Rechners im Internet bekannt ist.



1. Auswahl der richtigen Route

Ein Datenpaket aus einem Rechner findet den Weg ins Internet in erster Linie über die IP-Adresse des Empfängers. Mit dieser Adresse schickt der Rechner das Paket los über das LAN zum Router. Der Router ermittelt in seiner IP-Routing-Tabelle die Gegenstelle, über die die Ziel-IP-Adresse erreichbar ist, z. B. 'Provider'.

2. **Verbindungsdaten für die Gegenstelle**

   Mit diesem Namen prüft der Router dann die Gegenstellenliste und findet die notwendigen Verbindungsdaten für den Provider. Zu diesen Verbindungsdaten gehören z. B die WAN-Schnittstelle (DSL, ISDN) über die der Provider angewählt wird, Protokollinformationen oder die für eine ISDN-Wählverbindung notwendige Rufnummer. Außerdem erhält der Router aus der PPP-Liste Benutzernamen und Passwort, die für die Anmeldung notwendig sind.

3. **Aufbau der WAN-Verbindung**

   Der Router kann dann eine Verbindung über eine WAN-Schnittstelle zum Provider aufbauen. Er authentifiziert sich mit Benutzernamen und Passwort.

4. **Weitergabe des Datenpaketes**

   Sobald die Verbindung hergestellt ist, kann der Router das Datenpaket ins Internet weitergeben.

6.2 IP-Routing

Ein IP-Router arbeitet zwischen Netzen, die TCP/IP als Netzwerk-Protokoll verwenden. Dabei werden nur Daten übertragen, deren Zieladressen in der Routing-Tabelle eingetragen sind. In diesem Abschnitt erfahren Sie, wie die IP-Routing-Tabelle in einem Router von Hirschmann aufgebaut ist und mit welchen weiteren Funktionen das IP-Routing unterstützt wird.

6.2.1 Die IP-Routing-Tabelle

In der IP-Routing-Tabelle sagen Sie dem Router, an welche Gegenstelle (also welchen anderen Router oder Rechner) er die Daten für bestimmte IP-Adressen oder IP-Adress-Bereiche schicken soll. So ein Eintrag heißt auch „Route“, weil der Weg der Datenpakete damit beschrieben wird. Da Sie diese

Einträge selbst vornehmen und sie solange unverändert bleiben, bis Sie selbst sie wieder ändern oder löschen, heißt dieses Verfahren auch „statisches Routing“. Im Gegensatz dazu gibt es natürlich auch ein „dynamisches Routing“. Dabei tauschen die Router selbstständig untereinander Informationen über die Routen aus und erneuern diese fortlaufend. Bei aktiviertem IP-RIP beachtet der IP-Router die statische und die dynamische Routing-Tabelle.

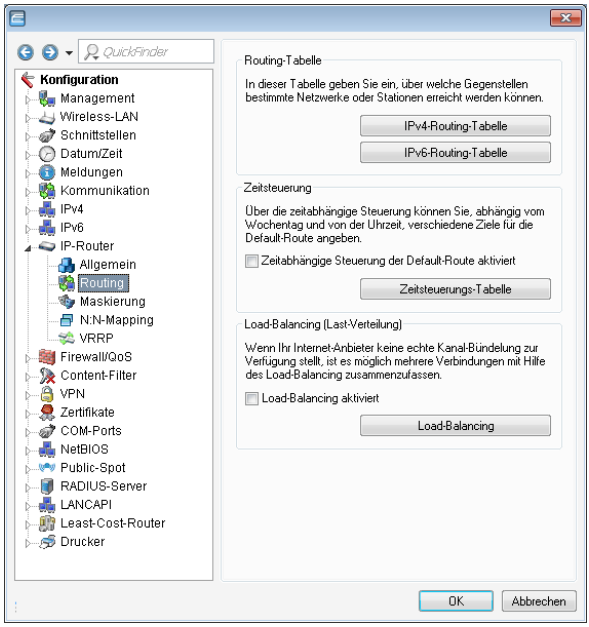
Außerdem sagen Sie dem Router in der IP-Routing-Tabelle, wie weit der Weg über diese Route ist, damit im Zusammenspiel mit IP-RIP bei mehreren Routen zum gleichen Ziel der günstigste ausgewählt werden kann. Die Grundeinstellung für die Distanz zu einem anderen Router ist 0, d.h., der Router ist direkt erreichbar. Alle lokal erreichbaren Geräte, also weitere Router im eigenen LAN oder Arbeitsplatzrechner, die über Proxy-ARP angeschlossen sind, werden mit der Distanz 0 eingetragen. Mit dem gezielten Eintrag einer höheren Distanz (bis 14) wird die „Qualität“ dieser Route herabgesetzt. Solche „schlechteren“ Routen sollen nur dann verwendet werden, wenn keine andere Route zu der entsprechenden Gegenstelle gefunden werden kann.

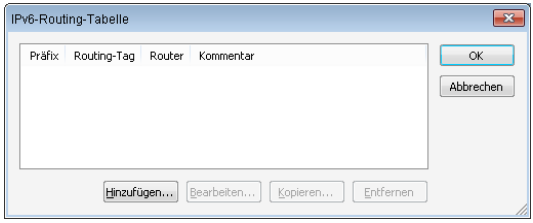
IP-Routing-Tabellen für IPv4/IPv6

Im Gegensatz zu früheren Versionen, in denen es im Konfigurationsmenü eine einzige IP-Routing-Tabelle gab, finden Sie nun an dieser Stelle die Möglichkeit, getrennte Routing-Tabellen für IPv4- und IPv6-Verbindungen zu konfigurieren.

Sie finden die neue Tabelle unter **IP-Router** > **Routing** > **IPv6-Routing-Tabelle**

Alle Einstellungen zu IPv4, die Sie zuvor in der Tabelle **IP-Routing-Tabelle** durchführen konnten, finden Sie nun in der Tabelle **IPv4-Routing-Tabelle**.





Die Tabelle enthält die Einträge für das Routing von Paketen mit IPv6-Adresse.

Präfix

Bestimmen Sie den Präfix des Netzbereiches, dessen Daten zur angegeben Gegenstelle geroutet werden sollen.

Routing-Tag

Geben Sie hier das Routing-Tag für diese Route an. Die so markierte Route ist nur aktiv für Pakete mit dem gleichen Tag. Die Datenpakete erhalten das Routing-Tag entweder über die Firewall oder anhand der verwendeten LAN- oder WAN-Schnittstelle.

Router

Wählen Sie hier die Gegenstelle für diese Route aus.

Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

Hinweis: Die Eingabe eines Kommentars ist optional.

Konfiguration der Routing-Tabelle

LANconfig: IP-Router / Routing / Routing-Tabelle

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / IP-Routing-Tabelle

Eine IP-Routing-Tabelle kann beispielsweise so aussehen:

IP-Adresse	*Netzmaske*	*Routing-Tag*	*Router*	*Distanz*	*Maskierung*	*Aktiv*
192.168.120.0	255.255.255.0	0	MAIN	2	Aus	Ja
192.168.125.0	255.255.255.0	0	NODE1	3	Aus	Ja
192.168.130.0	255.255.255.0	0	191.168.140.123	0	Aus	Ja

Was bedeuten die einzelnen Einträge in der Liste?

- IP-Adresse und Netzmaske

  Das ist die Adresse des Zielnetzes, zu dem Datenpakete geschickt werden können, mit der zugehörigen Netzmaske. Mit der Netzmaske und der Ziel-IP-Adresse aus den ankommenden Datenpaketen prüft der Router, ob das Paket in das Zielnetz gehört.

  Die Route mit der IP-Adresse '255.255.255.255' und der Netzmaske '0.0.0.0' ist die Default-Route. Alle Datenpakete, die nicht durch andere Routing-Einträge geroutet werden können, werden über diese Route übertragen.

- Routing-Tag

  Mit dem Routing-Tag kann die Auswahl der Zielroute genauer gesteuert werden. Dabei wird für die Auswahl der Route nicht nur die Ziel-IP-Adresse, sondern auch weitere Informationen ausgewertet, die den Datenpaketen

über die Firewall zugefügt werden (*Policy-based Routing* auf Seite 468). Mit dem Routing-Tag „0“ gilt der Routing-Eintrag für alle Pakete.

- Router

  An diese Gegenstelle überträgt der Router die zur IP-Adresse und Netzmaske passenden Datenpakete.

  - Ist die Gegenstelle ein Router in einem anderen Netz oder ein einzelner Arbeitsplatzrechner, dann steht hier der Name der Gegenstelle.
  - Kann der eigene Router die Gegenstelle nicht selbst erreichen, steht hier die IP-Adresse eines anderen Routers im LAN, der den Weg ins Zielnetz kennt.

  Der Name der Gegenstellen gibt an, was mit den zur IP-Adresse und Netzmaske passenden Datenpaketen geschehen soll.

  - Routen mit dem Eintrag '0.0.0.0' bezeichnen Ausschluss-Routen. Datenpakete für diese „Null-Routen“ werden verworfen und nicht weitergeleitet. Damit werden z. B. die im Internet verbotenen Routen (private Adressräume, z. B. '10.0.0.0') von der Übertragung ausgeschlossen.
  - Wird als Gegenstelle eine IP-Adresse eingetragen, handelt es sich dabei um einen lokal erreichbaren Router, der für die Übertragung der entsprechenden Datenpakete zuständig ist.

- Distanz

  Anzahl der zwischen dem eigenen und dem Ziel liegenden Router. Dieser Wert wird bei Weitverkehrsverbindungen oft auch mit den Kosten der Übertragung gleichgesetzt und zur Unterscheidung zwischen preiswerten und teuren Übertragungswegen genutzt. Die eingetragenen Distanzwerte werden wie folgt propagiert:

  - Während eine Verbindung zu einem Zielnetz existiert, werden alle über diese Verbindung erreichbaren Netze mit einer Distanz von 1 propagiert.
  - Alle nicht verbundenen Netze werden mit der Distanz propagiert, die in der Routing-Tabelle eingetragen ist (mindestens jedoch mit einer Distanz von 2), solange noch ein freier Übertragungskanal verfügbar ist.
  - Ist kein Kanal mehr frei, so werden die verbleibenden Netze mit einer Distanz 16 (= unreachable) propagiert.

– Eine Ausnahme bilden die Gegenstellen, die über Proxy-ARP angeschlossen sind. Diese „Proxy-Hosts“ werden gar nicht propagiert.

- Maskierung

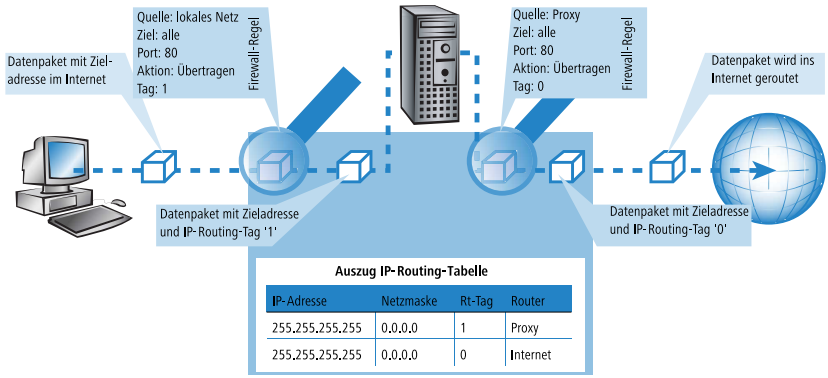
  Mit der Option 'Maskierung' in der Routing-Tabelle informieren Sie den Router darüber, welche IP-Adresse er bei der Weitergabe der Pakete verwenden soll.

  Weitere Informationen finden Sie im Abschnitt *IP-Masquerading* auf Seite 505.

6.2.2 Policy-based Routing

Beim Policy-based Routing wird die Zielroute (also die Gegenstelle, über die die Daten übertragen werden), nicht ausschließlich anhand der Ziel-IP-Adressen ausgewählt. Weitere Informationen wie z. B. der verwendete Dienst oder das verwendete Protokoll sowie Adressen von Absender oder Ziel der Datenpakete können für die Auswahl der Zielroute genutzt werden. Mit Hilfe von Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich, z. B. in folgenden Anwendungsszenarien:

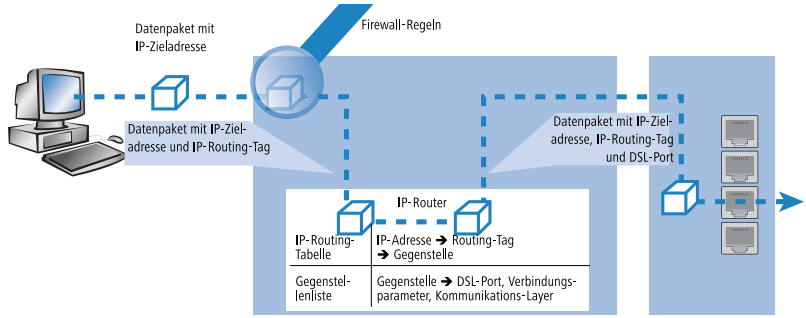
- Der gesamte Internetverkehr eines LANs wird über einen Proxy umgeleitet, ohne das Eintragen der Proxy-Adresse in den Browsern. Das Routing über den Proxy läuft unbemerkt für die Anwender ab, man spricht daher hier auch von einem „transparenten“ Proxy.



- Beim Load-Balancing wird der Datenverkehr für bestimmte Protokolle über einen bestimmten DSL-Port mit einem zusätzlichen externen ADSL-Modem geleitet.
- Ein Server im lokalen Netz, der über eine feste IP-Adresse aus dem WAN erreichbar sein sollte, wird über ein bestimmtes WAN-Interface geroutet.
- Der VPN-Verkehr wird mit dem Routing-Tag '0' durch einen VPN-Tunnel mit dynamischen Endpunkten geleitet, der restliche Internetverkehr der Firma wird mit einem entsprechenden Routing-Tag auf eine andere Firewall umgeleitet.

Um die Kanalauswahl aufgrund anderer Informationen als nur der Ziel-IP-Adresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag“ zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. So wird z. B. über eine Regel dem gesamten Datenverkehr einer lokalen Rechnergruppe (entsprechend dem IP-Adress-Bereich) das Routing-Tag '2' angehängt. Alternativ definieren gezielt einige Protokolle ein anderes Routing-Tag.

Die Zeichnung zeigt die Anwendung des Policy-based Routing beim Load-Balancing:



- Beim Aufbau der Verbindungen prüft zunächst die Firewall, ob die anstehenden Pakete zu einer Regel passen, in der ein Routing-Tag enthalten ist. Das Routing-Tag wird in das Datenpaket eingetragen.

- Mit dem gefundenen Routing-Tag und der Ziel-IP-Adresse kann in der IP-Routing-Tabelle die passende Gegenstelle gefunden werden. Dazu wird die IP-Routing-Tabelle wie üblich von oben nach unten durchgearbeitet.
- Wird ein übereinstimmender Eintrag für das Netzwerk gefunden, wird im zweiten Schritt das Routing-Tag geprüft. Mit dem passenden Routing-Tag kann so die gewünschte Gegenstelle gefunden werden. Über die Gegenstelle kann das Gerät beim Load-Balancing aus der Gegenstellenliste den richtigen DSL-Port ermitteln.

  Hinweis: Wenn das Routing-Tag den Wert „0“ hat (Default), dann gilt der Routing-Eintrag für alle Pakete.

- Interne Dienste verwenden implizit immer das Default-Tag. Wenn der Anwender z. B. die Default-Route durch einen VPN-Tunnel leiten will, der einen dynamischen Tunnelendpunkt hat, so nutzt das VPN-Modul standardmäßig die Default-Route mit dem Routing-Tag „0“.

  Um die Default-Route dennoch durch den VPN-Tunnel zu führen, legen Sie eine zweite Default-Route mit dem Routing-Tag „1“ und der VPN-Gegenstelle als Router-Namen an. Mit einer passenden Firewall-Regel übertragen Sie alle Dienste von allen Quell-Stationen zu allen Ziel-Stationen mit dem Routing-Tag „1“.

- Routing-Tags und RIP: Das Routing-Tag wird auch in RIP-Paketen versendet und beim Empfang ausgewertet, damit z. B. die geänderten Distanzen in den richtigen Routen geändert werden können.

Routing-Tags für VPN- und PPTP-Verbindungen

Routing-Tags werden im Gerät genutzt, um neben der IP-Adresse weitere Kriterien zur Auswahl der Zielroute auswerten zu können. Normalerweise werden die Routing-Tags den Datenpaketen über spezielle Regeln der Firewall hinzugefügt. In manchen Fällen ist es aber erwünscht, die Routing-Tags auf direkterem Wege zuzuweisen.

- Routing-Tags bei VPN-Verbindungen

In der VPN-Namenliste kann für jede VPN-Verbindung das Routing-Tag angegeben werden, das verwendet werden soll, um die Route zum Remote Gateway zu ermitteln (Default '0').

Zusätzlich kann in der Gateway-Tabelle jedem Gateway ein spezifisches Routing-Tag zugeordnet werden. Das Tag 0 hat in dieser Tabelle eine Sonderfunktion: Wenn bei einem Gateway das Tag 0 gesetzt ist, dann wird das Tag aus der VPN-Namenliste-Tabelle verwendet.

Die Einstellungen für die VPN-Routing-Tags finden Sie unter Setup/VPN/VPN-Peers bzw. Setup/VPN/Additional-Gateways sowie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' in der 'Verbindungsliste' und in der Liste 'Weitere entfernte Gateways'.

- Routing-Tags bei PPTP-Verbindungen

In der PPTP-Tabelle kann zusätzlich zur IP-Adresse des PPTP-Servers ein Routing-Tag angegeben werden. Mit Hilfe dieses Routing-Tags können z. B. mehrere DSL-Modems, die eine einheitliche IP-Adresse verwenden, an verschiedenen DSL-Ports betrieben werden.

Peer	*IP-Address*	*Rtg-tag*	*Port*	*SH-Time*
PEER01	10.0.0.138	1	1723	9999
PEER02	10.0.0.138	2	1723	9999

In der IP-Routing-Tabelle sind dazu zwei passend getaggte Routen nötig:

IP-Adresse	*IP-Netzmaske*	*Rtg-tag*	*Peer-oder-IP*	*Distanz*	*Maskierung*
10.0.0.138	255.255.255.255	2	PEER02-PPTP	0	Nein
10.0.0.138	255.255.255.255	1	PEER01-PPTP	0	Nein
192.168.0.0	255.255.0.0	0	0.0.0.0	0	Nein
172.16.0.0	255.240.0.0	0	0.0.0.0	0	Nein
10.0.0.0	255.0.0.0	0	0.0.0.0	0	Nein
224.0.0.0	224.0.0.0	0	0.0.0.0	0	Nein
255.255.255.255	0.0.0.0	0	PEER-LB	0	Ja

Mit diesen Einstellungen und dem entsprechenden Eintrag in der Load-Balancing-Tabelle kann z. B. ein Load-Balancing realisiert werden, dass auch in Österreich verwendet werden kann.

Peer	*Bundle-Peer-1*	*Bundle-Peer-2*	*Bundle-Peer-3*
PEER-LB	PEER01	PEER02	

6.2.3 Lokales Routing

Sie kennen das folgende Verhalten der Arbeitsplatzrechner in einem lokalen Netz: Möchte der Rechner ein Datenpaket an eine IP-Adresse senden, die nicht in seinem eigenen LAN liegt, sucht er nach einem Router, der ihm weiterhelfen kann. Dieser Router wird normalerweise dem Betriebssystem durch den Eintrag als Standard-Router oder Standard-Gateway bekanntgegeben. Gibt es in einem Netz mehrere Router, so kann oft nur ein Standard-Router eingetragen werden, der alle dem Arbeitsplatzrechner unbekannten IP-Adressen erreichen können soll. Manchmal kann dieser Standard-Router jedoch nicht selbst das Zielnetz erreichen, er kennt aber einen anderen Router, der zu diesem Ziel findet.

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man “ICMP-Redirect”). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem sendet er dann keine ICMP-Redirects mehr an die Clients.

Hinweis: Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

Mit dieser Option bestimmen Sie, ob das Gerät ICMP-Redirects versenden soll.

Wie helfen Sie dem Arbeitsplatzrechner nun weiter?

Standardmäßig schickt der Router dem Rechner eine Antwort mit der Adresse des Routers, der die Route ins Ziel-Netz kennt (diese Antwort nennt man “ICMP-Redirect”). Der Arbeitsplatzrechner übernimmt daraufhin diese Adresse und schickt das Datenpaket sofort an den anderen Router.

Manche Rechner können mit den ICMP-Redirects leider nichts anfangen. Um die Datenpakete trotzdem zustellen zu können, verwenden Sie das lokale Routing. Dadurch weisen Sie den Router in Ihrem Gerät an, das Datenpaket selbst zum anderen, zuständigen Router zu senden. Außerdem sendet er dann keine ICMP-Redirects mehr an die Clients. Die Einstellung erfolgt unter:

LANconfig: IP-Router / Allgemein / ICMP-Redirects senden

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / ICMP-Redirects senden

Lokales Routing kann im Einzelfall sehr hilfreich sein, sollte aber auch nur im Einzelfall verwendet werden. Denn lokales Routing führt zu einer Verdoppelung aller Datenpakete zum gewünschten Zielnetz. Die Daten werden erst zum Standard-Router und von diesem erneut zum eigentlich zuständigen Router im lokalen Netz geschickt.

6.2.4 Dynamisches Routing mit IP-RIP

Neben der statischen Routing-Tabelle verfügen Router von Hirschmann auch über eine dynamische Routing-Tabelle. Diese Tabelle füllt der Anwender im Gegensatz zu der statischen nicht aus, das erledigt der Router selbst. Dazu nutzt er das Routing Information Protocol (RIP). Über dieses Protokoll tauschen alle Geräte, die RIP beherrschen, Informationen über die erreichbaren Routen aus.

Welche Informationen werden über IP-RIP propagiert?

Ein Router teilt in den IP-RIP-Informationen den anderen Routern im Netz die Routen mit, die er in seiner eigenen Tabelle findet. Nicht berücksichtigt werden dabei die folgenden Einträge:

- Routen, die mit der Router-Einstellung '0.0.0.0' verworfen werden.
- Routen, die auf andere Router im lokalen Netz lauten.
- Routen, die einzelne Rechner über Proxy-ARP an das LAN anbinden.

Die Einträge in der statischen Routing-Tabelle werden zwar von Hand gesetzt, trotzdem ändern sich diese Informationen je nach Verbindungssituation der Router und damit auch die versendeten RIP-Pakete.

- Solange der Router eine Verbindung zu einer Gegenstelle aufgebaut hat, gibt er alle über diese Route erreichbaren Netze in den RIPs mit der Distanz

'1' weiter. Damit werden andere Router im LAN darüber informiert, dass hier bei diesem Router eine bestehende Verbindung zu dieser Gegenstelle genutzt werden kann. So kann zusätzlicher Verbindungsaufbau von Routern mit Wählverbindungen verhindert und ggf. Verbindungskosten reduziert werden.

- Wenn darüber hinaus in diesem Router keine weitere Verbindung zu einer anderen Gegenstelle aufgebaut werden kann, werden alle anderen Routen mit der Distanz '16' im RIP weitergemeldet. Die '16' steht dabei für „Im Moment ist diese Route nicht erreichbar“. Dass ein Router neben der bestehenden Verbindung keine weitere aufbauen kann, liegt an einer der folgenden Ursachen:
  - Auf allen anderen Kanälen ist schon eine andere Verbindung hergestellt.
  - Die Y-Verbindungen für den S0-Anschluss sind in der Interface-Tabelle ausdrücklich ausgeschlossen.
  - Die bestehende Verbindung benutzt alle B-Kanäle (Kanalbündelung).
  - Bei der bestehenden Verbindung handelt es sich um eine Festverbindung. Nur wenige ISDN-Anbieter ermöglichen es, neben einer Festverbindung auf dem ersten B-Kanal eine Wählverbindung auf dem zweiten B-Kanal aufzubauen.

Welche Informationen entnimmt der Router aus empfangenen IP-RIP-Paketen?

Wenn der Router IP-RIP-Pakete empfängt, baut er sie in seine dynamische IP-Routing-Tabelle ein, und die sieht etwa so aus:

IP-Adresse	*IP-Netzmaske*	*Zeit*	*Distanz*	*Router*
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Was bedeuten die Einträge?

IP-Adresse und Netzmaske bezeichnen das Ziel-Netz, die Distanz gibt die Anzahl der zwischen Sender und Empfänger liegenden Router an, die letzte Spalte zeigt an, welcher Router diese Route bekannt gemacht hat. Mit der

'Zeit' zeigt die dynamische Tabelle an, wie alt die entsprechende Route ist. Der Wert in dieser Spalte gilt als Multiplikator für das Intervall, in dem die RIP-Pakete eintreffen, eine '1' steht also für etwa 30 Sekunden, eine '5' für etwa 2,5 Minuten usw. Wenn eine Information über eine Route neu eintrifft, gilt diese Route natürlich als direkt erreichbar und erhält die Zeit '1'. Nach Ablauf der entsprechenden Zeit wird der Wert in dieser Spalte automatisch erhöht. Nach 3,5 Minuten wird die Distanz auf '16' gesetzt (Route nicht erreichbar), nach 5,5 Minuten wird die Route gelöscht.

Wenn der Router nun ein IP-RIP-Paket empfängt, muss er entscheiden, ob er die darin enthaltenen Routen in seine dynamische Tabelle aufnehmen soll oder nicht. Dazu geht er wie folgt vor:

- Die Route ist in der Tabelle noch gar nicht vorhanden, dann wird sie aufgenommen (sofern Platz in der Tabelle ist).
- Die Route ist in der Tabelle vorhanden mit der Zeit von '5' oder '6'. Die neue Route wird dann verwendet, wenn sie die gleiche oder eine bessere Distanz aufweist.
- Die Route ist in der Tabelle vorhanden mit der Zeit von '7' bis '10', hat also die Distanz '16'. Die neue Route wird auf jeden Fall verwendet.
- Die Route ist in der Tabelle vorhanden. Die neue Route kommt von dem gleichen Router, der auch diese Route bekannt gegeben hat, hat aber eine schlechtere Distanz als der bisherige Eintrag. Wenn ein Gerät so die Verschlechterung seiner eigenen statischen Routing-Tabelle bekannt macht (z. B. durch den Abbau einer Verbindung steigt die Distanz von '1' auf '2', siehe unten), dann glaubt der Router ihm das und nimmt den schlechteren Eintrag in seine dynamische Tabelle auf.

Hinweis: RIP-Pakete aus dem WAN werden nicht beachtet und sofort verworfen! RIP-Pakete aus dem LAN werden ausgewertet und nicht im LAN weitergeleitet!

Zusammenspiel: statische und dynamische Tabelle

Aus der statischen und der dynamischen Tabelle stellt der Router die eigentliche IP-Routing-Tabelle zusammen, mit der er den Weg für die Datenpakete bestimmt. Dabei nimmt er zu den Routen aus der eigenen statischen Tabelle die Routen aus der dynamischen Tabelle auf, die er selber nicht kennt oder die eine kürzere Distanz aufweisen als die eigene (statische) Route.

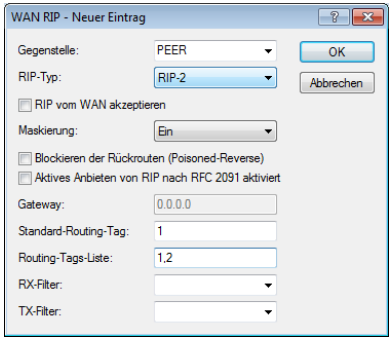
Skalierung durch IP-RIP

Verwenden Sie mehrere Router in einem lokalen Netz mit IP-RIP, können Sie die Router im lokalen Netz nach außen hin als einen einzigen großen Router darstellen. Dieses Vorgehen nennt man auch „Skalierung“. Durch den regen Informationsaustausch der Router untereinander steht so ein Router mit prinzipiell beliebig vielen Übertragungswegen zur Verfügung.

Konfiguration der IP-RIP-Funktion

Um die über RIP gelernten und statisch definierten Routen auch über das WAN bekannt zu machen oder Routen aus dem WAN zu lernen, können die entsprechenden Gegenstellen in der WAN-RIP-Tabelle eingetragen werden.

LANconfig: IP-Router / Allgemein / WAN RIP



WEBconfig: Setup / IP-Router / RIP / WAN-Tabelle

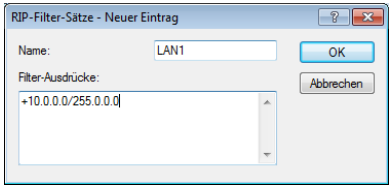
Hinweis: RIP-fähige Router versenden die RIP-Pakete ungefähr alle 30 Sekunden. Der Router ist nur dann auf das Versenden und Empfangen von RIPs eingestellt, wenn er eine eindeutige IP-Adresse hat. In der Grundeinstellung mit der IP-Adresse xxx.xxx.xxx.254 ist das IP-RIP-Modul ausgeschaltet.

RIP-Filter

Über RIP gelernte Routen können durch die Einstellungen bei LAN- und WAN-RIP nach dem Routing-Tag gefiltert werden. Um die Routen zusätzlich über

die Angabe von Netzadressen zu filtern (z. B. „Lerne nur Routen, die im Netz 192.168.0.0/255.255.0.0 liegen“), werden in einer zentralen Tabelle zunächst die Filter definiert, die dann von Einträgen in der LAN- und WAN-RIP-Tabelle genutzt werden können.

LANconfig: IP-Router / Allgemein / RIP-Filter-Sätze

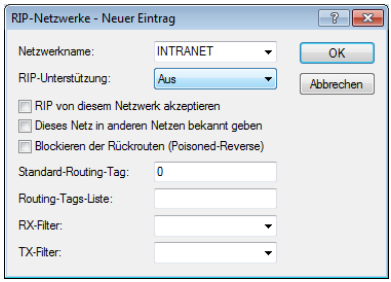


Telnet: Setup / IP-Router / RIP / Filter

RIP für Netzwerke getrennt einstellen

Ebenso wie beim NetBIOS-Proxy ist es meistens nicht erwünscht, dass die lokale Netzstruktur über RIP in die DMZ propagiert wird. Außerdem ist es zwar manchmal erwünscht, in ein Netzwerk die bekannten Routen zwar zu propagieren, von dort aber keine Routen zu lernen (wie z. B. auch im WAN). Der RIP-Funktionalität kann daher für jedes Netzwerk getrennt eingestellt werden

LANconfig: IP-Router / Allgemein / RIP-Netzwerke



WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / RIP / LAN-Tabelle

Timereinstellungen

Das Routing Information Protocol (RIP) versendet regelmäßige Update-Nachrichten an die benachbarten Router mit Informationen über die erreichbaren Netzwerke und die zugehörigen Metriken (Hops). RIP verwendet verschiedene Timer, um den Austausch der Routing-Informationen zeitlich zu steuern.

WEBconfig: Setup/ IP-Router/ RIP/ Parameter

Triggered Update im LAN

Bei einem Triggered Update werden Änderungen in den Metriken sofort an die benachbarten Router gemeldet, nicht erst beim nächsten regelmäßigen Update. Damit es bei Fehlkonfigurationen im Netzwerk nicht zu massenhaften Update-Nachrichten kommt, wird eine so genannte Update-Verzögerung (Update-Delay) definiert.

- Update-Delay

  Die Update-Verzögerung startet, sobald die Routing-Tabelle bzw. Teile davon propagiert wurden. Solange dieses Verzögerung läuft, werden neue Routing-Informationen zwar angenommen und in die Tabelle eingetragen, aber nicht sofort weitergeleitet. Der Router meldet die aktuellen Einträge erst nach Ablauf der Verzögerung aktiv weiter.

  Der hier konfigurierte Wert gibt die Obergrenze der Verzögerung an – die tatsächliche Verzögerung wird immer zufällig ermittelt und liegt zwischen einer Sekunde und dem hier angegebenen Wert.

Triggered Update im WAN

Anders als im LAN sind auf WAN-Strecken regelmäßige Updates alle 30 Sekunden ggf. unerwünscht, weil die Bandbreite beschränkt ist. Daher können nach RFC 2091 alle Routen im WAN nur noch einmal beim Verbindungsaufbau übertragen werden, danach nur noch Updates.

Da in diesem Fall die Updates explizit angefragt werden, können keine Broadcasts oder Multicasts für die Zustellung der RIP-Nachrichten verwendet werden. Stattdessen muss im Filialgerät die IP-Adresse des nächsten

erreichbaren Routers in der Zentrale statisch konfiguriert werden. Der Zentralrouter kann sich aufgrund der Anfragen merken, von welchen Filialroutern er Update-Requests empfangen hat, um etwaige Routenänderungen über passende Messages direkt an das Filialgerät zu senden.

Zur Konfiguration des triggered Update im WAN wird die WAN-RIP-Tabelle erweitert.

Poisoned Reverse

Poisoned Reverse dient dazu, Routing-Schleifen zu verhindern. Dazu wird an den Router, der die beste Route zu einem Netz propagiert hat, dieses Netz auf dem zugehörigen Interface als unerreichbar zurückpropagiert.

Gerade auf WAN-Strecken hat dies aber einen entscheidenden Nachteil: Hier werden von der Zentrale sehr viele Routen gesendet, die dann als nicht erreichbar zurückpropagiert werden und so gegebenenfalls die verfügbare Bandbreite belasten. Daher kann die Verwendung von Poisoned Reverse auf jedem Interface (LAN/WAN) manuell aktiviert werden.

Zur Konfiguration der Poisoned Reverse werden LAN- und WAN-RIP-Tabelle erweitert.

Statische Routen, die immer propagiert werden

Neben den dynamischen Routen propagiert ein Router über RIP auch die statisch konfigurierten Routen. Dabei sind manche der statischen Routen nicht immer erreichbar, z. B. weil eine notwendige Internetverbindung oder ein Wählzugang temporär nicht verfügbar sind.

Mit der Angabe der „Aktivität“ in der Routingtabelle kann für eine statische Route definiert werden, ob sie immer propagiert werden soll oder nur dann, wenn die Route auch tatsächlich erreichbar ist.

WEBconfig: Setup/ IP-Router/ IP-Routing-Tabelle

6.2.5 SYN/ACK-Speedup

Das SYN/ACK-Speedup-Verfahren dient der Beschleunigung des IP-Datenverkehrs. Beim SYN/ACK-Speedup werden IP-Kontrollzeichen (SYN für Synchronisation und ACK für Acknowledge) innerhalb des Sendebuffers

gegenüber einfachen Datenpaketen bevorzugt behandelt. Dadurch wird die Situation vermieden, dass Kontrollzeichen länger in der Sendeschlange hängen bleiben und die Gegenstelle deshalb aufhört, Daten zu senden.

Der größte Effekt tritt beim SYN/ACK-Speedup bei schnellen Anschlüssen (z. B. ADSL) ein, wenn gleichzeitig in beiden Richtungen mit hoher Geschwindigkeit Datenmengen übertragen werden.

Werkseitig ist der SYN/ACK-Speedup eingeschaltet.

Ausschalten in Problemfällen

Durch die bevorzugte Behandlung einzelner Pakete wird die ursprüngliche Paketreihenfolge geändert. Obwohl TCP/IP keine bestimmte Paketreihenfolge gewährleistet, kann es in einzelnen Anwendungen zu Problemen kommen. Das betrifft nur Anwendungen, die abweichend vom Protokollstandard eine bestimmte Paketreihenfolge voraussetzen. Für diesen Fall kann der SYN/ACK-Speedup ausgeschaltet werden:

LANconfig: IP-Router / Allgemein / TCP SYN- und ACK-Pakete bevorzugt weiterleiten

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Routing-Methode / SYN/ACK-Speedup

6.3 Advanced Routing and Forwarding (ARF)

6.3.1 Einleitung

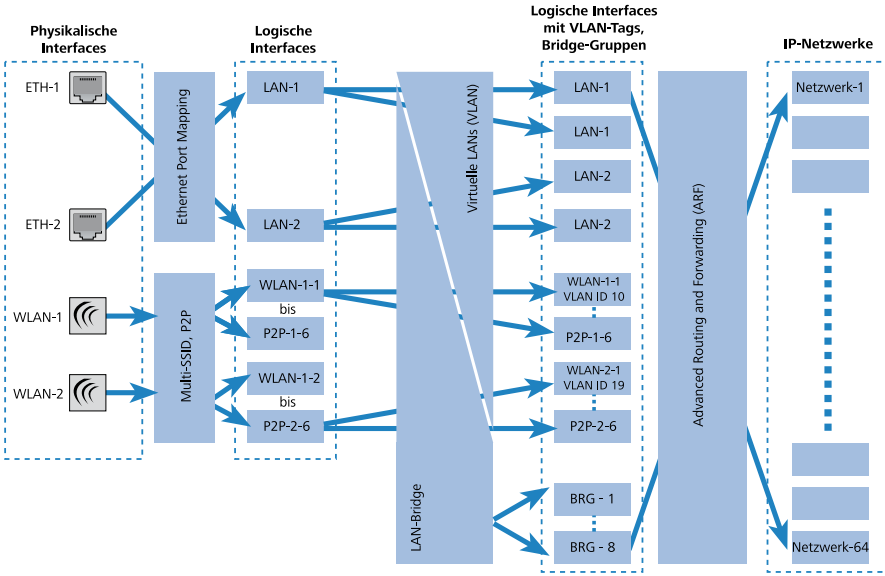
In einfachen Anwendungsfällen verwaltet ein Gerät lediglich zwei lokale Netzwerke: das Intranet und die DMZ. In einer komplexeren Umgebung ist es jedoch oft wünschenwert, mehr als ein Intranet und eine DMZ mit einem Gerät zu realisieren, um auf diese Weise z. B. mehreren IP-Netzen über ein zentrales Gerät den Zugang zum Internet zu ermöglichen. Aktuelle Geräte unterstützen je nach Modell bis zu 64 verschiedene IP-Netzwerke.

Bei der Realisierung von mehreren IP-Netzwerken sind mehrere Szenarien möglich:

- Ein Netzwerk je Interface.

- Mehrere Netzwerke je Interface.
- Mehrere VLANs je Interface, auf jedem VLAN ein oder mehrere Netzwerke (das entspricht einer Kombination aus den ersten beiden Szenarien).

Um diese Szenarien zu ermöglichen, stehen mit den Funktionen des Advanced Routing and Forwarding (ARF) sehr flexible Möglichkeiten zur Definition von IP-Netzwerken und der Zuordnung dieser Netzwerke zu den Interfaces bereit. Das untenstehende Diagramm verdeutlicht die Zuordnung von Netzwerken zu Interfaces auf verschiedenen Ebenen. Die dabei verwendeten Konfigurationsmöglichkeiten werden in den folgenden Kapiteln vorgestellt.



So verläuft die Zuordnung von IP-Netzwerken zu Interfaces:

- Je nach Modell haben die Geräte eine unterschiedliche Anzahl von physikalischen Interfaces, also Ethernet-Ports oder WLAN-Module. Diesen zugeordnet sind die logischen Interfaces:
  - Für die Ethernet-Ports geschieht die Zuordnung durch das Ethernet Port Mapping.

Hinweis: Die Anzahl der logischen LAN-Interfaces entspricht nicht bei allen Modellen der Anzahl der verfügbaren physikalischen Ethernet-Ports.

- Für die WLAN-Module entstehen durch den Aufbau von Point-to-Point-Strecken (P2P) bzw. durch die Verwendung von Multi-SSID auf jedem physikalischen WLAN-Modul mehrere WLAN-Interfaces: bis zu 16 WLAN-Netze und bis zu 16 P2P-Strecken pro Modul.

▶ Diese logischen Interfaces werden im nächsten Schritt weiter spezifiziert bzw. gruppiert:

- Bei Geräten mit VLAN-Unterstützung können für jedes logische Interface durch die Verwendung von VLAN-IDs mehrere VLANs definiert werden. Der Datenverkehr der verschiedenen VLANs läuft dann zwar ggf. über ein gemeinsames logisches Interface ab, wird aber durch die VLAN-ID streng von den anderen VLANs getrennt. Aus Sicht der Geräte stellen sich die VLANs also als separate Interfaces dar, aus einem einzelnen logischen Interface werden also für das Gerät mehrere logische Interfaces, die einzeln angesprochen werden können.
- Bei Geräten mit WLAN-Modulen können die einzelnen logischen Interfaces zu Gruppen zusammengefasst werden. Dazu wird die LAN-Bridge verwendet, welche die Datenübertragung zwischen den LAN- und WLAN-Interfaces regelt. Durch die Zusammenfassung zu Bridge-Gruppen (BRG) können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für das Gerät wie ein einzelnes Interface – damit wird also das Gegenteil des VLAN-Verfahrens erreicht.

▶ Im letzten Schritt wird durch die Möglichkeiten des ARF eine Verbindung zwischen den logischen Interfaces mit VLAN-Tags und den Bridge-Gruppen einerseits sowie den IP-Netzwerken andererseits hergestellt. Ein IP-Netzwerk enthält daher in der Konfiguration den Verweis auf ein logisches Interface (ggf. mit VLAN-ID) oder eine Bridge-Gruppe. Darüber hinaus kann für jedes IP-Netzwerk ein Schnittstellen-Tag festgelegt werden, mit dem ein IP-Netz auch ohne Firewall-Regel von anderen Netzen getrennt werden kann.

Gerade die zuletzt dargestellte Definition von Schnittstellen-Tags für IP-Netze stellt einen der bedeutenden Vorteile des Advanced Routing and Forwarding dar – mit Hilfe dieser Option werden „virtuelle Router“ realisiert. Ein virtueller

Router nutzt anhand des Schnittstellen-Tags für ein IP-Netz nur einen Teil der Routing-Tabelle und steuert so das Routing ganz speziell für dieses eine IP-Netzwerk. Auf diese Weise können in der Routing-Tabelle z. B. mehrere Default-Routen definiert werden, jeweils mit Routing-Tags versehen. Die virtuellen Router für die IP-Netze wählen anhand dieser Tags diejenige Default-Route aus, die für das jeweilige IP-Netz mit dem passenden Schnittstellen-Tag gilt. Die Separation der IP-Netzwerke über die virtuellen Router geht so weit, dass sogar mehrere IP-Netzwerke mit identischem Adresskreis problemlos parallel in einem Gerät betrieben werden können.

Ein Beispiel: In einem Bürogebäude sollen mehrere Firmen über ein zentrales Gerät an das Internet angebunden werden, dabei hat jede Firma einen eigenen Internetprovider. Alle Firmen wollen das oft verwendete IP-Netzwerk '10.0.0.0' mit Netzmaske '255.255.255.0' nutzen. Um diese Aufgabe zu realisieren, wird für jede Firma ein IP-Netz '10.0.0.0/255.255.255.0' mit einem eindeutigen Namen und einem eindeutigen Schnittstellen-Tag angelegt. In der Routing-Tabelle wird für jeden Internetprovider eine entsprechende Default-Route mit dem passenden Routing-Tag angelegt. Auf diese Weise können die Clients in den verschiedenen Firmennetzen mit den gleichen IP-Adressen über ihren jeweiligen Provider das Internet nutzen. Mit dem Einsatz von VLANs können die logischen Netzwerke auch auf demselben physikalischen Medium (Ethernet) voneinander getrennt werden.

Unterschiede zwischen Routing-Tags und Schnittstellen-Tags

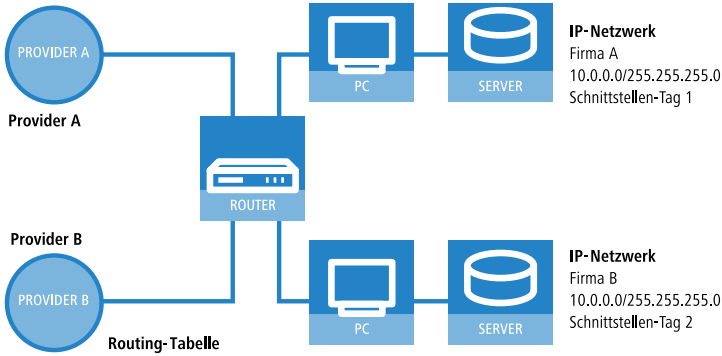
Routing-Tags, die über die Firewall zugewiesen werden, und die über IP-Netzwerke definierten Schnittstellen-Tags haben einiges gemeinsam, es gibt aber auch wichtige Unterschiede:

- Der Router wertet beide Tags gleich aus. Für die Pakete mit dem Schnittstellen-Tag '2' gelten also alle Routen mit Routing-Tag '2' in der Routing-Tabelle (und alle Routen mit Default-Routing-Tag '0'). Die gleichen Routen gelten auch für Pakete, denen die Firewall das Routing-Tag '2' zugewiesen hat.

  Das heißt, beim Routing wird das Schnittstellen-Tag wie ein Routing-Tag verwendet!

- Schnittstellen-Tags schränken aber darüber hinaus noch die Sichtbarkeit (oder Erreichbarkeit) der Netzwerke untereinander ein:

- Grundsätzlich können sich nur Netzwerke mit gleichem Schnittstellen-Tag untereinander „sehen“, also Verbindungen in das jeweils andere Netz aufbauen.
- Netzwerke mit dem Schnittstellen-Tag '0' haben eine besondere Bedeutung – sie sind quasi Supervisor-Netze. Diese Netze können alle anderen Netze sehen, also Verbindungen in andere Netze aufbauen. Netze mit Schnittstellen-Tag ungleich '0' können hingegen keine Verbindungen in die Supervisor-Netze aufbauen.
- Netzwerke vom Typ 'DMZ' sind unabhängig vom Schnittstellen-Tag für alle anderen Netzwerke sichtbar – das ist auch sinnvoll, da in der DMZ oft öffentlich zugängliche Server wie Webserver etc. stehen. Die DMZ-Netze selbst sehen aber nur die Netze mit gleichem Schnittstellen-Tag (und natürlich alle anderen DMZ-Netze).
- Einen Sonderfall stellen Netze vom Typ 'DMZ' mit dem Schnittstellen-Tag '0' dar: diese Netze können als „Supervisor-Netz“ selbst alle anderen Netze sehen, werden aber auch gleichzeitig von allen anderen Netze gesehen.



IP-Adresse	Netzmaske	Schnittstellen-Tag	Router
255.255.255.255	0.0.0.0	1	Provider A
255.255.255.255	0.0.0.0	2	Provider B

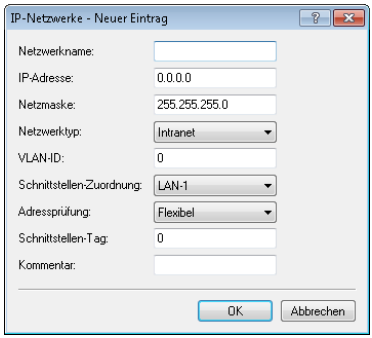
Hinweis: In Fällen, die keine eindeutige Zuordnung der IP-Adressen über die Schnittstellen-Tags erlauben, wird das Advanced Routing and Forwarding durch entsprechende Firewall-Regeln unterstützt. Das ist im vorge-

nannten Beispiel der Fall, wenn in jedem Netzwerk ein öffentlich erreichbarer Web- oder Mailserver steht, die ebenfalls die gleiche IP-Adresse verwenden.

6.3.2 Definition von Netzwerken und Zuordnung von Interfaces

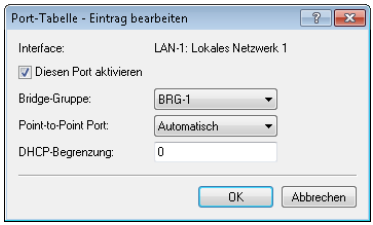
Bei der Definition eines Netzwerkes wird zunächst festgelegt, welcher IP-Adress-Kreis auf einem bestimmten lokalen Interface des Routers gültig sein soll. “Lokale Interfaces” sind dabei logische Interfaces, die einem physikalischen Ethernet- (LAN) oder Wireless-Port (WLAN) zugeordnet sind. Um die oben aufgeführten Szenarien zu realisieren, können durchaus mehrere Netzwerke auf einem Interface aktiv sein – umgekehrt kann ein Netzwerk auch auf mehreren Interfaces aktiv sein (über Bridge-Gruppen).

Die Netzwerke werden in einer Tabelle unter **IPv4** > **Allgemein** > **IP-Netzwerke** definiert. Neben der Definition des Adresskreises und der Interfacezuordnung wird darin auch ein eindeutiger Name für die Netzwerke festgelegt. Dieser Netzwerkname erlaubt es, die Netze in anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) zu identifizieren und diese Dienste nur in bestimmten Netzen anbieten zu können.



6.3.3 Zuweisung von logischen Interfaces zu Bridge-Gruppen

Unter **Schnittstellen** > **LAN** definieren Sie in der **Port-Tabelle** spezielle Eigenschaften der logischen Interfaces.



Diesen Port aktivieren

Mit dieser Option wird das logische Interface aktiviert oder deaktiviert.

Bridge-Gruppe

Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu diesem logischen Interface über die LAN-Bridge. Durch die Zuordnung zu einer gemeinsamen Bridge-Gruppe können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für den Router wie ein einzelnes Interface – z. B. für die Nutzung im Zusammenhang mit Advanced Routing and Forwarding.

Wird das Interface über die Einstellung **keine** aus allen Bridge-Gruppen entfernt, so findet keine Übertragung über die LAN-Bridge zwischen LAN und WLAN statt (isolierter Modus). In dieser Einstellung ist eine Datenübertragung zwischen LAN und WLAN für dieses Interface nur über den Router möglich.

Hinweis: Voraussetzung für die Datenübertragung von/zu einem logischen interface über die LAN-Bridge ist die Deaktivierung des globalen “Isolierten Modus”, der für die gesamte LAN-Bridge gilt. Außerdem muss das logische Interface einer Bridge-Gruppe zugeordnet sein – in der Einstellung **keine** ist keine Übertragung über die LAN-Bridge möglich.

Point-to-Point Port

Dieser Wert beschreibt die in der IEEE 802.1D definierte “adminPointToPointMAC”-Einstellmöglichkeit. Standardmäßig wird die Point-to-Point-Einstellung der LAN-Schnittstelle automatisch aufgrund der Technologie und des momentanen Status hergeleitet. Es ist jedoch möglich, diese automatisch getroffene Festlegung zu revidieren, falls diese z. B. nicht brauchbar für die vorliegende Konfiguration erscheint.

Hinweis: Schnittstellen im Point-to-Point-Modus haben besondere Fähigkeiten, die benutzt werden können, um z. B. im Rapid-Spanning-Tree Verfahren die Port-Status-Wechsel zu beschleunigen.

DHCP-Begrenzung

Anzahl der Clients, die über DHCP zugewiesen werden können. Bei Überschreiten des Limits wird der jeweils älteste Eintrag verworfen. Dies kann in Kombination mit der Protokoll-Filter-Tabelle genutzt werden, um den Zugang auf ein logisches Interface zu begrenzen.

6.3.4 Schnittstellen-Tags für Gegenstellen

Mit der Definition von Schnittstellen-Tags können im Rahmen des Advanced Routing and Forwarding (ARF) virtuelle Router genutzt werden, die nur einen Teil der gesamten Routing-Tabelle verwenden. Bei den aus dem WAN eingehenden Datenpaketen kann die Zuordnung der Schnittstellen-Tags auf unterschiedliche Weise geregelt werden:

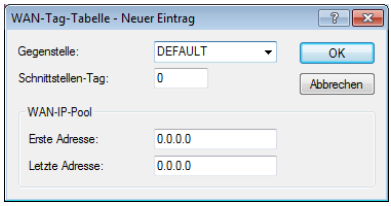
- mit Hilfe von entsprechenden Firewall-Regeln, die nur Datenpakete von bestimmten Gegenstellen, IP-Adressen oder Ports erfassen
- anhand der Routing-Tabelle
- über eine explizite Zuordnung der Tags zu den Gegenstellen.

Mit der Zuordnung der Tags zu den Gegenstellen kann die Trennung der ARF-Netze auch für WAN-seitig empfangende Pakete komfortabel genutzt werden (die standardmäßig das Tag 0 erhalten). Ohne eine Zuordnung der Tags explizit über die Firewall zu steuern kann der virtuelle Router in Form des Schnittstellen-Tags direkt aus der Gegenstelle bzw. der Quellroute bestimmt werden. Ein- und ausgehende Kommunikation kann somit einfacher bidirektional in virtuelle Router unterteilt werden.

Hinweis: Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

Zuweisung von Schnittstellen-Tags über die Tag-Tabelle

LANconfig: Kommukination / Gegenstellen / WAN-Tag-Tabelle



WEBconfig: Setup / IP-Router

- WAN-Tag-Erzeugung

  Mit der WAN-Tag-Erzeugung wird die Quelle für die Zuordnung von Schnittstellen-Tags definiert. Neben der Zuordnung über die Firewall oder direkte Zuordnung über die Tag-Tabelle kann das Schnittstellen-Tag auch anhand Quellroute in der effektiven Routing-Tabelle gewählt werden (statische Routing-Einträge plus Routen, die über RIP gelernt wurden). Die Quell-IP und der Name der Gegenstelle, über welche die IP-Verbindung aufgebaut wurde, wird mit der Routing Information verglichen. Das Routing-Tag dieser Quellroute wird den WAN-seitig empfangenen Paketen dieser Verbindung für die weitere Verarbeitung zugewiesen. Enthält die effektive Routing-Tabelle mehrere Einträge für eine Gegenstelle mit gleichem Netzwerk, so wird das kleinste Tag verwendet.

  Beispiel: Es sind folgende ARF-Netze definiert:

Netzwerk	*IP-Adresse*	*Rtg-tag*	*Port*
PRIVAT	192.168.1.1/24	1	LAN-1
HOMEOFFICE	192.168.10.1/24	10	LAN-2

  PRIVAT soll nur das Internet nutzen, HOMEOFFICE nur einen VPN Tunnel zur Gegenstelle VPN-FIRMA. Die entsprechende effektive Routing-Tabelle sieht so aus:

IP-Adresse	*IP-Netmaske*	*Rtg-tag*	*Gegenstelle*	*Distanz*	*Maskierung*
192.168.10.0	255.255.255.0	10	VPN-FIRMA	0	No

IP-Adresse	IP-Netmaske	Rtg-tag	Gegenstelle	Distanz	Maskierung
255.255.255.255	0.0.0.0	1	INTERNET	0	No

- Datenpaket kommt aus dem Netz 192.168.10.x: Tag = 10
- Datenpaket kommt aus dem Netz 192.168.1.x: Tag = 1
- Datenpaket kommt aus einem beliebigen anderen Netz: Tag = 0

Mögliche Werte:

- Manual: In dieser Einstellung werden die Schnittstellen-Tags ausschließlich über einen Eintrag in der Tag-Tabelle bestimmt. Die Routing-Tabelle hat keine Bedeutung für die Zuordnung der Schnittstellen-Tags.
- Auto: In dieser Einstellung werden die Schnittstellen-Tags zunächst über einen Eintrag in der Tag-Tabelle bestimmt. Wird dort kein passender Eintrag gefunden, so wird das Tag anhand der Routing-Tabelle ermittelt .

Hinweis: Sowohl die über die Tag-Tabelle, als auch die anhand der Routing-Tabelle ermittelten Schnittstellen-Tags können durch einen passenden Eintrag in der Firewall überschrieben werden.

6.3.5 Ermittlung des Routing-Tags für lokale Routen

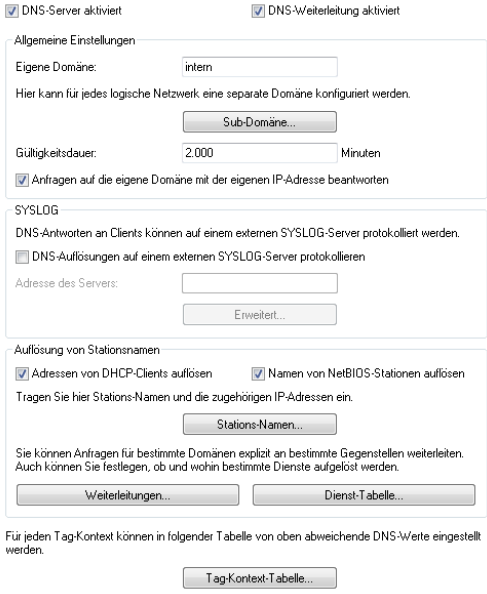
Mit der Definition von Schnittstellen-Tags können im Rahmen des Advanced Routing and Forwarding (ARF) virtuelle Router genutzt werden, die nur einen Teil der gesamten Routing-Tabelle verwenden. Für ein von einem anderen lokalen Router empfangenes Paket wird das Schnittstellen-Tag in den folgenden Schritten ermittelt:

1. Wenn die Absenderadresse eines Pakets direkt einem im Gerät definierten IP-Netz zugeordnet werden kann, dann wird das Schnittstellen-Tag des IP-Netzes verwendet.
2. Wenn an dem Interface, über das ein Paket empfangen wurde, nur ein IP-Netz gebunden ist, dann wird das Schnittstellen-Tag dieses IP-Netzes verwendet.
3. Wenn die Möglichkeiten a und b kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der MAC-Adresse die IP-Adresse des Next-Hops zu ermitteln (reverse ARP-Lookup). Anhand dieser IP-Adresse versucht das Gerät, das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.

4. Wenn die Möglichkeiten a bis c kein eindeutiges Ergebnis liefern, versucht das Gerät anhand der Einträge in der Routing-Tabelle das zugehörige IP-Netz und so das Schnittstellen-Tag zu ermitteln.

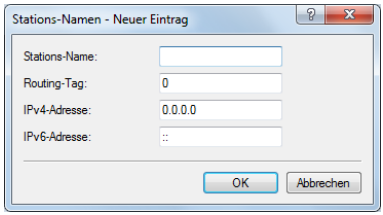
6.3.6 Routing-Tags für DNS-Weiterleitung

Bei der DNS-Weiterleitung sind mehrere voneinander unabhängige Forwarding-Definitionen (insbesondere allgemeine Wildcard-Definitionen mit "*") durch die Kennzeichnung mit eindeutigen Routing-Tags möglich. Abhängig vom Routing-Kontext des anfragenden Clients berücksichtigt der Router nur die passend gekennzeichneten Forwarding-Einträge sowie die allgemeinen, mit "0" gekennzeichneten Einträge.



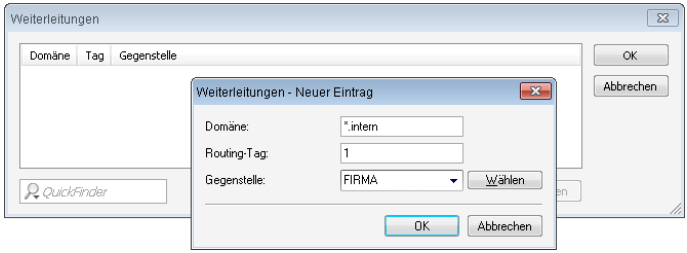
Stations-Namen

Unter **Konfiguration** > **IPv4** > **DNS** > **Stations-Namen** definieren Sie, welche Stations-Namen das Gerät wie und in welchem Tag-Kontext auflöst.



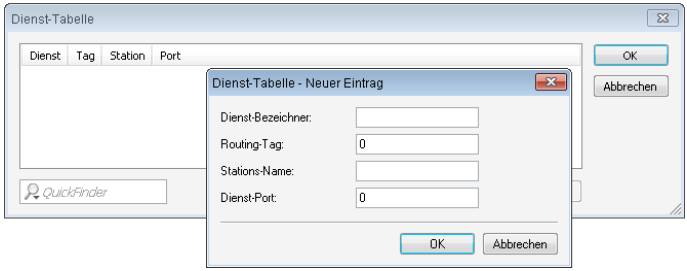
DNS-Weiterleitungen

Unter **Konfiguration** > **IPv4** > **DNS** > **Weiterleitungen** versehen Sie Weiterleitungsregeln mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag zur Verfügung stehen.



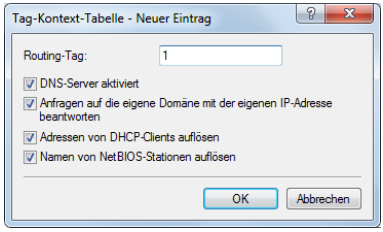
Dienst-Tabelle

Unter **Konfiguration** > **IPv4** > **DNS** > **Dienst-Tabelle** versehen Sie Dienste mit Routing-Tags, so dass diese nur mit dem korrekten Routing-Tag erreichbar sind.



Tag-Kontext-Tabelle

Im LANconfig lassen sich unter **Konfiguration** > **IPv4** > **DNS** > **Tag-Kontext-Tabelle** Tag-Kontexte definieren, die die globalen Einstellungen des DNS-Servers für bestimmte Schnittstellen- und Routing-Tags (Routing-Kontext) überschreiben:



Wenn ein Eintrag für einen Tag-Kontext existiert, dann gelten für diesen Kontext nur die DNS-Einstellungen in dieser Tabelle. Existiert hingegen kein Eintrag in dieser Tabelle, dann gelten die globalen Einstellungen des DNS-Servers.

Folgende Optionen sind je Tag-Kontext möglich:

- **Routing-Tag**: Eindeutiges Schnittstellen- bzw. Routing-Tag im Bereich von 1-65535, dessen folgende Einstellungen die globalen Einstellungen des DNS-Servers überschreiben sollen.
- **DNS-Server aktiviert**: Aktiviert den DNS-Server des Gerätes.
- **Anfragen auf die eigene Domäne mit der eigenen IP-Adresse beantworten**: Wenn aktiviert, werden DNS-Anfragen betreffs der eigenen Domäne mit der IP-Adresse des Routers beantwortet.
- **Adressen von DHCP-Clients auflösen**: Aktiviert die Auflösung von Stations-Namen, die über DHCP eine IP-Adresse angefordert haben.
- **Namen von NetBIOS-Stationen auflösen**: Aktiviert die Auflösung von Stations-Namen, die dem NetBIOS-Router bekannt sind.

6.3.7 Virtuelle Router

Die interfaceabhängige Filterung ermöglicht es – zusammen mit dem Policy-based Routing – für jedes Interface virtuelle Router zu definieren.

Beispiel:

Es werden zwei separate IP-Netze verwendet für Entwicklung und Vertrieb. Beide Netze hängen an verschiedenen Switchports, verwenden aber das gleiche Netz '10.1.1.0/255.255.255.0'. Der Vertrieb soll nur ins Internet dürfen, während die Entwicklung auch auf das Netz einer Partnerfirma ('192.168.1.0/255.255.255.0") zugreifen darf.

Es ergibt sich folgende Routing-Tabelle (dabei hat die Entwicklungsabteilung das Tag 2 und der Vertrieb das Tag 1):

IP-Adresse	*IP-Netzmaske*	*Rtg-tag*	*Peer-oder-IP*	*Distanz*	*Maskierung*	*Aktiv*
192.168.1.0	255.255.255.0	2	PARTNER	0	nein	ja
192.168.0.0	255.255.0.0	0	0.0.0.0	0	nein	ja
255.255.255.255	0.0.0.0	2	INTERNET	2	ja	ja
255.255.255.255	0.0.0.0	1	INTERNET	2	ja	ja

Stünden Entwicklung und Vertrieb in IP-Netzen mit unterschiedlichen Adressbereichen, wäre die Zuordnung der Routing-Tags über Firewall-Regeln kein Problem. Da aber beide Abteilungen im gleichen IP-Netz stehen, ist nur eine Zuordnung über die Netzwerknamen möglich.

Die Zuweisung der Tags kann direkt bei der Netzwerk-Definition erfolgen:

Netzwerkname	*IP-Adresse*	*Netzmaske*	*VLAN-ID*	*Interface*	*Adressprüfung*	*Typ*	*Rtg-Tag*
ENTWICKLUNG	10.1.1.1	255.255.255.0	0	LAN-1	streng	Intranet	2
VERTRIEB	10.1.1.1	255.255.255.0	0	LAN-2	streng	Intranet	1

Alternativ kann die Zuweisung der Tags auch über die Kombination von Netzwerkdefinitionen und Firewallregeln erfolgen. Die Netze sind wie folgt definiert:

Netzwerkname	*IP-Adresse*	*Netzmaske*	*VLAN-ID*	*Interface*	*Adressprüfung*	*Typ*	*Rtg-Tag*
ENTWICKLUNG	10.1.1.1	255.255.255.0	0	LAN-1	streng	Intranet	0
VERTRIEB	10.1.1.1	255.255.255.0	0	LAN-2	streng	Intranet	0

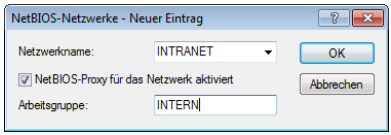
Dann lassen sich durch die Routing-Tags folgende Firewall-Regeln festlegen:

Name	*Protokoll*	*Quelle*	*Ziel*	*Aktion*	*verknuepft*	*Prio*	*(...)*	*Rtg-tag*
ENTWICKLUNG	ANY	%Lentwicklung	ANYHOST	%a	ja	255		2
VERTRIEB	ANY	%Lvertrieb	ANYHOST	%a	ja	255		1

Wichtig bei diesen Regeln ist die maximale Priorität (255), damit die Regeln immer als erstes ausgewertet werden. Damit nun trotz dieser Regeln noch eine Filterung nach Diensten möglich ist, muss die Option "verknuepft" in der Firewall-Regel gesetzt sein.

6.3.8 NetBIOS-Proxy

Aus Sicherheitsgründen muss der NetBIOS-Proxy in seinem Verhalten den jeweiligen Netzwerken angepasst werden, da er z. B. üblicherweise nicht in der DMZ aktiv sein soll. Der NetBIOS-Proxy kann daher für jedes Netzwerk getrennt eingestellt werden



LANconfig: NetBIOS / Allgemein / NetBIOS-Netzwerke

WEBconfig: HiLCOS-Menübaum / Setup / NetBIOS / Netzwerke

- Netzwerkname

  Name des Netzwerks, für das der NetBIOS-Proxy aktiviert werden soll.

- NetBIOS-Proxy für das Netzwerk aktiviert

  Diese Option gibt an, ob der NetBIOS-Proxy für das ausgewählte Netzwerk aktiviert wird oder nicht.

- Arbeitsgruppe

  Die Arbeitsgruppe oder Domäne, die von den Clients im Netzwerk verwendet wird. Bei mehreren Arbeitsgruppen reicht die Angabe einer Arbeitsgruppe.

  Hinweis: In der Default-Einstellung sind sowohl 'Intranet' als auch 'DMZ' in dieser Tabelle eingetragen, dabei ist der NetBIOS-Proxy für das Intranet aktiviert und für die DMZ deaktiviert.

Sobald ein Netzwerk über ein Schnittstellen-Tag verfügt, sind von diesem Netz aus nur Namen (Hosts und Gruppen) sichtbar, die in einem Netz mit dem gleichen Tag stehen, bzw. über eine passende (mit dem selben Tag)

getaggte WAN-Route erreichbar sind. Ein ungetaggtes Netz hingegen sieht alle Namen. Genauso sind alle Namen, die aus ungetaggten Netzen gelernt wurden, für alle Netze sichtbar.

Der DNS-Server berücksichtigt bei der Namensauflösung die Interface-Tags, d.h. es werden auch über DNS nur Namen aufgelöst, die aus einem Netz mit dem gleichen Tag gelernt wurden. Auch hier gilt die Sonderrolle ungetaggter Netze.

Die Arbeitsgruppe/Domäne dient dazu, beim Start des Gerätes das Netzwerk nach NetBIOS-Namen abscannen zu können. Diese ist i.A. für jedes Netz verschieden und muss daher überall angegeben werden. In Netzwerken ohne Domäne sollte hier der Name der größten Arbeitsgruppe angegeben werden.

6.4 Die Konfiguration von Gegenstellen

Gegenstellen werden in zwei Tabellen konfiguriert:

- In der Gegenstellenliste (bzw. den Gegenstellenlisten) werden alle Informationen eingestellt, die individuell für nur eine Gegenstelle gelten.
- Parameter für die unteren Protokollebenen (unterhalb von IP bzw. IPX) werden in der Kommunikations-Layer-Tabelle definiert.

Hinweis: In diesem Abschnitt wird die Konfiguration der Authentifizierung (Protokoll, Benutzername, Passwort) nicht behandelt. Informationen zur Authentifizierung finden Sie im Abschnitt *Verbindungsaufbau mit PPP* auf Seite 539.

6.4.1 Gegenstellenliste

Die verfügbaren Gegenstellen werden in der Gegenstellenliste mit einem geeigneten Namen und zusätzlichen Parametern angelegt. Für jedes WAN-Interface gibt es eine separate Gegenstellenliste. Die Gegenstellenlisten können auf folgenden Wegen aufgerufen werden:

LANconfig: Kommunikation / Gegenstellen / Gegenstellen (DSL)

WEBconfig: HiLCOS-Menübaum / Setup / WAN / DSL-Breitband-Gegenstellen bzw. Einwahl-Gegenstellen

Für eine Gegenstelle sind folgende Parameter erforderlich:

Gegenstellen-liste	*Parameter*	*Bedeutung*
DSL-Breitband-Gegenstellen	Name	Mit diesem Namen wird die Gegenstelle in den Router-Modulen identifiziert. Sobald das Router-Modul anhand der IP-Adresse ermittelt hat, bei welcher Gegenstelle das gewünschte Ziel erreicht werden kann, können aus der Gegenstellenliste die zugehörigen Verbindungsparameter ermittelt werden.
	Haltezeit	Diese Zeit gibt an, wie lange die Verbindung aktiv bleibt, nachdem keine Daten mehr übertragen wurden. Wird eine Null als Haltezeit angegeben, wird die Verbindung nicht automatisch beendet. Bei einer Haltezeit von 9999 Sekunden werden abgebrochene Verbindungen selbstständig wiederhergestellt (siehe *Dauerverbindung für Flatrates – Keep-alive* auf Seite 550).
	Access Concentrator	Der Access Concentrator (AC) steht für den Server, der über diese Gegenstelle erreicht werden kann. Stehen mehrere Provider zur Auswahl, die über Ihren ADSL-Anschluss genutzt werden können, wählen Sie mit dem Namen des AC den Provider aus, der für den IP-Adresskreis dieser Gegenstelle zuständig ist. Der Wert für den AC wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den AC eingetragen, wird jeder AC angenommen, der den geforderten Service anbietet.
	Service	Tragen Sie hier den Dienst ein, den Sie bei Ihrem Provider nutzen möchten. Das kann z. B. einfaches Internet-Surfen sein oder aber auch Video-Downstream. Der Wert für den Service wird Ihnen von Ihrem Provider mitgeteilt. Wird kein Wert für den Service eingetragen, wird jeder Service angenommen, den der geforderte AC anbietet.
	Layername	Wählen Sie den Kommunikations-Layer aus, der für diese Verbindung verwendet werden soll. Die Konfiguration dieser Layer ist im folgenden Abschnitt beschrieben.
	VPI	Virtual Path Identifier.
	VCI	Virtual Channel Identifier. Die Werte für VCI und VPI werden vom ADSL-Netzbetreiber mitgeteilt. Übliche Werte für die Kombination von VPI und VCI sind: 0/35, 0/38, 1/32, 8/35, 8/48.
Einwahl-Gegenstellen	Name	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Rufnummer	Eine Rufnummer wird nur benötigt, wenn die Gegenstelle angerufen werden soll. Das Feld kann leer bleiben, wenn lediglich Rufe angenommen werden sollen. Mehrere Rufnummern für dieselbe Gegenstelle können in der RoundRobin-Liste eingetragen werden.
	Haltezeit	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Haltezeit für Bündelung	Der zweite B-Kanal in einer Bündelung wird abgebaut, wenn er für die eingestellte Dauer nicht benutzt wurde.
	Layername	Wie in der Liste der DSL-Breitband-Gegenstellen.
	Automatischer Rückruf	Der automatische Rückruf ermöglicht eine sichere Verbindung und senkt die Kosten für den Anrufer.

Hinweis: Bitte beachten Sie bei der Bearbeitung der Gegenstellenlisten folgende Hinweise:

- Werden in zwei Gegenstellenlisten (z. B. DSL-Breitband-Gegenstellen und Einwahl-Gegenstellen) Einträge mit identischen Namen für die Gegenstelle vorgenommen, verwendet das Gerät beim Verbindungsaufbau zu der entsprechenden Gegenstelle automatisch das “schnellere” Interface. Das andere Interface wird in diesem Fall als Backup verwendet.
- Werden in der Liste der DSL-Breitband-Gegenstellen weder Access Concentrator noch Service angegeben, stellt der Router eine Verbindung zum ersten AC her, der sich auf die Anfrage über die Vermittlungsstelle meldet.
- Für ein ggf. vorhandenes DSLoL-Interface gelten die gleichen Einträge wie für ein DSL-Interface. Die Einträge dazu werden in der Liste der DSL-Breitband-Gegenstellen vorgenommen.

6.4.2 Layer-Liste

Mit einem Layer definieren Sie eine Sammlung von Protokoll-Einstellungen, die für die Verbindung zu bestimmten Gegenstellen verwendet werden soll. Die Liste der Kommunikations-Layer finden Sie unter:

LANconfig: Kommunikation / Allgemein / Kommunikations-Layer

WEBconfig: HiLCOS-Menübaum / Setup / WAN / Layer

In der Kommunikations-Layer-Liste sind die gängigen Protokollkombinationen bereits vordefiniert. Änderungen oder Ergänzungen sollten Sie nur vornehmen, wenn Gegenstellen inkompatibel zu den vorhandenen Layern sind. Die möglichen Optionen finden Sie in der folgenden Übersicht.

Hinweis: Beachten Sie, dass die im Gerät vorhandenen Parameter vom Funktionsumfang des Gerätes abhängen. Es kann daher sein, dass Ihr Gerät nicht alle hier beschriebenen Optionen anbietet.

Parameter	*Bedeutung*	
Layername	Unter diesem Namen wird der Layer in den Gegenstellenlisten ausgewählt.	
Encapsulation	Für die Datenpakete können zusätzliche Kapselungen eingestellt werden.	
	'Transparent'	Keine zusätzliche Kapselung.
	'Ethernet'	Kapselung als Ethernet-Frames.

Parameter	*Bedeutung*	
	'LLC-ETH'	Ethernet über ATM mit LLC-Kapselung nach RFC 2684.
	'LLC-MUX'	Multiplexing über ATM mit LLC/SNAP-Kapselung nach RFC 2684. Mehrere Protokolle können im selben VC (Virtual Channel) übertragen werden.
	'VC-MUX'	Multiplexing über ATM durch Aufbau zusätzlicher VCs nach RFC 2684.
Layer-3	Folgende Optionen stehen für die Vermittlungsschicht (oder Netzwerkschicht) zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'PPP'	Der Verbindungsaufbau erfolgt nach dem PPP-Protokoll (im synchronen Modus, d. h. bitorientiert). Die Konfigurationsdaten werden der PPP-Tabelle entnommen.
	'AsyncPPP'	Wie 'PPP', nur wird der asynchrone Modus verwendet. PPP arbeitet also zeichenorientiert.
	'... mit Script'	Alle Optionen können wahlweise mit eigenem Script ausgeführt werden. Das Script wird in der Script-Liste angegeben.
	'DHCP'	Zuordnung der Netzwerkparameter über DHCP.
Layer-2	In diesem Feld wird der obere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Folgende Optionen stehen zur Verfügung:	
	'Transparent'	Es wird kein zusätzlicher Header eingefügt.
	'X.75LAPB'	Verbindungsaufbau nach X.75 und LAPM (Link Access Procedure Balanced).
	'PPPoE'	Kapselung der PPP-Protokollinformationen in Ethernet-Frames.
Optionen	Hier können Sie die Kompression der übertragenen Daten aktivieren. Die gewählte Option wird nur dann wirksam, wenn sie sowohl von den verwendeten Schnittstellen als auch von den gewählten Layer-2- und Layer-3-Protokollen unterstützt wird.	
Layer-1	In diesem Feld wird der untere Teil der Sicherungsschicht (Data Link Layer) konfiguriert. Weitere Informationen finden Sie in der Dokumentation zu Setup-Parameter 2.2.4.6 Lay-1.	

6.5 Generic Routing Encapsulation (GRE)

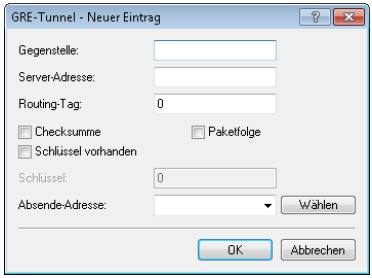
6.5.1 Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)

Das GRE-Protokoll tunnelt beliebige Layer-3-Datenpakete (u. a. IP, IPsec, ICMP etc.) über eine Point-to-Point-Netzwerkverbindung, indem es diese Daten mit einem IP-Daten-Gerüst umgibt. Das ist unter anderem dann hilfreich,

wenn beide Kommunikationspartner ein bestimmtes Übertragungsprotokoll verwenden (z. B. IPsec), das auf dem Übertragungsweg nicht zur Verfügung steht. Da GRE selbst keine Verschlüsselung der getunnelten Daten durchführt, müssen beide Kommunikationspartner für die Absicherung dieser Daten sorgen.

Konfiguration eines GRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines GRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **GRE-Tunnel**.



Gegenstelle

Name der Gegenstelle dieses GRE-Tunnels. Verwenden Sie diesen Namen z. B. in der Routing-Tabelle, um Daten durch diesen GRE-Tunnel zu versenden.

Server-Adresse

Adresse des GRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum GRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem GRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten

eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses GRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem GRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere GRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden GRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem GRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Hinweis: Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

Um IPv6 als GRE-Tunnel Transport Protokoll zu verwenden, erstellen Sie unter **IPv6** > **WAN-Schnittstellen** einen neuen Eintrag, z. B. "IPV6GRE". Diese Schnittstelle vergeben Sie anschließend bei der Konfiguration des entsprechenden GRE-Tunnels als **Gegenstelle**.

Falls die Angabe einer IP-Adresse für die Tunnel-Schnittstelle notwendig ist, gehen Sie wie folgt vor:

IPv4-Adresse

Erstellen Sie unter **Kommunikation** > **Protokolle** > **IP-Parameter** einen neuen Eintrag und geben Sie für den Gegenstellennamen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **IP-Adresse** und **Netzmaske** die notwendigen Werte.

IPv6

Erstellen Sie unter **IPv6** > **Allgemein** > **IPv6-Adressen** einen neuen Eintrag und geben Sie für den Netzwerknamen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **Adresse/Präfixlänge** die notwendigen Werte.

6.5.2 Ethernet-over-GRE (EoGRE)

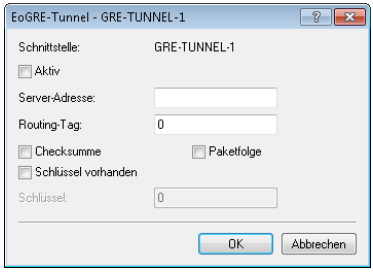
Hinweis: Weitere Informationen zum GRE-Potokoll finden Sie unter *Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)*.

Die aktuelle HiLCOS-Version stellt mehrere “Ethernet over GRE”-Tunnel (EoGRE) zur Verfügung, um Ethernet-Pakete per GRE zu übertragen. Da sich diese Ethernet-Pakete auf OSI-Layer-2 bewegen, bieten diese EoGRE-Tunnel lediglich eine Bridge-Funktionalität an.

Auf diese Weise lassen sich beispielsweise L2VPN (VPN als einfache Level-2-Brigde) oder eine transparente Ethernet-Bridge über WAN realisieren.

Konfiguration eines EoGRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines EoGRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **EoGRE-Tunnel** und der Auswahl des entsprechenden Tunnels.



Schnittstelle

Name des gewählten EoGRE-Tunnels.

Aktiv

Aktiviert oder deaktiviert den EoGRE-Tunnel. Deaktivierte EoGRE-Tunnel senden oder empfangen keinen Daten.

Server-Adresse

Adresse des EoGRE-Tunnel-Endpunktes (gültige IPv4- oder IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum EoGRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem EoGRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses EoGRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem EoGRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere EoGRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden EoGRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem EoGRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das

Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

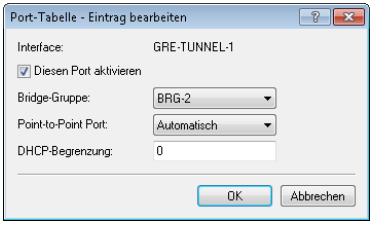
Lokale Schnittstelle mit einem EoGRE-Tunnel verbinden

Um eine lokale Schnittstelle mit einem EoGRE-Tunnel zu verbinden, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** > **EoGRE-Tunnel** einen neuen Eintrag.

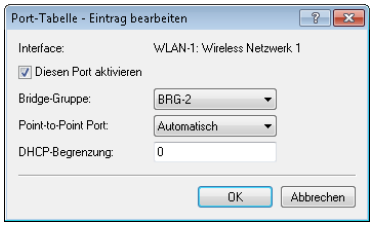
   Aktivieren Sie den Tunnel und geben Sie unter **Server-Adresse** die Adresse des entfernten Gerätes an, zu dem der EoGRE-Tunnel bestehen soll (IPv4- oder IPv6-Adresse oder FQDN).

2. Ergänzen Sie unter **Schnittstellen** > **LAN** > **Port-Tabelle** eine Bridge-Gruppe um den aktivierten EoGRE-Tunnel.



   Aktivieren Sie den Port und wählen Sie die gewünschte Bridge-Gruppe aus.

3. Ergänzen Sie ebenfalls unter **Schnittstellen** > **LAN** > **Port-Tabelle** dieselbe Bridge-Gruppe um das lokale Interface, das Sie über den EoGRE-Tunnel verbinden möchten (z. B. WLAN-1).



Aktivieren Sie den Port und wählen Sie aus der Liste dieselbe Bridge-Gruppe aus, in der sich auch der EoGRE-Tunnel befindet.

6.6 IP-Masquerading

Eine der häufigsten Aufgaben für Router ist heute die Anbindung vieler Arbeitsplätze in einem LAN an das Netz der Netze, das Internet. Jeder soll nach Möglichkeit direkt von seinem Arbeitsplatz aus z. B. auf das Internet zugreifen und sich brandaktuelle Informationen für seine Arbeit holen können.

Damit nicht jeder Arbeitsplatzrechner mit seiner IP-Adresse im gesamten Internet bekannt sein muss, wird das „IP-Masquerading“ als Versteck für alle Rechner im Intranet eingesetzt. Beim IP-Masquerading treffen zwei gegensätzliche Forderungen an den Router aufeinander: Zum einen soll er eine im lokalen Netz gültige Intranet-IP-Adresse haben, damit er aus dem LAN erreichbar ist, zum anderen soll er eine im Internet gültige, öffentliche IP-Adresse haben (fest vergeben sein oder vom Provider dynamisch zugewiesen).

Da diese beiden Adressen prinzipiell nicht in einem logischen Netz liegen dürfen, muss der Router über zwei IP-Adressen verfügen:

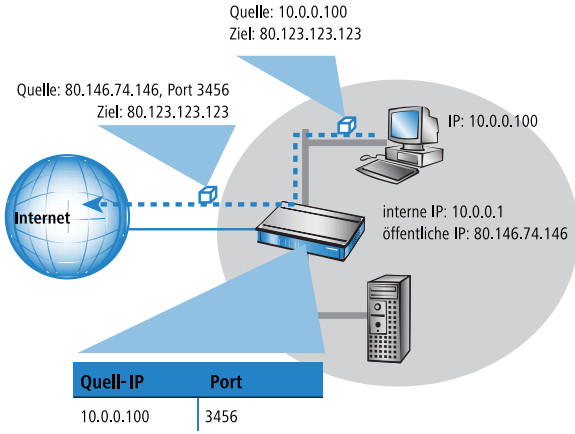
- die Intranet IP-Adresse zur Kommunikation mit den Rechnern im LAN
- die öffentliche IP-Adresse zur Kommunikation mit den Gegenstellen im Internet

Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet.

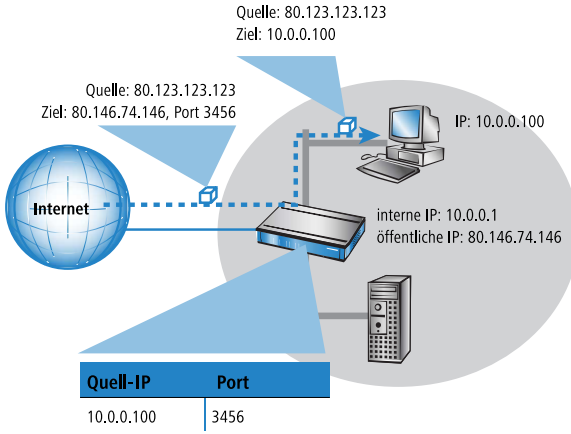
6.6.1 Einfaches Masquerading

Wie funktioniert IP-Masquerading?

Das Masquerading nutzt die Eigenschaft der Datenübertragung über TCP/IP aus, dass neben der Quell- und Ziel-Adresse auch Portnummer für Quelle und Ziel verwendet werden. Bekommt der Router nun ein Datenpaket zur Übertragung, merkt er sich die IP-Adresse und den Port des Absenders in einer internen Tabelle. Dann gibt er dem Paket seine eigene IP-Adresse und eine beliebige neue Portnummer. Diesen neuen Port trägt er ebenfalls in der Tabelle ein und leitet das Paket mit den neuen Angaben weiter.



Die Antwort auf dieses Paket geht nun an die IP-Adresse des Routers mit der neuen Absender-Portnummer. Mit dem Eintrag in der internen Tabelle kann der Router diese Antwort nun wieder dem ursprünglichen Absender zuordnen.



Welche Protokolle können mit IP-Masquerading übertragen werden?

Das IP-Masquerading funktioniert problemlos für all jene IP-Protokolle, die auf TCP, UDP oder ICMP basieren und dabei ausschließlich über Ports kommunizieren. Zu diesen unproblematischen Protokollen zählt beispielsweise das Basis-Protokoll des World Wide Web: HTTP.

Einzelne IP-Protokolle verwenden zwar TCP oder UDP, kommunizieren allerdings nicht ausschließlich über Ports. Derartige Protokolle verlangen beim IP-Masquerading eine entsprechende Sonderbehandlung. Zu den vom IP-Masquerading im Gerät unterstützten Protokollen mit Sonderbehandlung gehören:

- FTP (über die Standardports)
- H.323 (im Umfang, wie ihn Microsoft Netmeeting verwendet)
- PPTP
- IPSec
- IRC

Konfiguration des IP-Masquerading

Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle erreichen Sie wie folgt:

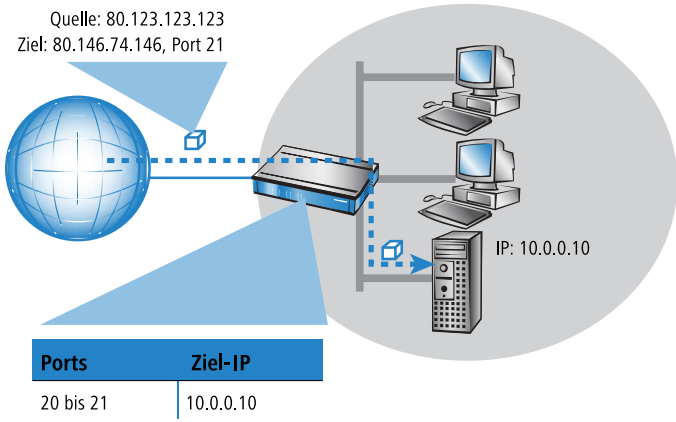
LANconfig: IP-Router / Routing / Routing-Tabelle

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / IP-Routing-Tab

6.6.2 Inverses Masquerading

Beim einfachen Masquerading werden alle IP-Adressen im lokalen Netz hinter der IP-Adresse des Routers maskiert (versteckt). Soll nun ein bestimmter Rechner im LAN für Stationen aus dem Internet erreichbar sein (z. B. ein FTP-Server), dann ist bei Einsatz des einfachen Masquerading auch die IP-Adresse des FTP-Servers im Internet nicht bekannt. Ein Verbindungsaufbau zu diesem FTP-Server aus dem Internet ist also so nicht mehr möglich.

Um den Zugriff auf einen solchen Server (“exposed host”) im LAN zu ermöglichen, wird in einer Tabelle (Port-Forwarding-Tabelle) die IP-Adresse des FTP-Servers eingetragen mit allen Diensten (Ports), die er auch außerhalb des LANs anbieten soll. Schickt nun ein Rechner aus dem Internet ein Paket an den FTP-Server im LAN, so sieht es für diesen Rechner so aus, als wäre der Router der FTP-Server. Der Router liest anhand des verwendeten Protokolls aus dem Eintrag in der Port-Forwarding-Tabelle die IP-Adresse des FTP-Servers im LAN und leitet das Paket an die dort eingetragene lokale IP-Adresse weiter. Alle Pakete, die vom FTP-Server im LAN kommen (Antworten des Servers), werden wieder hinter der IP-Adresse des Routers versteckt.



Der generelle Unterschied zwischen einfachem und inversem Masquerading:

- Der Zugriff von außen auf einen Dienst (Port) im Intranet muss beim inversen Masquerading manuell durch Angabe einer Port-Nummer definiert werden. In der Port-Forwarding-Tabelle wird dazu der Ziel-Port mit der Intranet-Adresse z. B. des FTP-Servers angegeben.
- Beim Zugriff aus dem LAN auf das Internet hingegen wird der Eintrag in der Tabelle mit Port- und IP-Adress-Informationen automatisch durch den Router selbst vorgenommen.

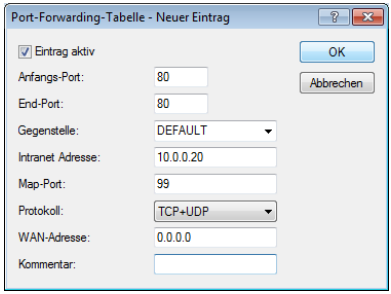
Hinweis: Die entsprechende Tabelle kann max. 2048 Einträge aufnehmen, also gleichzeitig 2048 Übertragungen zwischen dem maskierten und dem unmaskierten Netz ermöglichen.

Nach einer einstellbaren Zeit geht der Router jedoch davon aus, dass der Eintrag nicht mehr benötigt wird, und löscht ihn selbständig wieder aus der Tabelle.

Hinweis: Stateful-Inspection und inverses Masquerading: Wenn im Masquerading-Modul ein Port freigeschaltet wird (d.h. alle auf diesem Port empfangenen Pakete sollen an einen Rechner im lokalen Netz weitergeleitet werden), so erfordert dies bei einer Deny-All Firewall-Strategie einen **zusätzlichen** Eintrag in der Stateful-Inspection Firewall, der den Zugriff aller Rechner auf den jeweiligen Server ermöglicht.

Manchmal ist es allerdings gewünscht, dass der so eingerichtete „exposed host“ nicht mit dem standardmäßig verwendeten Port angesprochen wird, sondern aus Sicherheitsgründen ein anderer Port verwendet wird. In diesem Fall wird also nicht nur das Umsetzen von Ports auf eine IP-Adresse benötigt, sondern auch das Umsetzen auf andere Ports (Port-Mapping). Ein weiteres Anwendungsbeispiel für diese Port-Umsetzung ist das Umsetzen von mehreren Ports aus dem WAN auf einen gemeinsamen Port im LAN, die jedoch verschiedenen IP-Adressen zugeordnet werden (N-IP-Mapping).

Bei der Konfiguration des Port-Mappings wird einem Port oder Portbereich (Anfangs-Port bis End-Port) eine IP-Adresse aus dem LAN als Ziel und der im LAN zu verwendende Port (Map-Port) zugewiesen.



LANconfig: IP-Router / Maskierung / Port-Forwarding-Tabelle

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / 1-N-NAT / Service-Tabelle

- Anfangs-Port

  Anfangs-Port für den Dienst.

- End-Port

  End-Port für den Dienst.

- Gegenstelle

  Gegenstelle, für die dieser Eintrag gültig ist. Die Verwendung von virtuellen Routern (*Advanced Routing and Forwarding (ARF)* auf Seite 480) erfordert beim Port-Forwarding eine gezielte Auswahl der Gegenstelle. Wird keine Gegenstelle angegeben, gilt der Eintrag für alle Gegenstellen.

- Intranet-Adresse

Intranet-Adresse, an die ein im Portbereich liegendes Paket weitergeleitet wird.

- Map-Port

  Port, mit dem das Paket weitergeleitet wird.

  Hinweis: Wird als Map-Port die „0“ eingetragen, werden im LAN die gleichen Ports verwendet wie im WAN. Wird ein Portbereich umgesetzt, gibt der Map-Port den ersten verwendeten Port im LAN an. Beim Umsetzen des Portbereichs '1200' bis '1205' auf den internen Map-Port '1000' werden also die Ports von 1000 bis einschließlich 1005 für den Datenverkehr im LAN verwendet.

  Hinweis: Das Port-Mapping ist statisch, deshalb können zwei Ports oder Portbereiche nicht auf den gleichen Map-Port eines Ziel-Rechners im LAN umgesetzt werden. Für verschiedene Zielrechner können gleiche Port-Mappings verwendet werden.

- Protokoll

  Protokoll, für das dieser Eintrag gültig ist.

- WAN-Adresse

  WAN-Adresse, für die dieser Eintrag gültig ist. Wenn das Gerät über mehr als eine statische IP-Adresse verfügt, kann das Port-Forwarding so auf bestimmte Verbindungen eingeschränkt werden.

- Eintrag aktiv

  Schaltet den Eintrag ein oder aus.

- Kommentar

  Kommentar zum definierten Eintrag (64 Zeichen).

6.7 Demilitarisierte Zone (DMZ)

Eine demilitarisierte Zone (DMZ) bietet die Möglichkeit, bestimmte Rechner in einem Netzwerk aus dem Internet erreichbar zu machen. Mit diesen Rechnern in der DMZ werden üblicherweise Internetdienste wie E-Mail o.ä angeboten. Der Rest des Netzwerks soll natürlich weiterhin für Angreifer aus dem Internet unerreichbar bleiben.

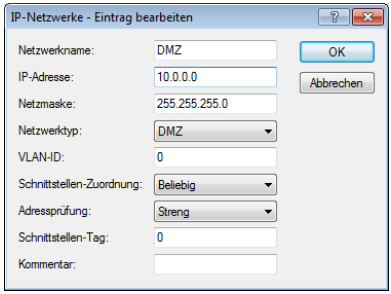
Um diesen Aufbau zu ermöglichen, muss der Datenverkehr zwischen den drei Zonen Internet, DMZ und LAN von einer Firewall geprüft werden. Diese Aufgaben der Firewall können durchaus in einem Gerät (Router) zusammengefasst werden. Dazu braucht der Router drei Interfaces, die getrennt voneinander durch die Firewall überwacht werden können:

- LAN-Interface
- WAN-Interface
- DMZ-Interface

Hinweis: In der Tabelle ist aufgelistet, welche Geräte diese Funktion unterstützen.

6.7.1 Zuordnung der Netzwerkzonen zur DMZ

Die Zuordnung der verschiedenen Netzwerk-Zonen (Adresskreise) zur DMZ, zum LAN und zum ARF wird bei den Adresseinstellungen vorgenommen. Dabei können je nach Verfügbarkeit auch WLAN-Interfaces ausgewählt werden.



LANconfig: TCP/IP / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / TCP-IP

6.7.2 Adressprüfung bei DMZ- und Intranet-Interfaces

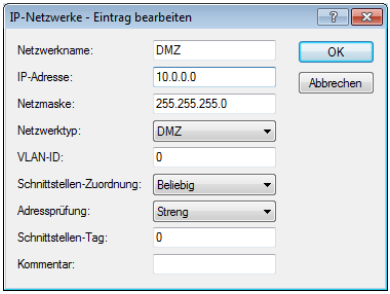
Zur besseren Abschirmung der DMZ (demilitarisierten Zone) und des Intranets gegen unerlaubte Zugriffe kann für die jeweiligen Interfaces eine zusätzliche Adressprüfung über das Intrusion Detection System (IDS) der Firewall aktiviert werden.

Die entsprechenden Schalter heißen 'DMZ-Check' bzw. 'Intranet-Check' und können die Werte 'loose' bzw. 'strict' annehmen:

- Wenn der Schalter auf 'loose' steht, dann wird jede Quelladresse akzeptiert, wenn das Gerät selbst angesprochen wird.
- Steht der Schalter jedoch auf 'strict', dann muss explizit eine Rückroute vorhanden sein, damit kein IDS-Alarm ausgelöst wird. Das ist also üblicherweise dann der Fall, wenn das Datenpaket eine Absenderadresse enthält, in die das entsprechende Interface auch selbst Daten routen kann. Absenderadressen aus anderen Netzen, in die das Interface nicht routen kann, oder Absenderadressen aus dem eigenen Adresskreis führen daher zu einem IDS-Alarm.

Hinweis: Der Default ist bei allen Geräten 'loose'.

Den Schalter zur Aktivierung von der DMZ- und Intranet-Adressprüfung finden Sie in LANconfig im Konfigurationsbereich 'TCP-IP' auf der Registerkarte 'Allgemein'.



LANconfig: TCP/IP / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / TCP-IP

6.7.3 Unmaskierter Internet-Zugang für Server in der DMZ

Das im vorangegangenen Abschnitt beschriebene inverse Maskieren erlaubt zwar, jeweils einen bestimmten Dienst zu exponieren (z. B. je ein Web-, Mail- und FTP-Server), hat aber z.T. weitere Einschränkungen:

- Der betreffende Dienst des 'exposed host' muss vom Maskierungsmodul unterstützt und verstanden werden. Zum Beispiel benutzen einige VoIP-Server nicht-standardisierte, proprietäre Ports für eine erweiterte Signalisierung. Dadurch können solche Server-Dienste nur an Verbindungen ohne Maskierung betrieben werden.
- Vom Sicherheitsstandpunkt muss beachtet werden, dass sich der 'exposed host' im lokalen Netz befindet. Falls der Rechner unter die Kontrolle eines Angreifers gebracht wird, so kann dieser Rechner als Ausgangsbasis für Angriffe gegen weitere Maschinen im lokalen Netz missbraucht werden.

Zwei lokale Netze - Betrieb von Servern in der DMZ

Hierfür ist ein Internetzugang mit mehreren statischen IP-Adressen notwendig. Bitte kontaktieren Sie Ihren ISP ggf. für ein entsprechendes Angebot.

Ein Beispiel: Sie erhalten die Internet IP-Netzadresse 123.45.67.0 mit der Netzmaske 255.255.255.248 vom Provider zugewiesen. Dann könnten Sie die IP-Adressen wie folgt verteilen:

öffentliche DMZ IP-Adresse	***Bedeutung/Verwendung***
123.45.67.0	Netzadresse
123.45.67.1	Intranet-Gateway
123.45.67.2	Beliebiges Gerät im lokalen Netzwerk, das unmaskierten Zugang ins Internet erhalten soll, beispielsweise ein Web-Server am DMZ-Port
123.45.67.7	Broadcast-Adresse

Alle Rechner und Geräte im Intranet haben keine öffentliche IP-Adresse und treten daher mit der IP-Adresse des Geräts (123.45.67.1) im Internet auf.

Trennung von Intranet und DMZ

Hinweis: Obwohl Intranet und DMZ vielleicht bereits schon auf Ethernet-Ebene durch dedizierte Interfaces voneinander getrennt sind, so muss in jedem Fall noch eine Firewall-Regel zur Trennung auf IP-Ebene eingerichtet werden!

Dabei soll der Server-Dienst vom Internet und aus dem Intranet heraus erreichbar sein, aber jeglicher IP-Traffic aus der DMZ Richtung Intranet soll unterbunden werden. Für das obige Beispiel ergäbe sich folgendes:

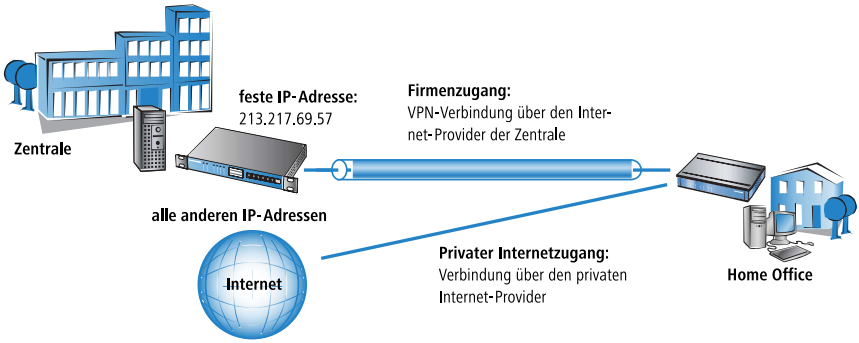
- Bei einer “Allow-All”-Strategie (default): Zugriff von “123.45.67.2” auf “Alle Stationen im lokalen Netz” verbieten
- Bei einer “Deny-All”-Strategie: Zugriff von “Alle Stationen im lokalen Netz” auf “123.45.67.2” erlauben

6.8 Multi-PPPoE

In den meisten Fällen wird auf einem DSL- oder ADSL-WAN-Interface immer nur eine Verbindung zu einer Zeit aufgebaut sein. Es gibt aber durchaus sinnvolle Anwendungen, in denen mehrere parallele Verbindungen auf dem WAN-Interface benötigt werden. Geräte mit DSL- oder ADSL-Interface können bis zu acht verschiedene Kanäle ins WAN parallel auf dem gleichen physikalischen Interface aufbauen.

6.8.1 Anwendungsbeispiel: Home-Office mit privatem Internetzugang

Eine mögliche Anwendung ist z. B. das Home-Office eines Außendienst-Mitarbeiters, der über eine VPN-Verbindung einen Zugang zum Netzwerk der Zentrale erhalten soll. Das Unternehmen zahlt dabei die Kosten für die VPN-Verbindung, der Mitarbeiter im Home-Office zahlt seinen privaten Internet-Datenverkehr selbst.



Um die beiden Datenverbindungen exakt trennen zu können, werden zwei Internetverbindungen für die jeweiligen Provider eingerichtet. Die Default-Route wird in der IP-Routing-Tabelle dann dem privaten Provider zugeordnet, das Netzwerk der Zentrale über die VPN-Verbindung wird über den Provider der Zentrale geroutet.

6.8.2 Konfiguration

Zur Konfiguration eines solchen Szenarios sind im Home-Office-Router die folgenden Schritte notwendig:

- Konfiguration des privaten Internetzugangs, z. B. über den Assistenten von LANconfig oder WEBconfig
- Konfiguration des Internetzugangs, der über die Zentrale abgerechnet wird
- Auswahl des privaten Providers für die Default-Route in der IP-Routing-Tabelle (z. B. manuell in LANconfig oder mit dem Assistenten zur Auswahl des Internetproviders unter WEBconfig)
- Konfiguration der VPN-Verbindung zum Netzwerk der Zentrale
- Zuweisung der VPN-Verbindung zum Provider der Zentrale:

  Damit der Datenverkehr zur Zentrale über den richtigen Internetprovider geroutet wird, muss in der IP-Routing-Tabelle noch ein neuer Eintrag angelegt werden. Darin wird das VPN-Gateway der Zentrale mit seiner festen IP-Adresse und der passenden Netzmaske eingetragen und auf die Gegenstelle für den Internetprovider der Zentrale geleitet.

Hinweis: Wichtig ist, dass die Route zum Internetprovider der Zentrale maskiert wird, denn sonst würde das Gerät nicht die WAN-Adresse, sondern seine LAN-Adresse in die VPN-Pakete einsetzen und die Verbindung käme niemals zustande.

Weitere Informationen zu diesen Konfigurationsschritten finden Sie an den entsprechenden Stellen in der Dokumentation zum Ihrem Gerät.

Hinweis: Administrator-Rechte des Mitarbeiters im Home-Office: Damit der Mitarbeiter im Home-Office nicht versehentlich die Einstellungen für die Internet-Provider oder den VPN-Zugang verändert, sollten Sie ihm je nach Vereinbarung nur die WEBconfig-Funktionsrechte für die Assistenten „Internet-Zugang“ und „Auswahl von Internet-Providern“ zuweisen.

Hinweis: Sorgen Sie mit den entsprechenden Filterregeln im Bereich 'Firewall/QoS' dafür, dass der Internetverkehr nicht versehentlich über das Netzwerk der Zentrale läuft.

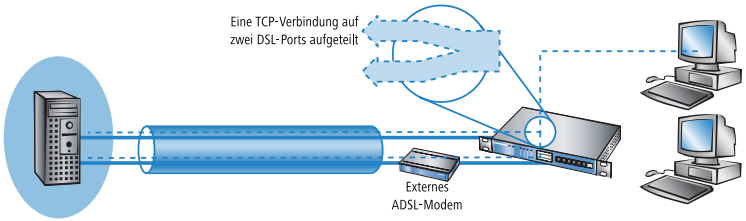
6.9 Load-Balancing

Trotz immer weiter steigender Bandbreite auf DSL-Zugängen stellen diese immer noch das Nadelöhr in der Kommunikation dar. In manchen Fällen ist es durchaus sinnvoll, mehrere DSL-Zugänge zu bündeln. Hierzu gibt es mehrere Möglichkeiten, die zum Teil vom Internet-Provider aktiv unterstützt werden müssen:

- DSL-Kanalbündelung (Multilink-PPPoE – MLPPPoE)

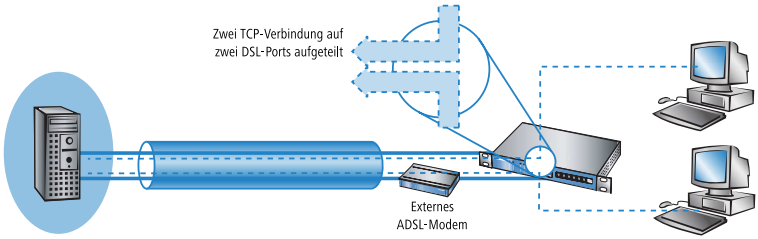
  Bei der direkten Bündelung ist der Anwender auf das Angebot des Carriers angewiesen, der dieses Verfahren unterstützen muss. Dem Anwender steht dabei die Summe der Bandbreiten aller gebündelter Kanäle zur Verfügung. Multilink-PPPoE kann nur zum Bündeln von PPP-Verbindungen eingesetzt werden.

Hinweis: Diese Variante der Kanalbündelung stellt als Summe ein Vielfaches der kleinsten der gebündelten Kanäle zur Verfügung. Sie ist daher besonders effizient, wenn Kanäle mit gleichen Bandbreiten verbunden werden. Bei der direkten Bündelung unterschiedlicher Bandbreiten geht für die Kanäle mit hohen Datenraten effektive Bandbreite verloren.



- Load-Balancing

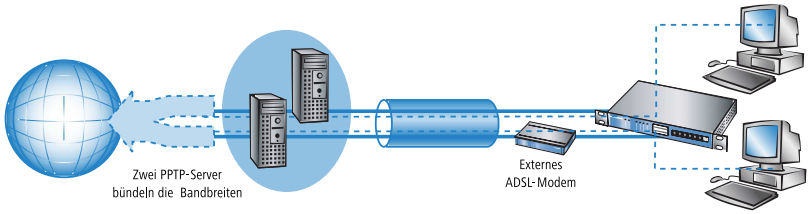
  Beim Load-Balancing werden TCP-Verbindungen dynamisch auf voneinander unabhängigen DSL-Verbindungen verteilt. Dem Anwender steht damit zwar auch die Summen-Bandbreite der gebündelten Kanäle zur Verfügung, dennoch ist jede einzelne TCP-Verbindung auf die Bandbreite des zugewiesenen DSL-Anschlusses beschränkt.



Hinweis: Im Gegensatz zur direkten Kanalbündelung steht beim Load-Balancing tatsächlich die Summe aller gebündelten Bandbreiten zur Verfügung. Diese Variante eignet sich daher besonders gut zum Verbinden unterschiedlicher Bandbreiten.

- Indirekte Bündelung für LAN-LAN-Kopplungen

  Bei der indirekten Bündelung wird auf zwei oder mehr voneinander unabhängigen DSL-Verbindungen je eine PPTP-Verbindung aufgebaut. Diese PPTP-Verbindungen werden dann gebündelt. Damit ist dann zumindest für LAN-LAN-Kopplungen durch das Internet hindurch eine echte Kanalbündelung möglich, auch wenn der Internetprovider selbst keine Kanalbündelung anbietet.



6.9.1 Dynamisches Load-Balancing

Wenn der Internet-Provider eine direkte Bündelung nicht unterstützt, werden mehrere normale DSL-Zugänge über einen Load-Balancer gekoppelt. Hierzu werden zuerst die DSL-Zugänge für die benötigten DSL-Ports eingerichtet. Danach werden diese über eine Load-Balancing-Tabelle miteinander gekoppelt. Diese Liste ordnet einer virtuellen Balancing-Verbindung (das ist die Verbindung, die in der Routing-Tabelle eingetragen wird) die weiteren realen DSL-Verbindungen (Bündel-Verbindungen) zu. Einer Balancing-Verbindung können dabei je nach Anzahl der verfügbaren DSL-Ports mehrere Bündel-Verbindungen zugeordnet werden.

Hinweis: Die Balancing-Verbindung wird als „virtuelle“ Verbindung angelegt. Für diese Verbindung werden also keine Zugangsdaten etc. eingetragen. Dieser Eintrag dient nur als „Verteiler“, um einem Eintrag in der Routing-Tabelle mit Hilfe der Load-Balancing-Tabelle mehrere „reale“ Bündel-Verbindungen zuweisen zu können.

Hinweis: Bei der DSL-Bündelung handelt es sich um eine statische Bündelung. Die evtl. zusätzlichen Kanäle werden also **nicht** nur nach Bedarf des übertragenen Datenvolumens auf- und wieder abgebaut.

Die Entscheidung über das Routing der Datenpakete kann beim Load-Balancing nicht mehr allein anhand der IP-Adressen getroffen werden, da die einzelnen gebündelten DSL-Verbindungen unterschiedliche IP-Adressen haben. Beim Load-Balancing werden daher zusätzlich die Informationen aus der Verbindungsliste der Firewall berücksichtigt. In dieser Liste wird für jede TCP-Verbindung ein Eintrag angelegt, der für das Load-Balancing zusätzlich die Information über den verwendeten DSL-Port bereitstellt.

Verbindungsaufbau

Bei der Anforderung für eine Datenübertragung zu einer Balancing-Gegenstelle wird zunächst die **erste** Bündel-Verbindung aus der Load-Balancing-Tabelle aufgebaut. Der weitere Verlauf hängt vom Erfolg der Verbindungsaufbaus ab:

- Wird die Verbindung erfolgreich aufgebaut, werden zunächst alle anstehenden TCP-Verbindungen diesem Kanal zugewiesen. Anschließend werden sukzessive alle konfigurierten Bündel-Verbindungen aufgebaut. Sobald mindestens zwei Bündel-Verbindungen aktiv sind, werden neue TCP-Verbindungen unter den aktiven Bündel-Verbindungen verteilt.
- Scheitert jedoch der Aufbau der ersten Bündel-Verbindung, so wird nacheinander der Aufbau der weiteren Bündel-Verbindungen versucht. Sobald eine der Bündel-Verbindungen aufgebaut werden konnte, werden alle zu diesem Zeitpunkt anstehenden TCP-Verbindungen auf diesen Kanal umgeleitet.

Verteilung der Datenlast

Für die Verteilung der Datenlast auf die verfügbaren Kanäle stehen prinzipiell zwei Varianten zur Auswahl:

- Wenn die Bandbreite des jeweiligen Kanals bekannt ist, dann werden die Verbindungen dem Kanal zugewiesen, der die geringste (prozentuale) Auslastung hat.

- Wenn die Bandbreite unbekannt ist, dann wird unterschieden, ob es sich bei der Verbindung um eine TCP-Verbindung handelt oder ob das Gerät eine VPN- oder PPTP-Verbindung aufbauen will.
  - Wenn eine TCP-Verbindung einen Kanal anfordert, dann wird derjenige mit der geringsten absoluten Last ausgewählt.
  - Wenn eine VPN- oder PPTP-Verbindung einen Kanal anfordert, dann werden die PPTP- und VPN-Verbindung gleichmäßig auf die verfügbaren Kanäle verteilt.

Hinweis: Für die sinnvolle Nutzung des Load-Balancing ist daher die Angabe der Bandbreite in der der Liste der WAN-Interfaces unter LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' unter der Schaltfläche **Interface-Einstellungen** erforderlich (Telnet: `/Setup/Schnittstellen/DSL`, WEBconfig: Expertenkonfiguration/ Setup / Schnittstellen / DSL).

Client-Binding

Der Einsatz von Load-Balancing führt bei Servern zu Problemen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden. Wählt der Load-Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen (Policy Based Routing). Damit ist jedoch der gesamte Datenverkehr zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt. Außerdem lassen sich so keine Backup-Verbindung aufbauen, falls die erste Verbindung gestört ist.

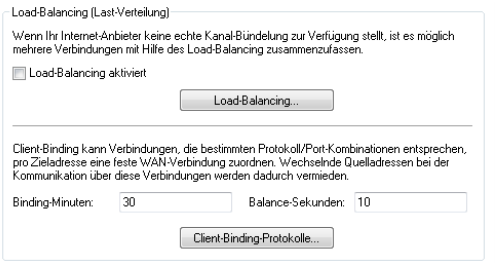
Das Client-Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions ebenfalls über diese Internetverbindung, was im Prinzip dem zuvor angesprochenen Policy Based Routing entspricht. Das erfolgt protokollabhän-

gig, d. h., es überträgt nur Daten des selben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Verbindung.

Um zu vermeiden, dass nun auch Daten über diese Internetverbindung fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Load-Balancing mit Client-Binding

In LANconfig konfigurieren Sie das Client-Binding unter **IP-Router** > **Routing** im Abschnitt **Load-Balancing (Lastverteilung)**.



Binding-Minuten

Definieren Sie hier die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

Balance-Sekunden

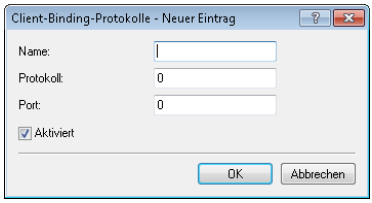
Um zu vermeiden, dass Daten über die Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit wei-

terhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

Das Client-Binding erfolgt protokollorientiert. Die entsprechenden Protokolle bestimmen Sie unter **Client-Binding-Protokolle**. Die Tabelle enthält bereits die Standard-Einträge

- HTTPS
- HTTP
- ANY



Name

Enthält eine aussagekräftige Bezeichnung dieses Eintrages.

Protokoll

Enthält die IP-Protokollnummer.

Hinweis: Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank* der IANA.

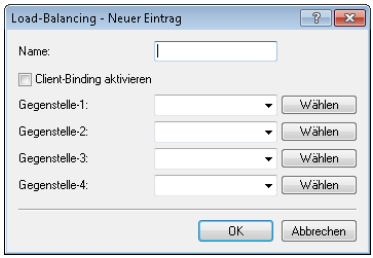
Port

Enthält den Port des IP-Protokolls.

Aktiviert

Aktiviert oder deaktiviert diesen Eintrag.

Das Client-Binding lässt sich unter **Load-Balancing** für den jeweiligen Eintrag aktivieren oder deaktivieren.



6.9.2 Statisches Load-Balancing

Neben der im vorhergehenden Abschnitt beschriebenen dynamischen Verbindungsauswahl sind Szenarien vorstellbar, in denen für eine bestimmte TCP-Verbindung immer die gleiche DSL-Verbindung benutzt werden soll. Hierbei sind zwei Fälle zu unterscheiden:

- Ein Server mit einer festen IP-Adresse ist nur über eine dedizierte Verbindung erreichbar. Hierfür reicht die Auswahl anhand der Ziel-IP-Adresse.
- Ein Server verwendet ein Protokoll, das neben einem Kontrollkanal weitere Kanäle zur Datenübertragung benötigt (z. B. FTP, H.323, PPTP). Dabei akzeptiert der Server den Aufbau der Datenkanäle nur von der gleichen IP-Adresse, von der auch der Kontrollkanal aufgebaut wurde.

Zielbasierte Kanalvorgabe

Für die Zielbasierte Kanalvorgabe genügt es, für den jeweiligen Server einen Eintrag in der Routing-Tabelle aufzunehmen, der als Ziel nicht die „virtuelle“ Balancing-Verbindung, sondern eine der Bündel-Verbindungen direkt verwendet.

Regelbasierte Kanalvorgabe (Policy-based Routing)

Um die Kanalauswahl aufgrund des Zielports oder der Quelladresse zu entscheiden, werden geeignete Einträge in der Firewall angelegt. Den Firewall-Einträgen wird dabei ein spezielles „Routing-Tag“ zugefügt, mit dem über die Routing-Tabelle die gewünschte Kanalauswahl gesteuert werden kann. Weitere Informationen finden Sie unter *Policy-based Routing* auf Seite 468.

6.9.3 Indirekte Bündelung für LAN-LAN-Kopplungen über PPTP

Die indirekte Bündelung erfolgt über gebündelte PPTP-Verbindungen, wodurch sich bei einer LAN-LAN-Kopplung die volle Bandbreite der gebündelten Kanäle nutzen lässt. Bei der Betrachtung der PPTP-Bündelung gibt es drei verschiedene Szenarien:

- Der Client bündelt DSL-Kanäle, der Server steht hinter einen Anschluss mit genügender Bandbreite
- Der Client steht hinter einem breitbandigen Anschluss, doch der Server muss bündeln
- Server und Client bündeln DSL-Kanäle

Zur Konfiguration werden lediglich in der Balancing-Tabelle die weiteren PPTP-Adressen aufgeführt.

6.9.4 Konfiguration des Load Balancing

Hinweis: Für die folgenden Konfigurationen gehen wir davon aus, dass die entsprechenden Gegenstellen mit allen Zugangsdaten bereits eingerichtet sind.

Direkte Kanalbündelung über PPPoE

Zur Konfiguration der direkten Kanalbündelung über PPPoE gehen Sie folgendermaßen vor:

1. Ordnen Sie den Ethernet-Ports die gewünschten DSL-Ports zu, in LANconfig über **Interfaces** / **LAN** / **Ethernet-Ports**.

   Telnet: `/Setup/Schnittstellen/Ethernet-Ports`

   WEBconfig: **Expertenkonfiguration** / **Setup** / **Schnittstellen** / **Ethernet-Ports**

2. Aktivieren Sie die zusätzlichen DSL-Interfaces in LANconfig über **Interfaces** / **WAN** / **Interface-Einstellungen**. Geben Sie dabei die Datenraten für Up- und Downstream an.

   Telnet: `/Setup/Schnittstellen/DSL`

WEBconfig: **Expertenkonfiguration** / **Setup** / **Schnittstellen** / **DSL**

3. Tragen Sie für die gewünschte Gegenstelle die zu verwendenden DSL-Ports in LANconfig über **Kommunikation** / **Gegenstellen** / **Gegenstellen (DSL)** ein.

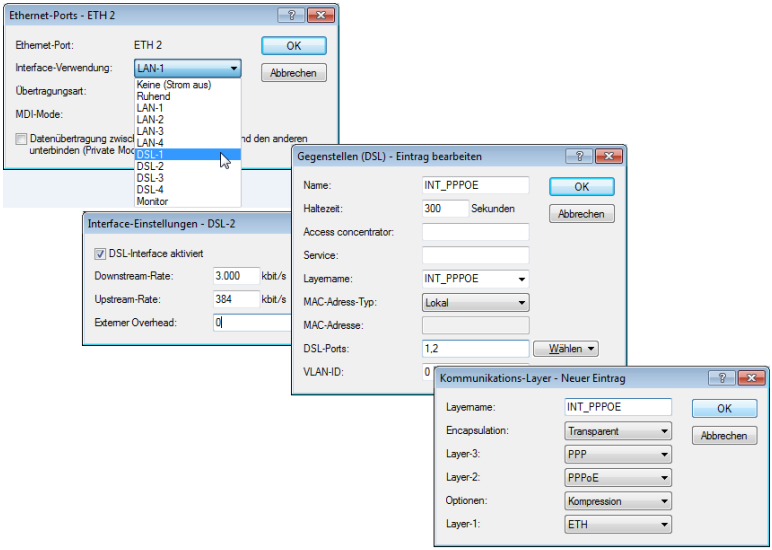
   Telnet: `/Setup/WAN/DSL-Breitband-Gegenstellen`

   WEBconfig: **Expertenkonfiguration** / **Setup** / **WAN** / **DSL-Breitband-Gegenstellen**

4. Aktivieren Sie für den verwendeten Layer die Kanalbündelung in LANconfig über **Kommunikation** / **Allgemein** / **Kommunikations-Layer**.

   Telnet: `/Setup/WAN/Layer`

   WEBconfig: **Expertenkonfiguration** / **Setup** / **WAN** / **Layer**



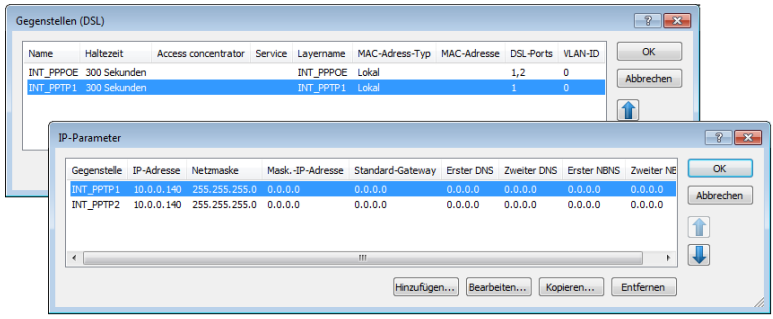
Direkte Kanalbündelung über PPTP

Zur Konfiguration der direkten Kanalbündelung über PPPoE gehen Sie folgendermaßen vor:

1. Konfigurieren Sie mehrere getrennte PPTP-Verbindungen (z. B. über den Assistenten von LANconfig). , die jeweils einen anderen DSL-Port nutzen. Die Verbindungen werden mit den gleichen Werten für die IP-Parameter eingetragen, die in LANconfig unter **Kommunikation** / **Protokolle** / **IP-Parameter** einzusehen sind.

   Telnet: `/Setup/WAN/IP-Liste`

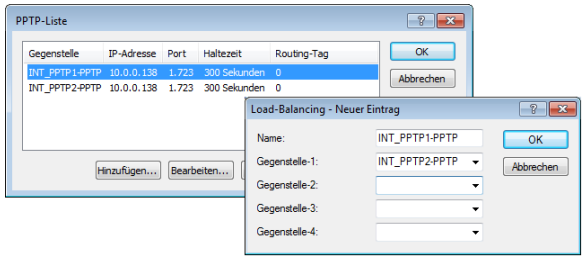
   WEBconfig: **Expertenkonfiguration** / **Setup** / **WAN** / **IP-Liste**



2. Eine Bündelung erfolgt dann, wenn für die physikalische Verbindung der PPTP-Gegenstelle in der Load-Balancing-Liste zusätzliche Gegenstellen definiert sind. Die PPTP-Verbindung fordert dann im Bündelfall die nächste physikalische Verbindung an und baut sie dorthin auf. Tragen Sie die Bündelverbindungen in LANconfig über **IP-Router** / **Routing** / **Load-Balancing** ein.

   Telnet: `/Setup/IP-Router/Load-Balancer`

   WEBconfig: **Expertenkonfiguration** / **Setup** / **IP-Router** / **Load-Balancer**



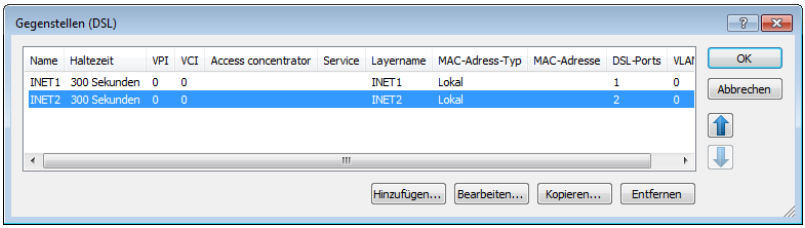
Dynamisches Load-Balancing mit mehreren DSL-Zugängen

Für das dynamische Load-Balancing werden zunächst die Internetzugänge z. B. mit den Assistenten von LANconfig eingerichtet, z. B. 'INET1' und 'INET2'.

1. Um den Internet-Traffic auf verschiedene DSL-Interfaces zu verteilen, werden den einzelnen Gegenstellen in LANconfig unter **Kommunikation** / **Gegenstellen** / **Gegenstellen (DSL)** unterschiedliche DSL-Ports zugewiesen.

   Telnet: `/Setup/WAN/DSL-Breitband-Gegenstellen`

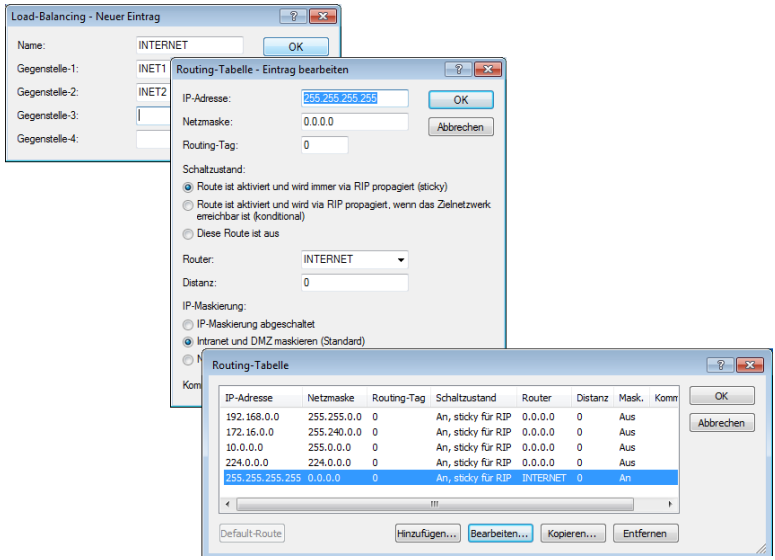
   WEBconfig: **Expertenkonfiguration** / **Setup** / **WAN** / **DSL-Breitband-Gegenstellen**



2. Die beiden DSL-Gegenstellen werden dann in der Load-Balancing-Liste in LANconfig über **IP-Router** / **Routing** / **Load-Balancing** einer neuen, virtuellen Gegenstelle 'INTERNET' zugeordnet.

   Telnet: `/Setup/IP-Router/Load-Balancer`

   WEBconfig: **Expertenkonfiguration** / **Setup** / **IP-Router** / **Load-Balancer**



3. Die virtuelle Gegenstelle wird in der Routing-Tabelle in LANconfig über **IP-Router** / **Routing** / **IP-Routing-Tabelle** als Router für die Default-Route eingetragen.

Telnet: `/Setup/IP-Router/IP-Routing-Tabelle`

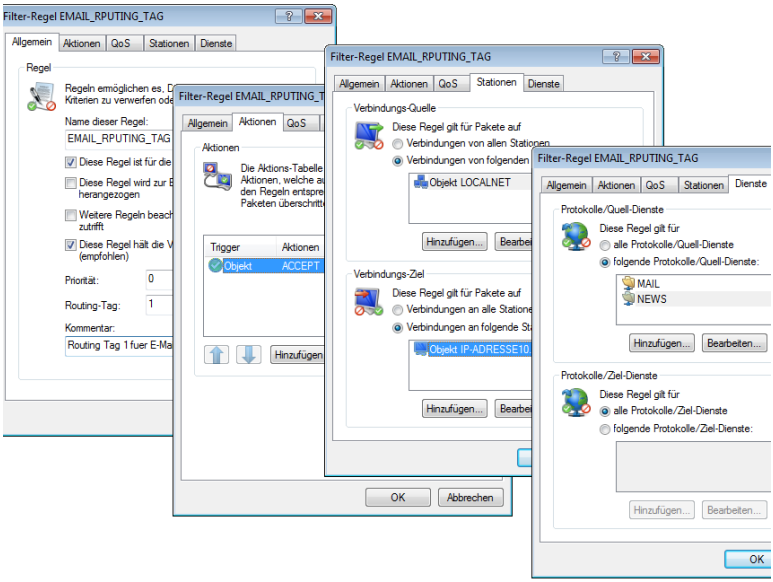
WEBconfig: **Expertenkonfiguration** / **Setup** / **IP-Router** / **IP-Routing-Tabelle**

Hinweis: Für den Zugang zum Internet wird nun die virtuelle Gegenstelle 'INTERNET' verwendet. Wenn Daten über diese Verbindung geroutet werden, werden anhand der Load-Balancing-Tabelle die „echten“ DSL-Verbindungen aufgebaut und die Daten entsprechend über die gewählten DSL-Ports übertragen.

4. Um den Datenverkehr je nach Anwendung gezielter auf die DSL-Ports zu verteilen, können die Routing-Tags genutzt werden. Soll z. B. der ausgehende E-Mail-Traffic über ein bestimmtes DSL-Interface mit einer bestimmten IP-Adresse geroutet werden, wird in der Firewall unter LANconfig über **Firewall/QoS** / **Regeln** eine entsprechende Regel angelegt, die den Datenverkehr über E-Mail-Dienste von allen lokalen Stationen zum Mail-Server überträgt und dabei das Routing-Tag '1' setzt.

Telnet: `/Setup/IP-Router/Firewall/Regel-Tabelle`

WEBconfig: **Expertenkonfiguration** / **Setup** / **IP-Router** / **Firewall** / **Regel-Tabelle**



6.10 N:N-Mapping

Das Verfahren der Network Address Translation (NAT) kann für mehrere Dinge benutzt werden:

- um die immer knapper werdenden IPv4-Adressen besser zu nutzen
- um Netze mit gleichen (privaten) Adressbereichen miteinander zu koppeln
- um eindeutige Adressen zum Netzwerkmanagement zu erzeugen

Für die erste Anwendung kommt das sogenannte N:1-NAT, auch als IP-Masquerading (*IP-Masquerading* auf Seite 505) bekannt, zum Einsatz. Hierbei werden alle Adressen (“N”) des lokalen Netzes auf eine einzige (“1”) öffentliche Adresse gemappt. Die eindeutige Zuordnung der Datenströme zu den jeweiligen internen Rechnern erfolgt in der Regel über die Ports der Protokolle TCP

und UDP, weshalb man hier auch von NAT/PAT (Network Address Translation/Port Address Translation) spricht.

Durch die dynamische Umsetzung der Ports sind beim N:1-Masquerading nur Verbindungen möglich, die vom internen Netz aus aufgebaut werden. Ausnahme: eine interne IP-Adresse wird statisch einem bestimmten Port zugeordnet, z. B. um einen Server im LAN von außen zugänglich zu machen. Dieses Verfahren nennt man “Inverses Masquerading” (*Inverses Masquerading* auf Seite 508).

Zur Kopplung von Netzwerken mit gleichen Adressräumen wird ein N:N-Mapping verwendet. Dieses setzt mehrere Adressen (“N”) des lokalen Netzes eineindeutig auf mehrere (“N”) Adressen eines beliebigen anderen Netzes um. Durch diese Umsetzung wird der Adresskonflikt verhindert.

Die Regeln für diese Adressumsetzung werden in einer statischen Tabelle im Gerät definiert. Dabei werden für einzelne Stationen im LAN, Teilnetze oder das gesamte LAN neue IP-Adressen festgelegt, unter denen die Stationen dann mit dem anderen Netzen in Kontakt treten können.

Bei einigen Protokollen (FTP, H.323) werden während der Protokollverhandlung Parameter ausgetauscht, die Einfluss auf die Adressumsetzung beim N:N-Mapping haben können. Die entsprechenden Verbindungsinformationen werden bei diesen Protokollen daher mit den Funktionen der Firewall in einer dynamischen Tabelle festgehalten und zusätzlich zu den Einträgen aus der statischen Tabelle für die korrekte Funktion der Adressumsetzung verwendet.

Hinweis: Die Adressumsetzung erfolgt “Outbound”, d.h. bei abgehenden Datenpaketen wird die Quelladresse umgesetzt, und bei eingehenden Datenpaketen wird die Zieladresse umgesetzt, sofern die Adressen im definierten Umsetzungsbereich liegen. Ein “Inbound”-Adressmapping, bei dem bei eingehenden Datenpaketen die Quelladresse (anstelle der Zieladresse) umgesetzt wird, muss stattdessen durch eine entsprechende “Outbound”-Adressumsetzung auf der Gegenseite eingerichtet werden.

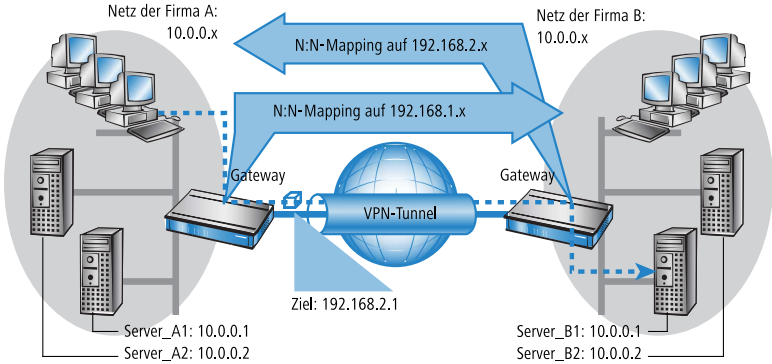
6.10.1 Anwendungsbeispiele

Im folgenden werden die folgenden typischen Anwendungen vorgestellt:

- Kopplung von privaten Netzen, die den gleichen Adressraum belegen
- Zentrale Fernüberwachung durch Dienstleister

Netzwerkkopplung

Ein häufig anzutreffendes Szenario stellt die Kopplung zweier Firmennetze dar, die intern den gleichen Adressraum (z. B. 10.0.0.x) belegen. Dies erfolgt meist dann, wenn eine Firma Zugriff auf einen (oder mehrere) Server der anderen erhalten soll:

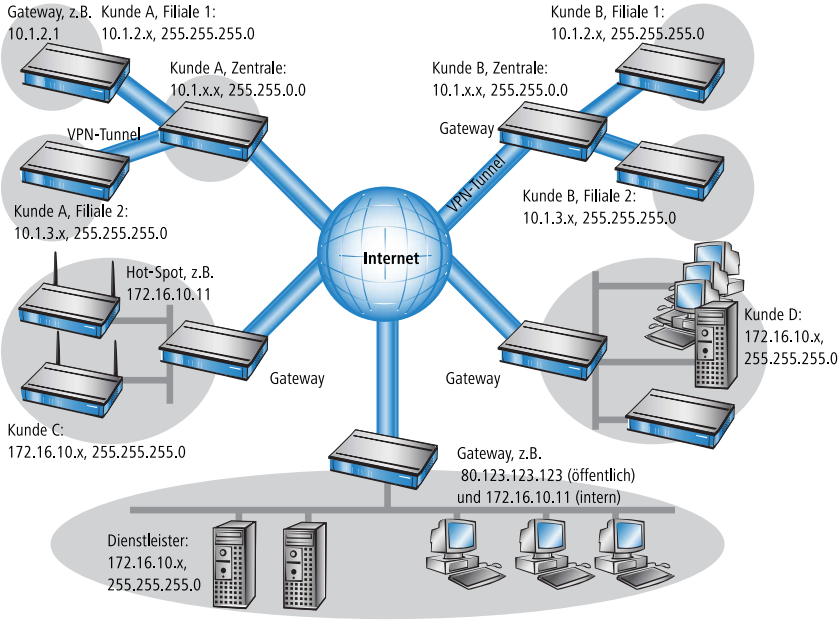


In diesem Beispiel stehen in den Netzen der Firmen A und B Server, die über einen VPN-Tunnel auf das jeweils andere Netz zugreifen wollen. Allen Stationen im LAN soll dabei der Zugang zu den Servern im remoten Netz erlaubt werden. Da beide Netze den gleichen Adresskreis nutzen, ist in dieser Konfiguration zunächst kein Zugriff in das andere Netz möglich. Wenn eine Station aus dem Netz der Firma A auf den Server 1 der Firma B zugreifen will, wird der Adressat (mit einer Adresse aus dem 10.0.0.x-Netz) im eigenen lokalen Netz gesucht, die Anfrage gelangt gar nicht bis zum Gateway.

Mit dem N:N-Mapping werden alle Adressen des LANs für die Kopplung mit dem anderen Netz in einen neuen Adresskreis übersetzt. Das Netz der Firma A wird z. B. auf die 192.168.1.x umgesetzt, das Netz der Firma B auf 192.168.2.x. Unter diesen neuen Adressen sind die beiden LANs nun für das jeweils andere Netz erreichbar. Die Station aus dem Netz der Firma A spricht den Server 1 der Firma B nun unter der Adresse 192.168.2.1 an. Der Adressat liegt nun nicht mehr im eigenen Netz, die Anfrage wird an das Gateway weitergeleitet und das Routing in das andere Netz funktioniert wie gewünscht.

Fernwartung und -überwachung von Netzwerken

Der Fernwartung und -überwachung von Netzwerken kommt durch die Möglichkeiten von VPN immer größere Bedeutung zu. Mit der Nutzung der fast flächendeckend vorhandenen Breitband-Internetanschlüsse kann sich der Administrator von solchen Management-Szenarien unabhängig machen von den unterschiedlichen Datenübertragungstechnologien oder teuren Standleitungen.



In diesem Beispiel überwacht ein Dienstleister von einer Zentrale aus die Netzwerke verschiedener Kunden. Zu diesem Zweck sollen die SNMP-fähigen Geräte die entsprechenden Traps über wichtige Ereignisse automatisch an den SNMP-Trap-Empfänger (z. B. LANmonitor) im Netz des Dienstleisters senden. Der Administrator im LAN des Dienstleisters hat damit jederzeit einen aktuellen Überblick über den Zustand der Geräte.

Die einzelnen Netze können dabei sehr unterschiedlich aufgebaut sein: Die Kunden A und B binden ihre Filialen mit eigenen Netzwerken über VPN-Ver-

bindungen in ihr LAN ein, Kunde C betreibt ein Netz mit mehreren öffentlichen WLAN-Basisstationen als Hot-Spots und Kunde D hat in seinem LAN u.a. einen weiteren Router für ISDN-Einwahlzugänge.

Hinweis: Die Netze der Kunden A und B in der jeweiligen Zentrale und den angeschlossenen Filialen nutzen verschiedene Adresskreise. Zwischen diesen Netzen ist also eine normale Netzwerkkopplung über VPN möglich.

Um den Aufwand zu vermeiden, zu jedem einzelnen Subnetz der Kunden A und B einen eigenen VPN-Tunnel aufzubauen, stellt der Dienstleister nur eine VPN-Verbindung zur Zentrale her und nutzt für die Kommunikation mit den Filialen die ohnehin vorhandenen VPN-Leitungen zwischen der Zentrale und den Filialen.

Die Traps aus den Netzen melden dem Dienstleister, ob z. B. ein VPN-Tunnel auf- oder abgebaut wurde, ob ein User sich dreimal mit dem falschen Passwort einloggen wollte, ob sich ein User an einem Hot-Spot angemeldet hat oder ob irgendwo ein LAN-Kabel aus einem Switch gezogen wurde.

Hinweis: Eine komplette Liste aller SNMP-Traps, die vom Gerät unterstützt werden, finden Sie im Anhang dieses Referenz-Handbuchs.

Das Routing dieser unterschiedlichen Netzwerke stößt dabei sehr schnell an seine Grenzen, wenn zwei oder mehrere Kunden gleiche Adresskreise verwenden. Wenn zusätzlich noch einige Kunden den gleichen Adressbereich nutzen wie der Dienstleister selbst, kommen weitere Adresskonflikte hinzu. In diesem Beispiel hat z. B. einer der Hot-Spots von Kunde C die gleiche Adresse wie das Gateway des Dienstleisters.

Für die Lösung dieser Adresskonflikte gibt es zwei verschiedene Varianten:

- Bei der dezentralen Variante werden den zu überwachenden Geräten per 1:1-Mapping jeweils alternative IP-Adressen für die Kommunikation mit dem SNMP-Empfänger zugewiesen. Diese Adresse ist in der Fachsprache auch als “Loopback-Adresse” bekannt, die Methode wird entsprechend als “Loopback-Verfahren” bezeichnet.

  Hinweis: Die Loopback-Adressen gelten jeweils nur für die Kommunikation mit bestimmten Gegenstellen auf den zugehörigen Verbindungen. Ein Gerät ist damit nicht generell unter dieser IP-Adresse erreichbar.

- Eleganter ist die Lösung des zentralen Mappings: statt jedes einzelne Gateway in den Filialnetzen zu konfigurieren, stellt der Administrator hier die Adressumsetzung im Gateway der Zentrale ein. Dabei werden automatisch auch alle “hinter” der Zentrale liegenden Subnetze mit den erforderlichen neuen IP-Adressen versorgt.

In diesem Beispiel wählt der Administrator des Dienstleisters für das Netz des Kunden B die zentrale Adressumsetzung auf 10.2.x.x, damit die beiden Netze mit eigentlich gleichen Adresskreisen für das Gateway des Dienstleisters wie zwei verschiedene Netz erscheinen.

Für die Kunden C und D wählt er die Adresskreise 192.168.2.x und 192.168.3.x, damit diese Netze sich in ihren Adressen von dem eigenen Netz des Dienstleisters unterscheiden.

Damit das Gateway des Dienstleisters die Netze der Kunden C und D ansprechen kann, richtet er auch für das eigene Netz eine Adressumsetzung auf 192.168.1.x ein.

6.10.2 Konfiguration

Einrichten der Adressumsetzung

Die Konfiguration des N:N-Mappings gelingt mit recht wenigen Informationen. Da ein LAN durchaus mit mehreren anderen Netzen per N:N gekoppelt werden kann, können für einen Quell-IP-Bereich bei verschiedenen Zielen auch unterschiedliche Adressumsetzungen gelten. In der NAT-Tabelle können maximal 64 Einträge vorgenommen werden, die folgende Informationen beinhalten:

- **Index**: Eindeutiger Index des Eintrags.
- **Quell-Adresse**: IP-Adresse des Rechners oder Netzes, dass eine alternative IP-Adresse erhalten soll.
- **Quell-Maske**: Netzmaske des Quell-Bereiches.
- **Gegenstelle**: Name der Gegenstelle, über die das entfernte Netzwerk erreicht werden kann.
- **Neue Netz-Adresse**: IP-Adresse oder -Adressbereich, der für die Umsetzung verwendet werden soll.

Für die neue Netzadresse wird jeweils die gleiche Netzmaske verwendet, die auch schon die Quell-Adresse verwendet. Für die Zuordnung von Quell- und Mapping-Adresse gelten folgende Hinweise:

- Bei der Umsetzung von einzelnen Adressen können Quelle und Mapping beliebig zugeordnet werden. So kann z. B. dem Server im LAN mit der IP-Adresse 10.1.1.99 die Mapping-Adresse 192.168.1.88 zugewiesen werden.
- Bei der Umsetzung von ganzen Adressbereichen wird der rechnerbezogene Teil der IP-Adresse direkt übernommen und nur an den netzbezogenen Teil der Mapping-Adresse angehängt. Bei einer Zuweisung von 10.0.0.0/255.255.255.0 nach 192.168.1.0 wird also dem Server im LAN mit der IP-Adresse 10.1.1.99 zwangsweise die Mapping-Adresse 192.168.1.99 zugewiesen.

Hinweis: Der Adressbereich für die Umsetzung muss mindestens so groß sein wie der Quell-Adressbereich.

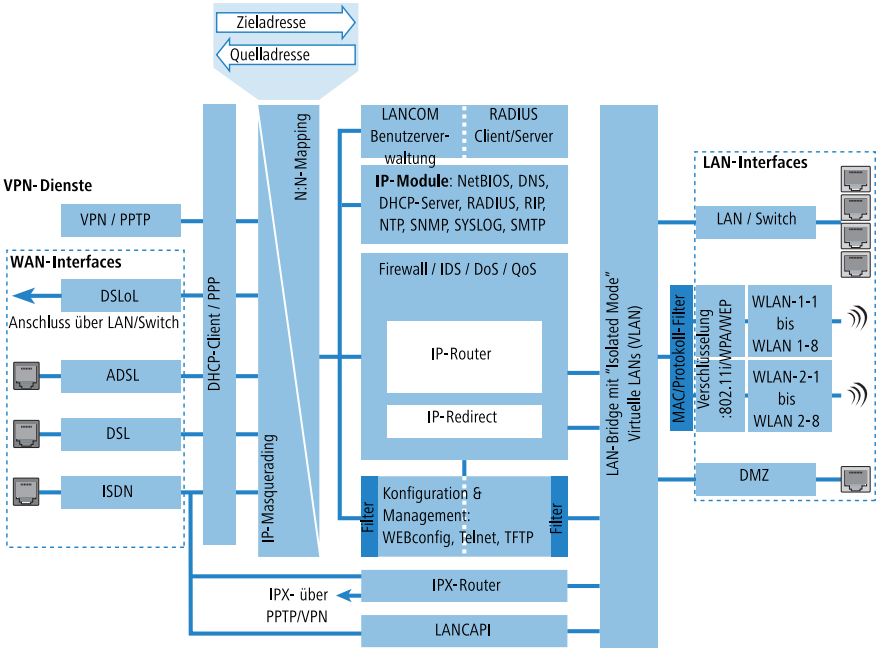
Hinweis: Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist!

Zusätzliche Konfigurationshinweise

Mit dem Einrichten der Adressumleitung in der NAT-Tabelle werden die Netze und Rechner zunächst nur unter einer anderen Adresse im übergeordneten Netzverbund sichtbar. Für das einwandfreie Routing der Daten zwischen den Netzen sind aber noch einige weitere Einstellungen notwendig:

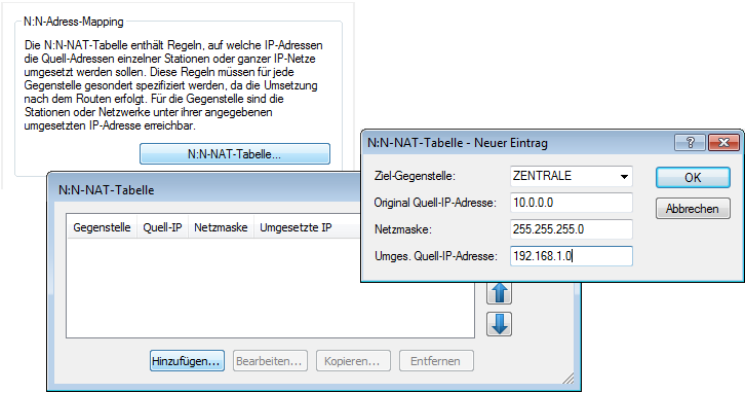
- Einträge in den Routing-Tabellen, damit die Pakete mit den neuen Adressen auch den Weg zum Ziel finden.
- DNS-Forwarding-Einträge, damit die Anfragen nach bestimmten Geräten in den jeweils anderen Netzen in die gemappten IP-Adressen aufgelöst werden können.
- Die Regeln der Firewalls in den Gateways müssen so angepasst werden, dass ggf. auch der Verbindungsaufbau von außen von den zulässigen Stationen bzw. Netzwerken her erlaubt ist.
- VPN-Regeln für Loopback-Adressen, damit die neu zugewiesenen IP-Adressen auch durch die entsprechenden VPN-Tunnel übertragen werden können.

Hinweis: Die Umsetzung der IP-Adressen findet im Gerät zwischen Firewall und IP-Router auf der einen Seite und dem VPN-Modul auf der anderen Seite statt. Alle Regeln, die sich auf das eigene lokale Netz beziehen, verwenden daher die “ungemappten”, originalen Adressen. Die Einträge für das entfernte Netz nutzen also die “gemappten” Adressen der Gegenseite, die auf der VPN-Strecke gültig sind.



Konfiguration mit den verschiedenen Tools

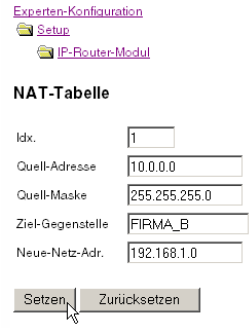
Unter LANconfig stellen Sie die Adressumsetzung im Konfigurationsbereich ’IP-Router’ auf der Registerkarte 'N:N-Mapping' ein:



Unter WEBconfig und Telnet finden Sie die NAT-Tabelle zur Konfiguration des N:N-Mappings an folgenden Stellen des Menübaums:

Konfigurationstool	***Aufruf***
WEBconfig	Expertenkonfiguration / Setup / IP-Router / NAT-Tabelle
Terminal/Telnet	Setup / IP-Router / NAT-Tabelle

Die NAT-Tabelle präsentiert sich unter WEBconfig beim Anlegen eines neuen Eintrags folgendermaßen:



6.11 Verbindungsaufbau mit PPP

Geräte von Hirschmann unterstützen auch das Point-to-Point Protocol (PPP). PPP ist ein Sammelbegriff für eine ganze Reihe von WAN-Protokollen, die das Zusammenspiel von Routern verschiedener Hersteller erleichtern, denn dieses Protokoll wird von fast allen Herstellern unterstützt.

Und gerade weil das PPP nicht einer bestimmten Betriebsart der Router zugeordnet werden kann und natürlich auch wegen der großen und in Zukunft noch weiter steigenden Bedeutung dieser Protokoll-Familie, möchten wir Ihnen die Funktionen der Geräte im Zusammenhang mit dem PPP hier in einem eigenen Abschnitt vorstellen.

6.11.1 Das Protokoll

Was ist PPP?

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle (auch ISDN, DSL u.ä.) entwickelt und hat sich als Standard für Verbindungen zwischen Routern behauptet. Es realisiert folgende Funktionen:

- Passwortschutz nach PAP, CHAP oder MS-CHAP
- Rückruf-Funktionen
- Aushandlung der über die aufgebaute Verbindung zu benutzenden Netzwerkprotokolle (z. B. IP). Dazu gehören auch für diese Protokolle notwendige Parameter wie z. B. IP-Adressen. Diese Verhandlung läuft über das Protokoll IPCP (IP Control Protocol) ab.
- Aushandeln von Verbindungsparametern wie z. B. der MTU (Maximum Transmission Unit, *Manuelle Definition der MTU* auf Seite 550).
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren ISDN- oder DSL-Kanälen (Multilink-PPP bzw. Multilink-PPPoE)

Für Router-Verbindungen ist PPP der Standard für die Kommunikation zwischen Geräten bzw. der WAN-Verbindungssoftware unterschiedlicher Hersteller. Um eine erfolgreiche Datenübertragung nach Möglichkeit sicherzustellen, erfolgt die Verhandlung der Verbindungsparameter und eine Einigung auf

einen gemeinsamen Nenner über standardisierte Steuerungsprotokolle (z. B. LCP, IPCP, CCP), die im PPP enthalten sind.

Wozu wird PPP verwendet?

Das Point-to-Point Protocol wird bei folgenden Anwendungen sinnvoll eingesetzt:

- aus Kompatibilitätsgründen z. B. bei Kommunikation mit Fremdroutern
- Remote Access von entfernten Arbeitsplatzrechnern mit ISDN-Adaptern
- Internet-Access (mit der Übermittlung von Adressen)

Das im Gerät implementierte PPP kann synchron oder asynchron sowohl über eine transparente HDLC-Verbindung als auch über eine X.75-Verbindung verwendet werden.

Die Phasen einer PPP-Verhandlung

Der Verbindungsaufbau über PPP startet immer mit einer Verhandlung der Parameter, die für die Verbindung verwendet werden sollen. Diese Verhandlung läuft in vier Phasen ab, deren Kenntnis für die Konfiguration und Fehlersuche wichtig sind.

- Establish-Phase

  Nach einem Verbindungsaufbau über den Datenkommunikationsteil startet die Aushandlung der Verbindungsparameter über das LCP.

  Es wird festgestellt, ob die Gegenstelle auch bereit ist, PPP zu benutzen, die Paketgrößen und das Authentifizierungsprotokoll (PAP, CHAP, MS-CHAP oder keines) werden festgelegt. Danach wechselt das LCP in den Opened-Zustand.

- Authenticate-Phase

  Falls notwendig, werden danach die Passworte ausgetauscht. Bei Authentifizierung nach PAP wird das Passwort nur einmalig übertragen. Bei Benutzung von CHAP oder MS-CHAP wird ein verschlüsseltes Passwort periodisch in einstellbaren Abständen gesendet.

  Evtl. wird in dieser Phase auch ein Rückruf über CBCP (Callback Control Protocol) ausgehandelt.

- Network-Phase

  Im Gerät sind die Protokolle IPCP und IPXCP implementiert.

  Nach erfolgreicher Übertragung des Passwortes können die Netzwerk-Layer IPCP und/oder IPXCP aufgebaut werden.

  Ist die Verhandlung der Parameter für mindestens eines der Netzwerk-Layer erfolgreich verlaufen, können von den Router-Modulen IP- und/oder IPX-Pakete auf der geöffneten (logischen) Leitung übertragen werden.

- Terminate-Phase

  In der letzten Phase wird die Leitung geschlossen, wenn die logischen Verbindungen für alle Protokolle abgebaut sind.

Die PPP-Verhandlung im Gerät

Der Verlauf einer PPP-Verhandlung wird in der PPP-Statistik der Geräte protokolliert und kann im Fehlerfall mit Hilfe der dort detailliert gezählten Protokoll-Pakete überprüft werden.

Eine weitere Analyse-Möglichkeit bieten die PPP-Trace-Ausgaben. Mit dem Befehl

```
trace + ppp
```

kann die Ausgabe der ausgetauschten PPP-Protokoll-Frames innerhalb einer Terminal-Sitzung gestartet werden. Wird diese Terminal-Sitzung in einem Log-File protokolliert, kann nach Abbruch der Verbindung eine detaillierte Analyse erfolgen.

6.11.2 Alles o.k.? Leitungsüberprüfung mit LCP

Beim Verbindungsaufbau über PPP handeln die beteiligten Geräte ein gemeinsames Verhalten während der Datenübertragung aus. Sie entscheiden z. B. zunächst, ob mit den Einstellungen der Sicherungsverfahren, Namen und Passwörter überhaupt eine Verbindung zustande kommen darf.

Wenn die Verbindung einmal steht, kann mit Hilfe des LCPs die Zuverlässigkeit der Leitung ständig überprüft werden. Innerhalb des Protokolls geschieht dies mit dem LCP-Echo-Request und dem zugehörigen LCP-Echo-Reply. Der LCP-Echo-Request ist eine Anfrage in Form eines Datenpakets, das neben

den reinen Nutzdaten zur Gegenstelle übertragen wird. Wenn auf diese Anfrage eine gültige Antwort (LCP-Echo-Reply) zurückgeschickt wird, ist die Verbindung zuverlässig und stabil. Zur dauerhaften Überprüfung der Verbindung wird dieser Request in bestimmten Abständen wiederholt.

Was passiert nun, wenn der Reply ausbleibt? Zuerst werden einige Wiederholungen der Anfrage gestartet, um kurzfristige Störungen der Leitung auszuschließen. Wenn alle diese Wiederholungen unbeantwortet bleiben, wird die Leitung abgebaut und ein Ersatzweg gesucht. Streikt beispielsweise die Highspeed-Verbindung, kann als Backup eine vorhandene ISDN-Schnittstelle den Weg ins Internet bahnen.

Hinweis: Beim Remote Access von einzelnen Arbeitsplatzrechnern mit Windows-Betriebssystem empfehlen wir, die regelmäßigen LCP-Anfragen des Geräts auszuschalten, weil diese Betriebssysteme die LCP-Echo-Requests nicht beantworten und die Verbindung dadurch abgebaut würde.

Hinweis: Das Verhalten der LCP-Anfragen stellen Sie in der PPP-Liste für jede Verbindung einzeln ein. Mit dem Eintrag in die Felder 'Zeit' und 'Wdh.' legen Sie fest, in welchen Abständen die LCP-Anfrage gestellt werden soll und wie viele Wiederholungen beim Ausbleiben der Antwort gestartet werden, bis die Leitung als gestört bezeichnet werden darf. Mit einer Zeit von '0' und '0' Wiederholungen stellen Sie die LCP-Requests ganz ab.

6.11.3 Zuweisung von IP-Adressen über PPP

Zur Verbindung von Rechnern, die TCP/IP als Netzwerkprotokoll einsetzen, benötigen alle Beteiligten eine gültige und eindeutige IP-Adresse. Wenn nun eine Gegenstelle keine eigene IP-Adresse hat (z. B. der einzelne Arbeitsplatzrechner eines Teleworkers), dann kann das Gerät ihm für die Dauer der Verbindung eine IP-Adresse zuweisen und so die Kommunikation ermöglichen.

Diese Art der Adresszuweisung wird während der PPP-Verhandlung durchgeführt und nur für Verbindungen über das WAN eingesetzt. Die Zuweisung von Adressen mittels DHCP wird dagegen (normalerweise) innerhalb eines lokalen Netzwerks verwendet.

Hinweis: Die Zuweisung einer IP-Adresse wird nur dann möglich, wenn das Gerät die Gegenstelle beim Eintreffen des Anrufs über die Rufnummer oder den Namen identifizieren kann, d.h. die Authentifizierung erfolgreich war.

Beispiele

- Remote Access

  Die Zuweisung der Adresse wird durch einen speziellen Eintrag in der IP-Routing-Tabelle ermöglicht. Neben dem Eintrag der IP-Adresse, die der Gegenstelle aus dem Feld 'Router-Name' zugewiesen werden soll, wird als Netzmaske die 255.255.255.255 angegeben. Der Routername ist in diesem Fall der Name, mit dem sich die Gegenstelle beim Gerät anmelden muss.

  Neben der IP-Adresse werden der Gegenstelle bei dieser Konfiguration auch die Adressen der DNS- und NBNS-Server (Domain Name Server und NetBIOS Name Server) inkl. des Backup-Servers aus den Einträgen im TCP/IP-Modul übermittelt.

  Damit das Ganze funktioniert, muss die Gegenstelle natürlich auch so eingestellt sein, dass sie die IP-Adresse und die Namensserver vom Gerät bezieht. Das geschieht z. B. im DFÜ-Netzwerk von Windows durch die Einträge in den 'TCP-Einstellungen' unter 'IP-Adresse' bzw. 'DNS-Konfiguration'. Hier werden die Optionen 'Vom Server zugewiesene IP-Adresse' und 'Vom Server zugewiesene Namensserveradressen' aktiviert.

- Internet-Zugang

  Wird über das Gerät der Zugang zum Internet für ein lokales Netz realisiert, kann die Zuweisung von IP-Adressen den umgekehrten Weg nehmen. Hierbei sind Konfigurationen möglich, in denen das Gerät selbst keine im Internet gültige IP-Adresse hat und sich für die Dauer der Verbindung eine vom Internet-Provider zuweisen lässt. Neben der IP-Adresse erhält das Gerät während der PPP-Verhandlung auch Informationen über DNS-Server beim Provider.

  Im lokalen Netz ist das Gerät nur mit seiner intern gültigen Intranet-Adresse bekannt. Alle Arbeitsplatzrechner im lokalen Netz können dann auf den gleichen Internet-Account zugreifen und auch z. B. den DNS-Server erreichen.

Die zugewiesenen Adressen schauen sich Windows-Anwender per LANmonitor an. Neben dem Namen der verbundenen Gegenstelle finden Sie hier die aktuelle IP-Adresse sowie die Adressen von DNS- und NBNS-Servern. Auch Optionen wie die Kanalbündelung oder die Dauer der Verbindung werden angezeigt.

6.11.4 Einstellungen in der PPP-Liste

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

Darüberhinaus können Sie festlegen, ob die Datenkommunikation über eine IPv4- oder eine IPv6-Verbindung erfolgen soll.

Zur Authentifizierung von Point-to-Point-Verbindungen im WAN wird häufig eines der Protokolle PAP, CHAP, MSCHAP oder MSCHAPv2 eingesetzt. Dabei haben die Protokolle untereinander eine „Hierarchie“, d. h. MSCHAPv2 ist ein „höheres“ Protokoll als, MSCHAP, CHAP und PAP (höhere Protokolle zeichnen sich durch höhere Sicherheit aus). Manche Einwahlrouter bei den Internetprovidern erlauben vordergründig die Authentifizierung über ein höheres Protokoll wie CHAP, unterstützen im weiteren Verlauf aber nur die Nutzung von PAP. Wenn im Gerät das Protokoll für die Authentifizierung fest eingestellt ist, kommt die Verbindung ggf. nicht zustande, da kein gemeinsames Authentifizierungsprotokoll ausgehandelt werden kann.

Hinweis: Prinzipiell ist es möglich, während der Verbindungsaushandlung eine erneute Authentifizierung durchzuführen und dafür ein anderes Protokoll auszuwählen, wenn dies zum Beispiel erst durch den Usernamen erkannt werden konnte. Diese erneute Aushandlung wird aber nicht in allen Szenarien unterstützt.

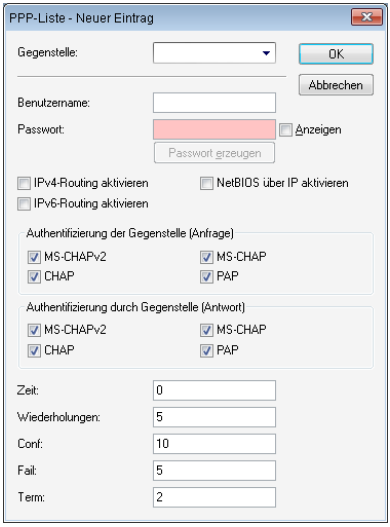
Mit der flexiblen Einstellung der Authentifizierungsprotokolle im Gerät wird sichergestellt, dass die PPP-Verbindung wie gewünscht zustande kommt. Dazu können ein oder mehrere Protokolle definiert werden, die zur Authentifizierung von Gegenstellen im Gerät (eingehende Verbindungen) bzw. beim Login des Gerätes in andere Gegenstellen (ausgehende Verbindungen) akzeptiert werden.

- Das Gerät fordert beim Aufbau eingehender Verbindungen das niedrigste der zulässigen Protokolle, lässt aber je nach Möglichkeit der Gegenstelle auch eines der höheren (im Gerät aktivierten) Protokolle zu.

- Das Gerät bietet beim Aufbau ausgehender Verbindungen alle aktivierten Protokolle an, lässt aber auch nur eine Auswahl aus genau diesen Protokollen zu. Das Aushandeln eines der nicht aktivierten, evtl. höheren Protokolle ist nicht möglich.

Die Einstellung der PPP-Authentifizierungsprotokolle finden Sie in der PPP-Liste.

LANconfig: **Kommunikation** > **Protokolle** > **PPP-Liste**



6.11.5 Die Bedeutung der DEFAULT-Gegenstelle

Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim Gerät an. Anhand des Namens kann das Gerät aus der PPP-Tabelle die zulässigen Werte für die Authentifizierung entnehmen. Manchmal kann die Gegenstelle bei Verhandlungsbeginn nicht über Rufnummer (ISDN-Einwahl), IP-Adresse (PPTP-Einwahl) oder MAC-Adresse (PPPoE-Einwahl) identifiziert werden, die zulässigen Protokolle können also im ersten Schritt nicht ermittelt werden. In diesen Fällen wird die Authentifizierung zunächst mit den Protokollen vorgenommen, die für die Gegenstelle mit dem Namen DEFAULT aktiviert sind. Wenn die Gegenstelle mit diesen Einstellungen erfolgreich authentifiziert wurde, können auch die für die Gegenstelle zulässigen Protokolle ermittelt werden.

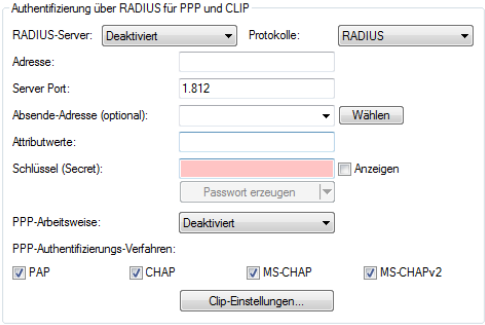
Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

6.11.6 RADIUS-Authentifizierung von PPP-Verbindungen

PPP-Verbindungen können auch über einen externen RADIUS-Server authentifiziert werden. Diese externen RADIUS-Server unterstützen jedoch nicht unbedingt alle verfügbaren Protokolle. Bei der Konfiguration der RADIUS-Authentifizierung können daher auch die zulässigen Protokolle ausgewählt werden. Die LCP-Verhandlung wird mit den erlaubten Protokollen neu gestartet, wenn der RADIUS-Server das ausgehandelte Protokoll nicht unterstützt.

WAN-RADIUS-Tabelle

LANconfig: Kommunikation / RADIUS



Telnet: Setup / WAN / RADIUS

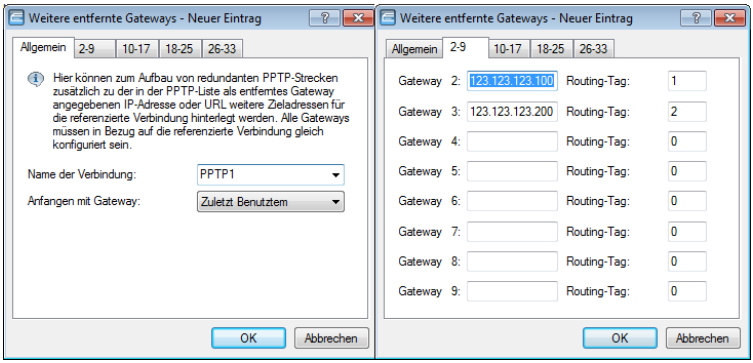
6.11.7 32 zusätzliche Gateways für PPTP-Verbindungen

Einleitung

Zur Sicherung der Erreichbarkeit können für jede PPTP-Gegenstelle bis zu 32 zusätzliche Gateways konfiguriert werden, so dass insgesamt pro PPTP-Gegenstelle 33 Gateways genutzt werden können.

Konfiguration

Die zusätzlichen PPTP-Gateways weden in einer separaten Liste definiert.



LANconfig: Kommunikation / Protokolle / Weitere entfernte Gateways

WEBconfig: HiLCOS-Menübaum / Setup / WAN / Zusaetzliche-PPTP-Gateways

▶ **Name der Verbindung**

Wählen Sie hier aus, für welche PPTP-Gegenstelle dieser Eintrag gelten soll.

Mögliche Werte:

– Auswahl aus der Liste der definierten PPTP-Gegenstellen.

Default:

– leer.

▶ **Anfangen mit**

Wählen Sie hier aus, in welcher Reihenfolge die Einträge versucht werden sollen.

Mögliche Werte:

– Zuletzt benutztem: Wählt den Eintrag, zu dem zuletzt erfolgreich eine Verbindung hergestellt werden konnte.
– Erstem: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.

– Zufall: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

Default:

– Zuletzt benutztem

▶ **Gateway 2 bis 33**

Tragen Sie hier die IP-Adressen der zusätzlichen Gateways ein, die für diese PPTP-Gegenstelle verwendet werden können.

Mögliche Werte:

– IP-Adresse oder 63 alphanumerische Zeichen.

Default:

– leer.

▶ **Routing-Tag**

Geben Sie hier das Routing-Tag an, mit dem die Route zum zugehörigen entfernten Gateway ermittelt wird.

Mögliche Werte:

– maximal 5 Ziffern.

Default:

– 0.

Hinweis: Wenn Sie hier kein Routing-Tag angeben (d.h. das Routing-Tag ist 0), dann wird für den zugehörigen Gateway das in der PPTP-Verbindungsliste für diese Gegenstelle konfigurierte Routing-Tag verwendet.

6.12 DSL-Verbindungsaufbau mit PPTP

Einige DSL-Anbieter ermöglichen die Einwahl nicht über PPPoE, sondern über PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol). Bei PPTP handelt es sich um

eine Protokoll-Erweiterung von PPP, die vorrangig von Microsoft entwickelt wurde.

PPTP ermöglicht es, „Tunnel“ über IP-Netze zu einer Gegenstelle aufzubauen. Unter einem Tunnel versteht man eine logisch abgeschirmte Verbindung, die die übertragenen Daten vor dem unbefugten Zugriff Dritter schützen soll. Dazu wird der Verschlüsselungsalgorithmus RC4 eingesetzt.

Hinweis: Künftig ist es durch den Umbau des IPv4-Routers mit bestimmten Windows-Versionen nicht mehr möglich, mittels IPSec via PPTP eine VPN-Verbindung herzustellen. Davon betroffen sind die Systeme Windows 2000 und Windows XP.

6.12.1 Konfiguration von PPTP

Im Gerät werden alle notwendigen PPTP-Parameter vom Internet-Zugangs-Assistenten abgefragt, sobald der Internet-Zugang über PPTP ausgewählt wird. Zusätzlich zu den Eingaben, die auch beim normalen PPPoE-Zugang abgefragt werden, ist dabei nur die IP-Adresse des PPTP-Gateways anzugeben. Beim PPTP-Gateway handelt es sich zumeist um das DSL-Modem. Genauere Informationen stellt Ihnen Ihr DSL-Anbieter zur Verfügung.

Änderungen an der Konfiguration werden in der PPTP-Liste vorgenommen:

LANconfig: Kommunikation / Protokolle / PPTP-Liste

WEBconfig: HiLCOS-Menübaum / Setup / WAN / PPTP-Liste

Die PPTP-Konfiguration besteht aus drei Parametern:

- 'Gegenstelle' – Die Bezeichnung aus der Liste der DSL-Breitband-Gegenstellen.
- 'IP-Adresse' – IP-Adresse des PPTP-Gateways, zumeist die Adresse des DSL-Modems
- 'Port' – IP-Port, über den das PPTP-Protokoll läuft. Dem Protokollstandard gemäß sollte immer Port '1.723' angegeben sein.

6.13 Dauerverbindung für Flatrates – Keep-alive

Als Flatrates bezeichnet man pauschale Verbindungstarife, die nicht nach Verbindungszeiten, sondern pauschal für feste Perioden abgerechnet werden. Bei Flatrates lohnt sich der Verbindungsabbau nicht mehr. Im Gegenteil: Neue Mails sollen direkt am PC gemeldet werden, der Heimarbeitsplatz soll kontinuierlich mit dem Firmennetzwerk verbunden sein und man möchte für Freunde und Kollegen über Internet Messenger Dienste pausenlos erreichbar sein. Es ist also wünschenswert, dass Verbindungen ununterbrochen aufrechterhalten werden.

Beim Gerät sorgt das Keep-alive-Verfahren dafür, dass Verbindungen immer dann aufgebaut werden, wenn die Gegenstelle sie gekappt hat.

6.13.1 Konfiguration des Keep-alive-Verfahrens

Das Keep-alive-Verfahren wird in der Gegenstellenliste konfiguriert.

Wird die Haltezeit auf 0 Sekunden gesetzt, so wird die Verbindung nicht aktiv vom Gerät beendet. Der automatische Abbau von Verbindungen, über die längere Zeit keine Daten mehr übertragen wurden, wird mit einer Haltezeit von 0 Sekunden also deaktiviert. Durch die Gegenseite unterbrochene Verbindungen werden in dieser Einstellung allerdings nicht automatisch wiederhergestellt.

Bei einer Haltezeit von 9999 Sekunden wird die Verbindung nach jeder Trennung immer automatisch wieder neu aufgebaut. Ebenso wird die Verbindung nach dem Booten des Gerätes automatisch wieder aufgebaut ('auto reconnect').

6.14 Manuelle Definition der MTU

Verschiedene Internet-Provider betreiben zwar einen eigenen Backbone, bedienen sich aber für die Einwahl ihrer Kunden der Zugangsknoten der Telekom. Dieses „zweistufige“ Einwahlverfahren kann zu Problemen mit dem realisierten Datendurchsatz führen:

- Bei der Einwahl in den Knoten der Telekom handelt ein Gerät in der PPP-Verhandlung eine zulässige MTU aus, also die maximale Größe eines unfragmentierten Datenpakets. Diese MTU wird dann von Seiten des Geräts auch verwendet.
- Bei der Weitergabe der Datenpakete an den Backbone des eigentlichen Providers wird ein zusätzlicher Header aufgeschlagen, die Datenpakete werden also noch einmal größer. Um nun trotzdem wieder in die erlaubte Größe zu passen, werden die Datenpakete fragmentiert, also in kleinere Teile aufgeteilt. Diese zusätzliche Fragmentierung kann zu Geschwindigkeitseinbußen in der Datenübertragung führen.

Um diese Problematik zu umgehen, kann für jede Gegenstelle eine feste MTU eingetragen werden.

6.14.1 Konfiguration

WEBconfig: HiLCOS-Menübaum / Setup / WAN / MTU-Liste

Die Tabelle enthält folgende Einträge:

- Gerätename: Name der Gegenstelle. Es kann eine physikalische oder eine virtuelle (PPTP/VPN) Gegenstelle sein
- MTU: Auf der Verbindung zu verwendende MTU

6.14.2 Statistik

Unter **Status** / **WAN-Statistik** finden Sie die MTU-Statistik, in der für alle aktiven Verbindungen die verwendeten MTUs festgehalten werden. Diese Tabelle ist halbdynamisch und beginnt mit 16 Einträgen. Sie enthält wie die MTU-Liste unter **Setup** / **WAN** zwei Spalten in denen der Gegenstellen-Name und die MTU abgelegt werden.

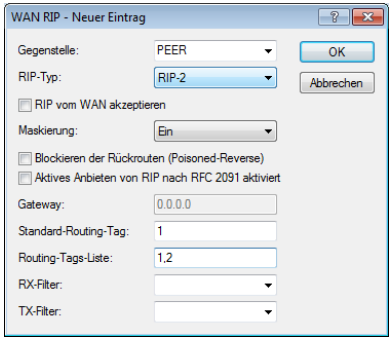
Gegenstelle	*MTU*	*Bemerkung*
INET	1200	Die Gegenstelle INET ist die Internet-Verbindung und hat eine erzwungene MTU von 1200 Bytes.
MULTI	1492	MULTI ist eine PPPoE-Verbindung, auf der die MTU ausgehandelt wurde (daher beträgt sie 1492 Bytes).
TESTVPN	1100	TESTVPN ist eine VPN-Verbindung, die über die Internet-Verbindung aufgebaut wurde. Für VPN- Verbindungen wird ein fester Overhead von 100 Bytes angenommen, weshalb die MTU hier 1100 Bytes beträgt.

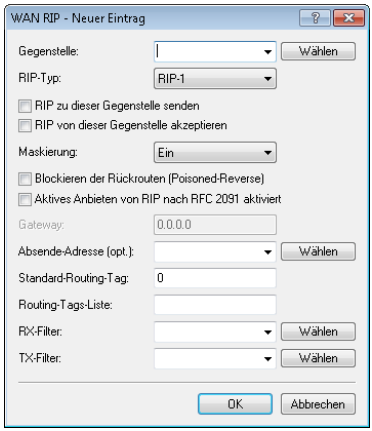
Gegenstelle	*MTU*	*Bemerkung*
TESTVPN-PPTP	1060	TESTVPN-PPTP ist eine PPTP-Verbindung, die über die VPN-Verbindung TESTVPN aufgebaut wurde. Der Overhead von PPTP-Verbindungen beträgt 40 Bytes, weshalb die MTU hier 1060 Bytes beträgt.

Hinweis: MTU-Liste und MTU-Statistik existieren nur auf Geräten mit DSL oder ADSL-Interface.

6.15 WAN-RIP

Um die über RIP gelernten Routen auch über das WAN bekannt zu machen, können die entsprechenden Gegenstellen unter **IP-Router** > **Allgemein** > **WAN-RIP** in der WAN-RIP-Tabelle eingetragen werden.





Die WAN-RIP-Tabelle enthält folgende Werte:

Peer

Enthält den Namen der Gegenstelle.

RIP-Typ

Gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden.

RIP zu dieser Gegenstelle senden

Stellen Sie ein, ob RIP auf dem WAN Routen propagiert. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

RIP von dieser Gegenstelle akzeptieren

Stellen Sie ein, ob RIP aus dem WAN akzeptiert wird. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

Achtung: Bitte beachten Sie, dass WAN-seitiges RIP ein potenzielles Sicherheits-Risiko darstellt.

Maskierung

Geben Sie an, ob und wie das Gerät auf der Strecke maskiert. Durch diesen Eintrag ist es möglich, das WAN-RIP auch mit einer leeren Routing-Tabelle zu starten. Es sind folgende Werte möglich:

- **Auto**: Der Maskierungstyp wird aus der Routing-Tabelle entnommen (Wert: 0). Existiert für die Gegenstelle kein Routing-Eintrag, so wird nicht maskiert.
- **An**: Alle Verbindungen werden maskiert (Wert: 1).
- **Intranet**: Verbindungen aus dem Intranet werden maskiert, Verbindungen aus der DMZ gehen transparent hindurch (Wert: 2).

Blockieren der Rückrufrouten (Poisoned-Reverse)

Beim Blockieren der Rückrouten (Poisoned-Reverse) werden alle über diese Schnittstelle gelernten/empfangenen Routen als “nicht erreichbar” gekennzeichnet und zurückgesendet, indem die Anzahl der Hops direkt auf 16 (bzw. die maximale Anzahl) gesetzt wird.

Aktives Anbieten von RIP nach RFC 2091 aktiviert

Das Gerät unterstützt grundsätzlich RIP nach RFC 2091.

Die Einstellung “RFC 2091 anbieten” ist nur für den aktiven Verbindungsaufbau relevant. Bei passiven Verbindungen wird für jede Gegenstelle die RIP-Version genommen, die die Gegenstelle anbietet - unabhängig von der Stellung dieses Schalters.

Bei aktiven Verbindungsaufbauten gibt es zudem bei aktiviertem Anbieten von RIP nach RFC-2091 einen Rückfall auf “normales” RIP nach RFC 2453: Wenn die Gegenstelle nach 10 Wiederholungen des ersten Pakets nicht geantwortet hat, wird zurückgeschaltet (10 Wiederholungen dauern ca. 30 Sekunden).

Als Gateway wird die IP-Adresse des RIP-Partners auf der anderen Seite der WAN-Strecke eingetragen. Hier kann 0.0.0.0 eingetragen werden, wenn auf der WAN-Strecke eine PPP-Verhandlung läuft und dabei die IP-Adresse der Gegenseite übermittelt wird.

Hinweis: In einem Zentral-Gateway kann die Einstellung “RFC 2091” immer aus und der Eintrag "Gateway" immer auf 0.0.0.0 stehen, da das Zentral-Gateway immer die Vorgabe des Filial-Gateway berücksichtigt.

Gateway

Tragen Sie die IP-Adresse des RIP-Partners ein.

Absende-Adresse (opt.)

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben. Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- “INT” für die Adresse des ersten Intranets.
- “DMZ” für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens “DMZ” gibt, dann wird deren Adresse genommen).
- LB0…LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Hinweis: Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Standard-Routing-Tag

Gibt das für die WAN-Verbindung geltende “Standard-Routing-Tag”. Alle ungetaggten Routen taggt das Gerät beim Versenden im WAN mit diesem Tag.

Routing-Tags-Liste

In dieser Liste steht eine kommaseparierte Liste der Tags, die das Gerät auf dem Interface akzeptiert. Wenn diese Liste leer ist, akzeptiert das Gerät alle Tags. Steht mindestens ein Tag in der Liste, dann akzeptiert das Gerät nur die Tags in dieser Liste. Ebenso propagiert das Gerät beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags.

Alle vom WAN gelernten Routen behandelt das Gerät intern als ungetaggte Routen und propagiert diese über das LAN mit dem Default-Tag (0). Über das WAN hingegen propagiert es die Routen mit dem Tag, mit dem es sie auch gelernt hat.

RX-Filter

Geben Sie hier beim Empfang (RX) von RIP-Paketen die anzuwendenden Filter an.

Hinweis: Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

TX-Filter

Geben Sie hier beim Senden (TX) von RIP-Paketen die anzuwendenden Filter an.

Hinweis: Definieren Sie die Filter zuerst in der RIP-Filterliste, um sie hier verwenden zu können.

6.16 Das Rapid-Spanning-Tree-Protokoll

In Netzwerken mit mehreren Switches und Bridges können zwischen zwei angeschlossenen Netzwerkteilnehmern durchaus mehrere physikalische Verbindungen bestehen. Diese redundanten Datenwege sind auch durchaus erwünscht, da sie bei Ausfall einzelner Netzstränge alternative Wege zum Ziel anbieten können. Auf der anderen Seite kann es durch diese Mehrfachverbindungen zu unerwünschten Schleifen (Loops) oder zu mehrfach empfangenen Frames kommen. Beide Effekte stören den reibungslosen Datenverkehr im Netz.

Das Spanning-Tree-Protokoll (STP) ermöglicht die Analyse des Netzwerks auf Layer-2-Ebene und bietet somit auch unterhalb der Routing-Schicht Lösungen zur intelligenten Wegeauswahl zwischen zwei Netzteilnehmern. Durch das Auffinden redundanter Wege zwischen den Netzteilnehmern bildet STP eine eindeutige Struktur, in der Loops und doppelte Pakete vermieden werden. Dazu werden so genannte Bridge Protocol Data Units (BPDUs) als Multicast an eine bestimmte MAC-Adresse gesendet. Die BPDUs ermöglichen das Auffinden von doppelten Strecken sowie der Entfernung und der auf dieser Verbindung verfügbaren Datenrate. Aus diesen Werten errechnet das Spanning-Tree-Protokoll eine Priorität (auch Wege- oder Pfadkosten genannt), mit der die verschiedenen Verbindungen zu behandeln sind. Die Verbindungen

mit geringerer Priorität werden deaktiviert und stehen somit nicht für die Clients zur Verfügung. Durch die Reduktion auf nicht redundante Verbindungen zwischen den Clients baut das Protokoll einen Baum auf, in dem von einem zentralen Switch (Root-Bridge) aus alle Verbindungen eindeutig sind.

Die BPDUs werden regelmäßig im Netzwerk verschickt, um die Verfügbarkeit der Verbindungen zu prüfen. Fällt eine der Verbindungen aus, wird die Analyse des Netzwerks erneut ausgelöst, die möglichen Wege und die zugehörigen Prioritäten werden neu festgelegt.

Nach der Initialisierung befinden sich zunächst alle Ports im Zustand „Blocking“, in dem nur BPDUs übertragen werden. Anschließend wechseln die Ports über die Zustände Listening und Learning in den Zustand „Forwarding“, in dem Nutzdaten über die Ports übertragen werden können.

6.16.1 Classic und Rapid Spanning Tree

Das zunächst verwendete Spannig-Tree-Protokoll nach IEEE 802.1D – im Weiteren auch als Classic Spanning Tree bezeichnet – hatte jedoch das Problem, dass die Aktualisierung der Topologie durch den Ausfall einer Verbindung nur recht langsam umgesetzt wurde: 20 bis 30 Sekunden, je nach Komplexität des Netzwerkes auch bis zu einer Minute braucht das klassische Spanning Tree zum Aufbau neuer Verbindungswege. Für viele Netzwerkdienste sind solch lange Ausfallzeiten nicht akzeptabel.

Das Spanning Tree Protokoll wurde daher verbessert und als „Rapid Spanning Tree Protokoll“ (RSTP) zunächst in einem eigenen Standard IEEE 802.1t/w, später als Teil der Neufassung von IEEE 802.1D veröffentlicht. Auch wenn das klassische Spanning Tree Protokoll damit zurückgezogen wurde, wird es in HiLCOS weiter unterstützt und zur Auswahl angeboten.

6.16.2 Verbesserungen durch Rapid Spanning Tree

Wie zuvor bemerkt ist das Hauptziel von RSTP die beschleunigte Aktivierung von Netzwerkpfaden, wenn eine der aktiven Verbindungen ausfällt. RSTP verzichtet dabei u.a. auf die Zustände Blocking und Listening und reduziert die benötigte Zeit zur Aktualisierung der Netzwerkpfade auf wenige Sekunden. Beim Ausfall eines Netzwerkpfades werden nicht mehr alle Links blockiert, bis die neue Topologie berechnet ist, sondern nur die ausgefallenen Verbindungen fallen für die Nutzung aus.

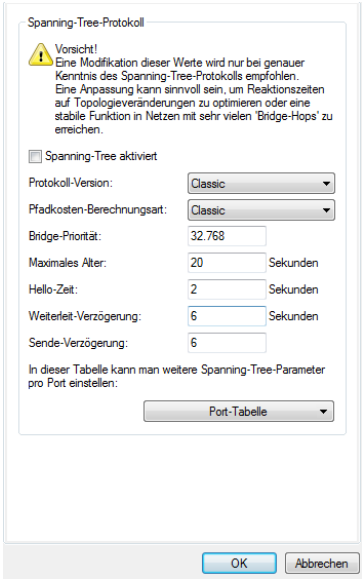
RSTP ermöglicht es dem Administrator darüber hinaus, Informationen über die Topologie des Netzwerk zu konfigurieren:

- Ein Bridge-Port kann dazu als „Grenz-Port“ (Edge-Port) definiert werden. Ein Edge-Port ist der einzige Bridge-Port, der zu dem angeschlossenen LAN-Segment führt – an dem LAN-Segment sind also keine anderen Bridges angeschlossen, sondern nur z. B. Workstations oder Server. Da diese Ports nicht zu Loops führen können, wechseln sie sofort in den Forwarding-Zustand, ohne die Ermittlung der Netzwerktopologie abzuwarten. Das RSTP überwacht solche Ports jedoch weiterhin – falls unerwartet doch BPDUs auf einem Edge-Port empfangen werden, weil doch eine andere Bridge am LAN angeschlossen wurde, fällt der Port automatisch in den Normalzustand zurück.
- Ein Bridge-Port kann auch als Point-to-Point-Link eingesetzt werden. In diesem Fall ist der Port direkt mit einer weiteren Bridge verbunden. Da zwischen den beiden Bridges keine weiteren Zwischenstationen auftreten können, kann der Wechsel in den Forwarding-Zustand schneller erfolgen.

Im Idealfall kann RSTP bekannte alternative Netzwerkpfade sofort nutzen, wenn eine Verbindung ausfällt.

6.16.3 Konfiguration des Spanning-Tree-Protokolls

Zur Konfiguration der RSTP- bzw. STP-Funktion im Gerät stehen folgende Parameter bereit:



LANconfig: Schnittstellen / Span. Tree

WEBconfig, Telnet: HiLCOS-Menübaum / Setup / LAN-Bridge / Spanning-Tree

Allgemeine Parameter

- Spanning-Tree aktiviert

  Bei ausgeschaltetem Spanning Tree verschickt ein Gerät keine Spanning-Tree-Pakete und leitet empfangene Spanning-Tree-Pakete durch, anstatt sie selber zu verarbeiten.

- Protokoll-Version

  - Classic: Verwendet die Verfahren des klassischen STP zur Bestimmung der Netzwerktopologie.
  - Rapid: Verwendet die Verfahren des RSTP zur Bestimmung der Netzwerktopologie.

Hinweis: RSTP ist kompatibel zu STP. Wenn Komponenten im Netzwerk verwendet werden, die nur das klassische STP unterstützen, werden auch bei Aktivierung von RSTP die Verfahren von STP verwendet.

- Pfadkosten-Berechnung
  - Classic: Verwendet die Verfahren des klassischen STP zur Pfadkostenberechnung.
  - Rapid: Verwendet die Verfahren des RSTP zur Pfadkostenberechnung.
- Bridge-Priorität

  Legt die Priorität der Bridge im LAN fest. Damit kann man beeinflussen, welche Bridge vom Spanning-Tree-Protokoll bevorzugt zur Root-Bridge gemacht wird.

  Hinweis: Aus Gründen der Kompatibilität zu RSTP sollte dieser Wert nur in Schritten von 4096 verändert werden, da bei RSTP die unteren 12 Bit dieses 16-Bit-Wertes für andere Zwecke verwendet werden.

- Maximales Alter

  Dieser Wert bestimmt die Zeit (in Sekunden), nach der eine Bridge über Spanning-Tree empfangene Nachrichten als 'veraltet' verwirft. Dieser Parameter bestimmt, wie schnell der Spanning-Tree-Algorithmus auf Änderungen z. B. durch ausgefallene Bridges reagiert.

- Hello-Zeit

  Dieser Parameter (in Sekunden) legt fest, in welchen Intervallen ein als Root-Bridge ausgewähltes Gerät Spanning-Tree-Informationen ins LAN schickt.

- Weiterleit-Verzögerung

  Diese Zeit (in Sekunden) legt fest, wieviel Zeit mindestens vergehen muss, bevor ein Spanning-Tree-Port den Zustand (Listening, Learning, Forwarding) wechseln darf.

Hinweis: Bei Verwendung des RSTP hat die Weiterleitungs-Verzögerung oft keine Auswirkung, da das RSTP selbst über geeignete Mechanismen verfügt, um den schnellen Wechsel in den Forwarding-Zustand auszulösen.

Hinweis: Eine Modifikation dieser drei Zeitwerte wird nur bei genauer Kenntnis des Spanning-Tree-Protokolls empfohlen. Eine Anpassung kann sinnvoll sein, um Reaktionszeiten auf Topologieveränderungen zu optimieren oder eine stabile Funktion in Netzen mit sehr vielen 'Bridge-Hops' zu erreichen.

- Sende-Verzögerung

  Anzahl der BPDUs, die bei RSTP gesendet werden dürfen, bevor eine Sekunde Pause eingelegt wird.

  Hinweis: Bei Verwendung des klassischen STP hat die Sende-Verzögerung keine Auswirkung.

Port-Tabelle

In der Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte separat eingestellt werden.

- Als Edge-Port kennzeichnen

  Kennzeichnet den Port als Edge-Port, an dem keine weitere Bridge, sondern nur Endgeräte wie Workstations oder Server angeschlossen sind. Edge-Ports wechseln sofort in den Forwarding-Zustand.

  Hinweis: Edge-Ports werden weiterhin vom RSTP überwacht. Werden an einem solchen Port BPDU entdeckt, verliert der Port den Status als Edge-Port.

- Priorität

  Legt die Priorität des Ports fest. Bei mehreren möglichen Netzwerkpfaden mit gleichem Pfadkosten entscheidet die Priorität, welcher Port verwendet

wird. Bei Gleichheit der Priorität wird der Port gewählt, der weiter oben in der Liste steht.

Hinweis: Aus Gründen der Kompatibilität zu RSTP darf dieser Wert nur in Schritten von 16 verändert werden, da bei RSTP nur die oberen 4 Bit dieses 16-Bit-Wertes genutzt werden.

- Pfadkosten-Beeinflussung

  Mit diesem Parameter wird die Priorität von gleichwertigen Pfaden gesteuert. Der hier eingestellte Wert wird anstelle der berechneten Pfadkosten für die Auswahl verwendet.

  - Besondere Werte: 0 schaltet die Pfadkosten-Beeinflussung aus.
  - Default: 0

6.16.4 Statusmeldungen über das Spanning-Tree-Protokoll

Die aktuellen Werte des STP können im LAN-Bridge-Status über Telnet oder Browser eingesehen werden.

WEBconfig: HiLCOS-Menübaum / Status / LAN-Bridge / Spanning-Tree

Allgemeine Statusinformationen

- Bridge-ID

  Dies ist die ID des Gerätes, die vom Spanning-Tree-Algorithmus benutzt wird. Sie setzt sich aus der vom Benutzer festgelegten Priorität (obere 16 Bit) und der Geräte-MAC-Adresse (untere 48 Bit) zusammen.

- Root-Bridge

  Die ID des momentan zur Root-Bridge gewählten Geräts.

- Root-Port

  Der Port, über den von diesem Gerät aus die Root-Bridge erreicht werden kann. Falls das Gerät gerade selber die Root-Bridge ist, wird das mit dem Sonderwert '255' angezeigt.

- Root-Pfadkosten

Die aufsummierten Pfad-Kosten aller Hops, um von diesem Gerät aus die Root-Bridge zu erreichen.

- Protokoll-Version

  Aktuell eingestellte Protokollversion zur Bestimmung der Netzwerktopologie.

- Pfadkosten-Berechnung

  Aktuell eingestellte Protokollversion zur Pfadkostenberechnung.

- Bridge-Priorität

  Aktuell eingestellte Priorität der Bridge.

Informationen in der Port-Tabelle

In der Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte eingesehen werden.

- Priorität

  Die aus der Port-Konfiguration übernommene Priorität dieses Ports.

- **Status**

  Der momentane Status des Ports:

  - disabled: keinerlei Pakete über diesen Port senden oder empfangen. Das tritt ein, wenn der Port entweder manuell deaktiviert wurde oder einen negativen Link-Status hat.
  - Listening: Zwischenzustand auf dem Weg zur Aktivierung. Es wird nur auf Spanning-Tree-Pakete gehört, Datenpakete werden ignoriert und auch nicht an diesen Port weitergeleitet.
  - Learning: weiterer Zwischenzustand. Gegenüber 'listening' werden zusätzlich MAC-Adressen von an diesem Port ankommenden Datenpaketen gelernt, es werden aber weiterhin keine Datenpakete weitergeleitet.
  - Forwarding: der Port ist vollständig aktiv, Datenpakete werden in beiden Richtungen entgegengenommen und weitergeleitet
  - Blocking: Spanning Tree hat diesen Port als redundant erkannt und für Datenverkehr deaktiviert.

- **Root**

Die ID der über diesen Port zu erreichenden Root-Bridge.

- **Bridge**

  Dies ist die ID der Bridge, über welche die Root-Bridge erreicht werden kann.

- **Kosten**

  Dieser Wert gibt die 'Kosten' für diesen Port an. Der Wert ergibt sich aus der Technologie (Ethernet, WLAN etc.) des Ports sowie der Bandbreite. Verwendete Werte sind z. B.:

Übertragungstechnologie	*Kosten für Classic Spanning Tree*	*Kosten für Rapid Spanning Tree*
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

Hinweis: Wurden manuell Pfadkosten für einen Port vorgegeben, erscheint in dieser Spalte der konfigurierte Wert.

Informationen in der RSTP-Port-Statistik

In der RSTP-Port-Tabelle können für alle verfügbaren Ports (LAN, Wireless LAN, Point-to-Point-Strecken) folgende Werte eingesehen werden.

- **Rolle**

  Root- oder Nicht-Root-Bridge.

- Learning

  Port im Learning-Zustand.

- Forwarding

Port im Forwarding-Zustand.

- Edge-Port

  Port als Edge-Port definiert.

- Protokoll-Version

  Klassisch oder Rapid.

- **Kosten**

  Eingestellte Kosten für diesen Port.

6.17 Die Aktions-Tabelle

6.17.1 Einleitung

Über die Aktions-Tabelle werden Aktionen gesteuert, die bei einem Zustandswechsel von WAN-Verbindungen ausgelöst werden. Als WAN-Verbindung kommen dabei sowohl die direkten Verbindungen z. B. zum Internetprovider in Frage als auch die darüber liegenden VPN-Verbindungen, z. B. bei der Anbindung von Filialen an eine Zentrale. Jede Aktion ist an eine Bedingung geknüpft, die den Zustandswechsel der WAN-Verbindung beschreibt (Aufbau, Abbau, Ende, Fehler oder Aufbaufehler). Als Aktionen können grundsätzlich alle Befehle genutzt werden, die über die Telnet-Konsole zur Verfügung stehen. Darüber hinaus können die Aktionen Benachrichtigungen per E-Mail oder SYSLOG versenden, einen HTTP-Aufruf absetzen oder eine DNS-Anfrage versenden. Mit verschiedenen Variablen können Informationen wie die aktuelle IP-Adresse oder der Name des Gerätes oder eine Fehlermeldung mit in die Aktionen eingebaut werden.

6.17.2 Aktionen für Dynamic DNS

Damit auch Systeme mit dynamischen IP-Adressen über das WAN – also beispielsweise über das Internet – erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server Anbietern. Die Server bei diesen Diensten ordnen die aktuelle IP-Adresse eines Gerätes dem gewählten FQDN-Namen zu (Fully Qualified Domain Name, z. B. “MyDevice.dynDNS.org”).

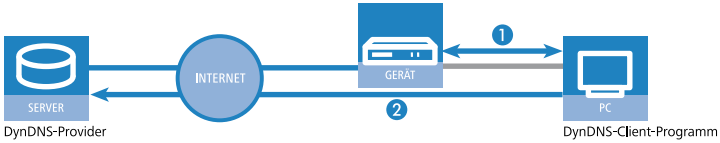
Der Vorteil liegt auf der Hand: Wenn Sie z. B. eine Fernwartung über WEBconfig/HTTP durchführen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen. Außerdem können die DynDNS-Namen auch zum Aufbau von VPN-Verbindungnen zwischen Gegenstellen mit wechselnden IP-Adressen genutzt werden.

Damit die Zuordnung von aktueller IP-Adresse und DynDNS-Name jederzeit funktioniert, muss bei jeder Änderung der IP-Adresse der entsprechende Eintrag auf dem DynDNS-Server aktualisiert werden. Diese Änderung wird von einem Dynamic-DNS-Client ausgelöst.

- Der DynDNS-Server, der von den DynDNS-Dienstleistern im Internet angeboten wird, steht mit Internet-DNS-Servern in Verbindung.
- Der Dynamic-DNS-Client kann als separates Clientprogramm auf einer Workstation laufen. Alternativ ist im Gerät ein Dynamic-DNS-Client integriert. Er kann zu einer Vielzahl von Dynamic-DNS-Serviceanbietern Kontakt aufnehmen und bei jeder Änderung seiner IP-Adresse automatisch ein vorher angelegtes Benutzerkonto zur DNS-Namensauflösung beim Dynamic-DNS-Anbieter aktualisieren.

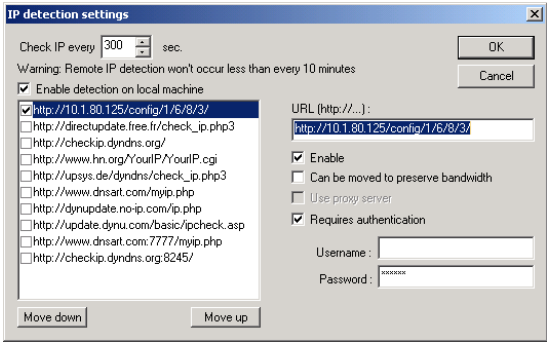
Dynamic-DNS-Client auf der Workstation

Dynamic-DNS-Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines Geräts ermitteln können **1** und im Falle einer Änderung an den jeweiligen Dynamic-DNS-Server übertragen **2**.



Die aktuelle WAN-seitige IP-Adresse eines Geräts kann unter folgender Adresse ausgelesen und dann in ein geeignetes Clientprogramm eingetragen werden:

```
http://<Adresse des Geräts>/config/1/6/8/3/
```



Dynamic-DNS-Client im Gerät über HTTP

Alternativ kann das Gerät die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:

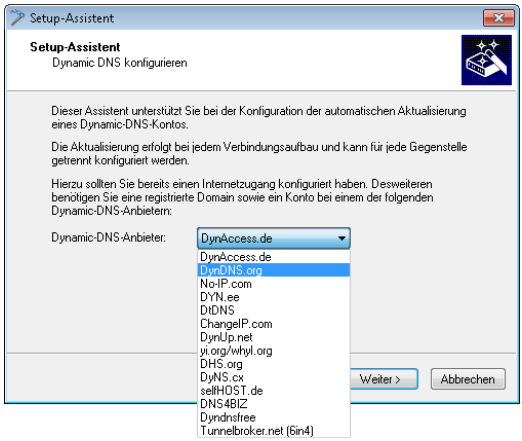
DynDNS-Provider

Dazu definieren Sie eine Aktion, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org kann z. B. so aussehen:

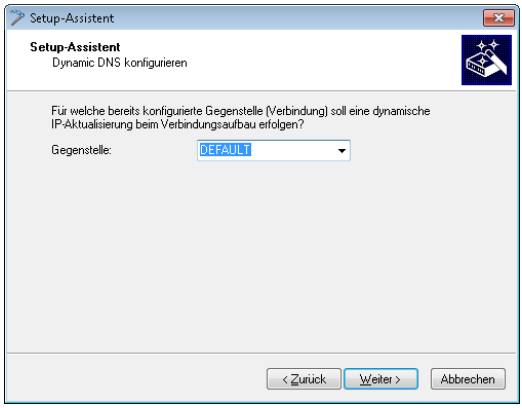
```
http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

Damit übermittelt das Gerät den Hostnamen der Aktion und seine aktuelle IP-Adresse an das durch Username und Password spezifizierte Konto beim DynDNS-Dienstleister DynDNS.org, der daraufhin den entsprechenden Eintrag aktualisiert. Die dazu notwendigen Einstellungen können Sie komfortabel mit dem Setup-Assistenten von LANconfig vornehmen.

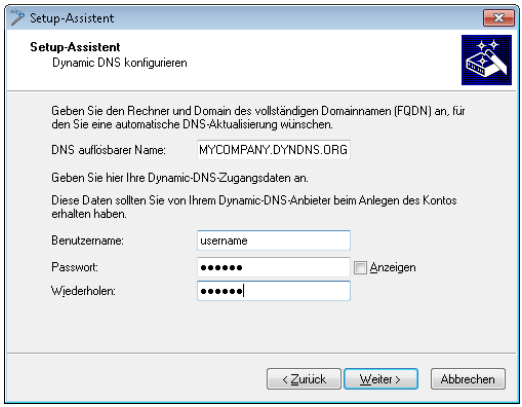
Wählen Sie aus der Liste zunächst den Dienstleister aus, den Sie verwenden möchten.



Bestimmen Sie jetzt die WAN-Gegenstelle, für die die Aktion gelten soll.



Geben Sie abschließend noch Ihre Zugangsdaten ein.



Der Setup-Assistent ergänzt die beschriebene Basis-Aktion um weitere anbieter-spezifischen Parameter, die hier nicht näher beschrieben sein sollen. Außerdem legt der Setup-Assistent weitere Aktionen an, die das Verhalten des Geräts steuern für den Fall, dass der DynDNS-Dienstleister die Aktualisierung nicht im ersten Versuch erfolgreich durchführen konnte.

Dynamic-DNS-Client im Gerät über GnuDIP

Als Alternative zur Aktualisierung der DynDNS-Informationen über eine einfache HTTP-Anfrage nutzen manche Dienste das GnuDIP-Protokoll. Das GnuDIP-Protokoll basiert auf einem Challenge-Response-Mechanismus:

1. Der Client öffnet die Verbindung zum GnuDIP-Server.
2. Der Server antwortet mit einem für die Sitzung berechneten Zufallswert.
3. Der Client erzeugt aus dem Zufallswert und dem Password einen Hashwert und sendet diesen an den Server zurück.
4. Der Server prüft diesen Hashwert und meldet das Ergebnis in Form einer Ziffer zurück an den Client.

Das GnuDIP-Protokoll kann die Nachrichten zwischen Client und Server entweder auf einer einfachen TCP-Verbindung austauschen (Standard-Port 3495) oder als CGI-Skript auf einem Internetserver laufen. Die Variante über einen HTTP-Aufruf des CGI-Skripts hat den Vorteil, dass auf dem Server kein weiterer Port für GnuDIP geöffnet werden muss, außerdem sichert HTTPS zusätzlich gegen passives Abhören und Offline-Wörterbuch-Attacken.

Die Anfragen an einen GnuDIP-Server werden aus dem Gerät mit einer Aktion in der folgenden Form ausgelöst:

- gnudip://<srv>[:port][/pfad]?<parameter>
  - <srv> – Die Adresse des GnuDIP-Servers.
  - [:port] – Die Angabe des Ports ist optional, falls nicht definiert, werden die Standardwerte verwendet (3495 für TCP, 80 bzw. 443 für HTTP/HTTPS).
  - [/pfad] – Die Pfadangabe wird nur bei HTTP/HTTPS benötigt, um den Speicherort des CGI-Skriptes zu definieren.

  Die folgenden Parameter erweitern den Aufruf:

  - method=<tcp|http|https> – Wählt das Protokoll aus, das für die Übertragung zwischen GnuDIP-Server und -Client verwendet werden soll. Hier kann nur genau ein Protokoll gewählt werden.
  - user=<username> – Gibt den Benutzernamen für das Konto auf dem GnuDIP-Server an.
  - pass=<password> – Gibt das Kennwort für das Konto auf dem GnuDIP-Server an.
  - domn=<domain> – Gibt die DNS-Domäne an, in der sich der DynDNS-Eintrag befindet.
  - reqc=<0|1|2> – Definiert die Aktion, die mit der Anfrage ausgelöst werden soll. Mit der Aktion <0> wird eine dedizierte IP-Adresse an den Server übermittelt, die für das Update verwendet werden soll. Mit der Aktion <1> wird ein DynDNS-Eintrag gelöscht. Mit der Aktion <2> wird ein Update ausgelöst, es wird aber keine IP-Adresse an den Server übermittelt. Statt dessen verwendet der Server die IP-Adresse des GnuDIP-Clients für das Update.
  - addr=<address> – Gibt für eine Aktion mit dem Parameter <0> die IP-Adresse an, die für das Update des DynDNS-Eintrags verwendet werden soll. Fehlt diese Angabe bei einer <0>-Aktion, so wird die Anfrage wie eine <2>-Aktion behandelt.

  Beim GnuDIP-Protokoll entspricht der Hostname, der registriert werden soll, dem an den Server übermittelten Benutzernamen. Wenn der Benutzername z. B. “myserver” lautet und die DNS-Domäne “mydomain.org”, dann wird der DNS-Name “myserver.mydomain.org” registriert.

  Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen,

sobald eine Verbindung aufgebaut wurde, und dabei die aktuelle IP-Adresse des Geräts (%a) übertragen:

– gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a

Um einen DynDNS-Eintrag zu löschen, wenn z. B. eine Verbindung getrennt wurde, verwenden Sie die folgende Aktion:

– gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=1

Der Zeilenumbruch dient jeweils nur der Lesbarkeit und wird nicht in die Aktion eingetragen.

Der GnuDIP-Server gibt als Ergebnis der Anfrage einen der folgenden Werte an den GnuDIP-Client zurück (vorausgesetzt, die Verbindung zwischen Server und Client konnte hergestellt werden):

- 0 – Der DynDNS-Eintrag wurde erfolgreich aktualisiert.
- 0:Adresse – Der DynDNS-Eintrag wurde erfolgreich mit der angegebenen Adresse aktualisiert.
- 1 – Die Authentifizierung am GnuDIP-Server war nicht erfolgreich.
- 2 – Der DynDNS-Eintrag wurde erfolgreich gelöscht.

Diese Antworten können in den Aktionen des Geräts ausgewertet werden, um bei Bedarf weitere Aktionen einzuleiten.

6.17.3 Weitere Beispiele für Aktionen

Information über Verbindungsabbruch als SMS auf Mobiltelefon melden

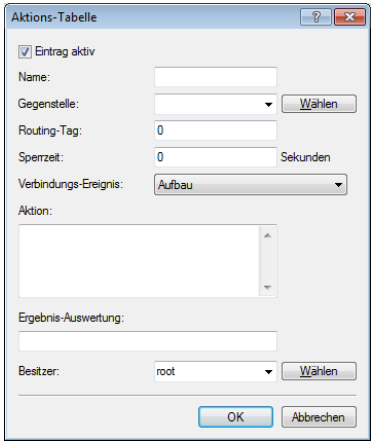
Mit dem Platzhalter %t kann die aktuelle Zeit über ein Ereignis in eine Benachrichtigung mit aufgenommen werden. So kann z. B. der Abbruch einer wichtigen VPN-Verbindung per E-Mail oder SMS an das Mobiltelefon eines Systemadministrators gemeldet werden.

Folgende Voraussetzungen müssen für die Benachrichtigung erfüllt sein:

- Der Zustand der VPN-Verbindung muss überwacht werden, z. B. durch die „Dead-Peer-Detection“ DPD.

- Das Gerät muss als NTP-Client konfiguriert sein, damit das Gerät über eine aktuelle Systemzeit verfügt.
- Ein SMTP-Konto zum Versand der E-Mails muss eingerichtet sein.

Wenn diese Voraussetzungen erfüllt sind, kann die Benachrichtigung eingerichtet werden. Legen Sie dazu in der Aktionstabelle einen neuen Eintrag an, z. B. mit LANconfig unter **Kommunikation** / **Allgemein** / **Aktionstabelle**.



In dem Eintrag wählen Sie die Gegenstelle aus, für die ein Verbindungsabbruch gemeldet werden soll. Dazu wählen Sie als Ereignis den 'Abbruch' und geben als Aktion den Versand einer Mail ein:

```
mailto:admin@mycompany.de?subject=VPN-Verbindung
abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde
unterbrochen.
```

Mit dieser Aktion wird bei Abbruch der Verbindung eine Mail an den Administrator versendet, dabei wird die Zeit bei Verbindungsabbruch in den Betreff eingefügt.

Hinweis: Wenn die Mail an ein entsprechendes Mail2SMS-Gateway gesendet wird, kann die Benachrichtigung auch direkt auf ein Mobiltelefon zugestellt werden.

Hinweis: In einem komplexen Aufbau mit mehreren Filialen wird im Gerät der Zentrale für jede Gegenstelle ein passender Eintrag angelegt. Zur Über-

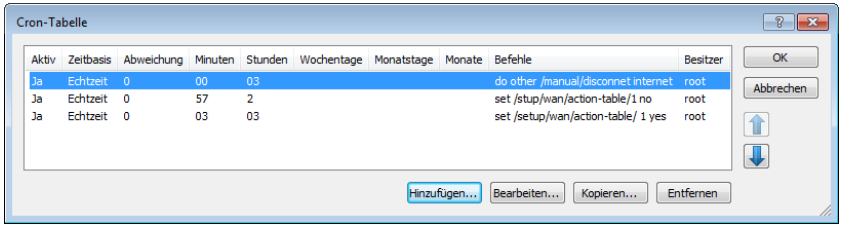
wachung der Zentrale selbst wird eine Aktion in einem Gerät in einer der Filialen angelegt. So kann der Administrator auch dann benachrichtigt werden, wenn das VPN-Gateway der Zentrale selbst ausfällt und vielleicht keine Nachricht mehr versenden kann.

Beispiel: Benachrichtigung bei Zwangstrennung der DSL-Verbindung unterdrücken

Je nach Anbieter wird die für VPN-Verbindungen genutzte DSL-Leitung einmal alle 24 Stunden zwangsweise getrennt. Damit der Administrator nicht auch über diese regelmäßigen Unterbrechungen informiert wird, kann die Benachrichtigung für die Zeit der Zwangstrennung ausgeschaltet werden.

Dazu wird zunächst mit einer Aktion die Zwangstrennung auf einen definierten Zeitpunkt gelegt, üblicherweise in die Nacht, wenn die Internetverbindung nicht benötigt wird. Der Eintrag wird z. B. auf 3:00 Uhr nachts gelegt und trennt die Internetverbindung mit dem Befehl `do other/manual/disconnect internet`.

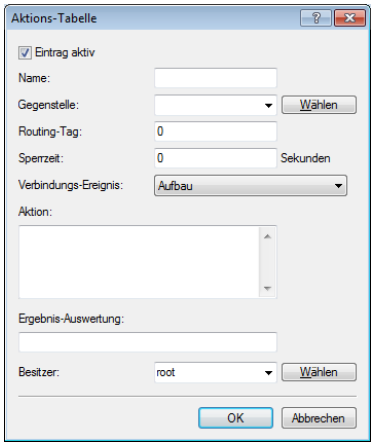
Mit zwei weiteren Cron-Befehlen `set /setup/wan/action-table/1 yes/no` wird der entsprechende Eintrag in der Aktionstabelle drei Minuten vor 3.00 Uhr aus- und drei Minuten nach 3:00 Uhr wieder eingeschaltet. Die Ziffer 1 nach dem Pfad zu Aktionstabelle steht dabei als Index für den ersten Eintrag der Tabelle.



6.17.4 Konfiguration

In der Aktions-Tabelle können Sie Aktionen definieren, die das Gerät ausführen soll, wenn sich der Zustand einer WAN-Verbindung ändert.

Im LANconfig finden Sie die Aktions-Tabelle unter **Kommunikation** > **Allgemein** > **Aktions-Tabelle**



- **Eintrag aktiv**: Aktiviert oder deaktiviert diesen Eintrag.
- **Name**: Name der Aktion. Diesen Namen können Sie mit dem Platzhalter %h (Hostname) in den Feldern **Aktion** und **Ergebnis-Auswertung** referenzieren.
- **Gegenstelle**: Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.
- **Routing-Tag**: Über das Routing-Tag bestimmen Sie, über welche Gegenstelle das Gerät die Aktion ausführt. Diese Gegenstelle muss natürlich mit dem entsprechenden Routing-Tag versehen sein.
- **Sperrzeit**: Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden (max. 10 Zeichen).
- **Verbindungs-Ereignis**: Die Aktion erfolgt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt. Mögliche Werte sind:
  - Aufbau – die Aktion erfolgt, wenn das Gerät die Verbindung erfolgreich aufgebaut hat.
  - Abbau ohne Fehler – die Aktion erfolgt, wenn das Gerät die Verbindung selbst beendet (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).
  - Ende (Abbau oder Abbruch) – die Aktion erfolgt, sobald die Verbindung beendet ist (unabhängig vom Grund für den Verbindungsabbau).
  - Abbruch mit Fehler – die Aktion erfolgt, wenn die Verbindung beendet ist, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.

- Aufbaufehler – die Aktion erfolgt, wenn ein Verbindungsaufbau nicht erfolgreich war.
- Volumen erreicht – die Aktion erfolgt, wenn das festgelegte Volumen erreicht ist.
- Volumen zurückgesetzt – die Aktion erfolgt, wenn ein Zustandswechsel von 'Volumen überschritten' zu 'Volumen nicht mehr überschritten' stattfindet; also z. B. Sie ein überschrittenes Volumen zurücksetzen oder das Gerät nach dem Überschreiten eine neue Abrechnungsperiode beginnt. Ist zum Zeitpunkt der Rücksetzung das Volumen noch nicht überschritten, erfolgt keine Aktion.

▶ **Aktion**: Hier beschreiben Sie die Aktion, die das Gerät beim Zustandswechsel der WAN-Verbindung ausführen soll. Pro Eintrag dürfen Sie nur eine Aktion angeben (max. 250 Zeichen). Für jeden der folgenden Werte ist der Doppelpunkt (:) Teil des Aktions-Wertes. Mögliche Werte sind:

- `exec:` – Mit diesem Präfix leiten Sie alle Befehle ein, wie Sie sie auch an der Telnet-Konsole eingegeben würden. Sie können z. B. mit der Aktion `exec:do /o/m/d` alle bestehenden Verbindungen beenden.
- `dnscheck:` – Mit diesem Präfix leiten Sie eine IPv4-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck:myserver.dyndns.org` die IPv4-Adresse des angegebenen Servers ermitteln.
- `dnscheck6:` – Mit diesem Präfix leiten Sie eine IPv6-DNS-Namensauflösung ein. Sie können z. B. mit der Aktion `dnscheck6:myserver.dyndns.org` die IPv6-Adresse des angegebenen Servers ermitteln.
- `http:` – Mit diesem Präfix lösen Sie eine HTTP-Get-Anfrage aus. Sie können z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei dyndns.org durchführen:

  ```
  http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
  ```

  Die Bedeutung der Platzhalter `%h` und `%a` erfahren Sie in den folgenden Absätzen.
- `https:` – Wie `http:`, nur über eine verschlüsselte Verbindung.
- `gnudip:` – Mit diesem Präfix lösen Sie eine Anfrage über das GnuDIP-Protokoll an einen entsprechenden DynDNS-Server aus. Sie können

z. B. mit der folgenden Aktion eine DynDNS-Aktualisierung bei einem DynDNS-Anbieter über das GnuDIP-Protokoll durchführen:

```
gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a
```

Die Bedeutung des Platzhalters `%a` erfahren Sie in den folgenden Absätzen.

- `repeat:` – Mit diesem Präfix und der Angabe einer Zeit in Sekunden erfolgen alle Aktionen mit der Bedingung "Aufbau" wiederholt, sobald die Verbindung aufgebaut ist. Mit der Aktion `repeat:300` erfolgen z. B. alle Aufbau-Aktionen wiederholt im fünf Minuten-Rythmus.
- `mailto:` – Mit diesem Präfix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, sobald eine Verbindung beendet ist: `mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen`.

  Mögliche Variablen zur Erweiterung der Aktionen sind:

  - `%a` – WAN-IPv4-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
  - `%z` – WAN-IPv6-Adresse der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
  - `%H` – Hostname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
  - `%h` – wie `%H`, nur Hostname in Kleinbuchstaben.
  - `%c` – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion erfolgt.
  - `%n` – Gerätename
  - `%s` – Seriennummer des Gerätes
  - `%m` – MAC-Adresse des Gerätes (wie im Sysinfo)
  - `%t` – Uhrzeit und Datum, im Format `YYYY-MM-DD hh:mm:ss`
  - `%e` – Bezeichnung des Fehlers, der bei einem nicht erfolgreichen Verbindungsaufbau gemeldet wurde.

Wichtig: Der Gebrauch der Variablen %z erfordert die Angabe der IPv6-Adresse. Wenn Sie keine Adresse bereitstellen, führt das Gerät das Skript nicht aus.

Wichtig: Die Variable %z steht ausschließlich bei nativen IPv6-WAN-Verbindungen und nicht bei Tunnel-Verbindungen (6to4, 6in4, 6rd) zur Verfügung.

Das Ergebnis der Aktionen werten Sie anschließend im Feld **Ergebnis-Auswertung** aus.

- **Ergebnis-Auswertung**: Das Ergebnis der Aktion können Sie hier auswerten, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen. Mögliche Werte für die Aktionen sind (maximal 50 Zeichen):
  - `contains=` – Dieses Präfix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
  - `isequal=` – Dieses Präfix prüft, ob das Ergebnis der Aktion der definierten Zeichenkette genau entspricht.
  - `?skipiftrue=` – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis WAHR liefert.
  - `?skipiffalse=` – Dieses Suffix überspringt die definierte Anzahl von Zeilen in der Liste der Aktionen, wenn das Ergebnis der Abfrage mit "contains" oder "isequal" das Ergebnis FALSCH liefert.

  Optionale Variablen für die Aktionen sind dieselben wie für die Aktion oben.

  Beispiel: Mit einem DNS-Check fragt das Gerät die IP-Adresse einer Adresse der Form "myserver.dyndns.org" ab. Mit der Prüfung `contains=%a?skipiftrue=2` können Sie die beiden folgenden Einträge der Aktions-Tabelle überspringen, wenn die mit dem DNS-Check ermittelte IP-Adresse mit der aktuellen IP-Adresse des Gerätes (%a) übereinstimmt.

- **Besitzer**: Besitzer der Aktion. Mit den Rechten dieses Besitzers werden die exec-Aktionen ausgeführt. Verfügt der Besitzer nicht über die notwendigen Rechte (z. B. Administratoren mit Leserechten), so kann das Gerät die Aktion nicht ausführen.

6.18 Verwendung der seriellen Schnittstelle im LAN

6.18.1 Einleitung

COM-Port-Server sind in der IT als Geräte bekannt, die Daten zwischen TCP- und seriellen Anschlüssen übertragen. Die Anwendungsmöglichkeiten sind vielfältig:

- Einbinden von Geräten mit serieller Schnittstelle, aber ohne Netzwerkschnittstelle in ein Netzwerk.
- Fernwartung von Geräten, die nur eine serielle Schnittstelle zur Konfiguration anbieten.
- Virtuelle Verlängerung einer seriellen Verbindung zwischen zwei Geräten mit serieller Schnittstelle über ein Netzwerk.

Nahezu alle Geräte verfügen über eine serielle Schnittstelle, die entweder zur Konfiguration oder zum Anschluss eines Modems genutzt werden kann. In manchen Fällen wird diese Schnittstelle jedoch für keine der beiden Möglichkeiten genutzt, ein COM-Port-Server in der Nähe des Gerätes wäre aber erwünscht. In diesen Fällen kann das Gerät seine serielle Schnittstelle als COM-Port-Server nutzen, wobei die Kosten für einen externen COM-Port-Server eingespart werden. Wenn auch der Fokus dieser Anwendung auf der seriellen Konfigurationsschnittstelle der Geräte liegt, so können je nach Modell über entsprechende CardBus- oder USB-Adapter weitere serielle Schnittstellen bereitgestellt werden, sodass in einem Gerät mehrere Instanzen des COM-Port-Servers genutzt werden können.

6.18.2 Betriebsarten

Ein COM-Port-Server kann in zwei verschiedenen Betriebsarten genutzt werden:

- Server-Modus: Der COM-Port-Server wartet auf einem definierten TCP-Port auf Anfragen zum Aufbau von TCP-Verbindungen. Diese Betriebsart wird z. B. für Fernwartungen genutzt.
- Client-Modus: Sobald ein an die serielle Schnittstelle angeschlossenes Gerät aktiv wird, öffnet der COM-Port-Client eine TCP-Verbindung zu einer

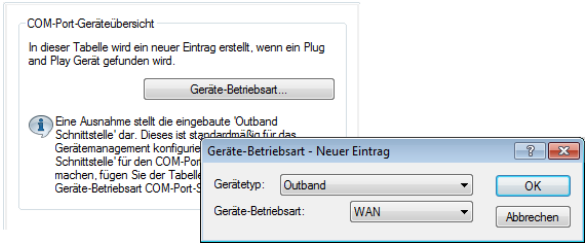
definierten Gegenstelle. Diese Betriebsart wird z. B. für Geräte genutzt, die nur über eine serielle Schnittstelle verfügen, denen aber ein Netzwerkzugang bereitgestellt werden soll.

In beiden Fällen wird eine transparente Verbindung zwischen der seriellen Schnittstelle und der TCP-Verbindung hergestellt: Datenpakete, die auf der seriellen Schnittstelle empfangen werden, werden auf der TCP-Verbindung weitergeleitet und umgekehrt. Eine häufige Anwendung im Server-Modus ist die Installation eines virtuellen COM-Port-Treibers auf der Gegenstelle, die sich mit dem COM-Port-Server verbindet. Mit einem solchen Treiber kann die TCP-Verbindung wie ein zusätzlicher COM-Port der Gegenstelle von den dort laufenden Anwendungen genutzt werden. Die Norm IETF RFC 2217 definiert entsprechende Erweiterungen des Telnet WILL/DO-Protokolls, mit denen die Anfragen zur Verhandlung der seriellen Verbindung (Bitrate, Daten- und Stopp-Bits, Handshake) an den COM-Port-Server übertragen werden können. Da die Verwendung dieses Protokolls optional ist, können im COM-Port-Server sinnvolle Defaultwerte eingestellt werden.

6.18.3 Konfiguration der seriellen Schnittstellen

Die seriellen Schnittstellen können im Gerät für verschiedene Anwendungen genutzt werden, z. B. für den COM-Port-Server oder als WAN-Schnittstelle. In der Geräte-Tabelle können den einzelnen seriellen Geräten bestimmte Anwendungen zugewiesen werden. Sobald ein HotPlug-fähiger USB-Adapter erkannt wird, wird automatisch ein neuer Eintrag für die von diesem USB-Adapter bereitgestellten seriellen Schnittstellen in dieser Tabelle erzeugt. Diese Automatik erleichert die Konfiguration der seriellen Geräte. Eine Ausnahme stellt die eingebaute serielle Schnittstelle dar, die standardmäßig zur Konfiguration genutzt wird. Um diese Schnittstelle für den COM-Port-Server oder WAN-Anwendungen zu nutzen, können in der Gerätetabelle manuell Einträge hinzugefügt werden.

LANconfig: COM-Ports / Geräte / Geräte Betriebsart



Telnet: Setup / COM-Ports / Geräte

- Device-Type

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Dienst

  Aktivierung des Ports für den COM-Port-Server.

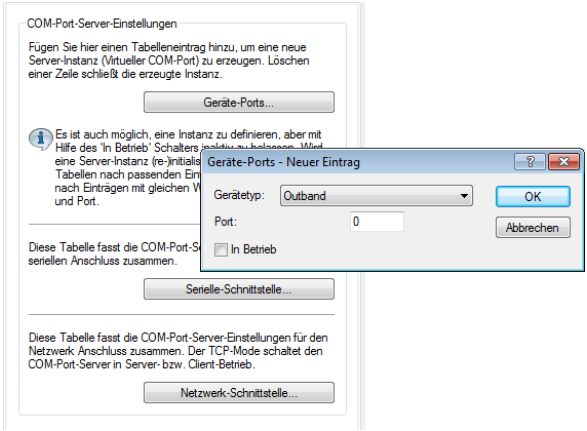
6.18.4 Konfiguration des COM-Port-Servers

Die Konfiguration des COM-Port-Servers umfasst drei Tabellen. Allen drei Tabellen gemeinsam ist die Identifikation eines bestimmten Ports auf einer seriellen Schnittstelle über die Werte Device-Type und Port-Nummer. Da manche seriellen Geräte wie z. B. eine CardBus-Karte mehrere Ports haben, muss der verwendete Port explizit angegeben werden. Bei einem Gerät mit nur einem Port wie bei der seriellen Konfigurationsschnittstelle wird die Port-Nummer auf Null gesetzt.

Betriebs-Einstellungen

Diese Tabelle aktiviert den COM-Port-Server auf einem Port einer bestimmten seriellen Schnittstelle. Fügen Sie dieser Tabelle eine Zeile hinzu, um eine neue Instanz des COM-Port-Servers zu starten. Löschen Sie eine Zeile, um die entsprechende Server-Instanz abzubrechen. Mit dem Schalter Operating kann eine Server-Instanz in der Tabelle deaktiviert werden.

Wenn eine Server-Instanz angelegt oder aktiviert wird, werden die anderen Tabellen der COM-Port-Serverkonfiguration nach Einträgen mit übereinstimmenden Werten für Device-Type und Port-Nummer durchsucht. Falls kein passender Eintrag gefunden wird, verwendet die Server-Instanz sinnvolle Default-Werte.



LANconfig: COM-Ports / Server / Geräte Ports

WEBconfig: Setup / COM-Ports / COM-Port-Server / Geraete

- Device-Type

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

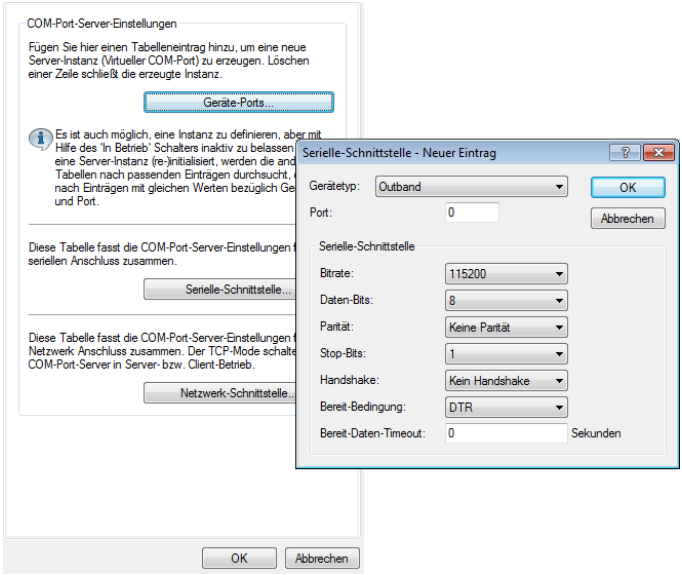
- Operating

  Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

COM-Port-Einstellungen

Diese Tabelle enthält die Einstellungen für die Datenübertragung auf der seriellen Schnittstelle.

Hinweis: Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: COM-Ports / Server / Serielle Schnittstelle

WEBconfig: Setup / COM-Ports / COM-Port-Server / COM-Port-Einstellungen

- Device-Type

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

- Bit-Rate

  Verwendete Bitrate auf dem COM-Port.

- Daten-Bits

  Anzahl der Daten-Bits.

- Paritaet

  Auf dem COM-Port verwendetes Prüfverfahren.

- Stop-Bits

  Anzahl der Stop-Bits.

- Handshake

  Auf dem COM-Port verwendete Datenflusskontrolle.

- Bereit-Bedingung

  Eine wichtige Eigenschaft eines seriellen Ports ist die Bereit-Bedingung. Der COM-Port-Server überträgt keine Daten zwischen dem seriellen Port und dem Netzwerk, solange er sich nicht im Zustand “Bereit” befindet. Außerdem wird der Wechsel zwischen den Zuständen “Bereit” und “Nicht-Bereit” verwendet, um im Client-Modus TCP-Verbindungen aufzubauen bzw. abzubrechen. Die Bereitschaft des Ports kann auf zwei verschiedene Arten ermittelt werden. Im DTR-Modus (Default) wird nur der DTR-Handshake überwacht. Die serielle Schnittstelle wird solange als bereit angesehen, wie die DTR-Leitung aktiv ist. Im Daten-Modus wird die serielle Schnittstelle als bereit betrachtet, sobald sie Daten empfängt. Wenn für die eingestellte Timeout-Zeit keine Daten empfangen werden, fällt der Port zurück in den Zustand “Nicht-Bereit”.

- Bereit-Daten-Timeout

  Der Timeout schaltet den Port wieder in den Zustand Nicht-Bereit, wenn keine Daten empfangen werden. Mit einem Timeout von Null wird diese Funktion ausgeschaltet. In diesem Fall ist der Port immer bereit, wenn der Daten-Modus gewählt ist.

Erweiterungen für die seriellen COM-Ports

Einleitung

Die Konfiguration der COM-Ports wurde um verschiedene Parameter erweitert.

Konfiguration

Die zusätzlichen Parameter befinden sich in den Netzwerkeinstellungen der COM-Ports.

WEBconfig: HiLCOS-Menübaum / Setup / COM-Ports / COM-Port-Server / Netzwerk-Einstellungen

▶ **Nehme-Binaermodus-an**

Manche Netzwerkgeräte, die an einem seriellen COM-Port angeschlossen sind, versenden Datenstrukturen, die als Steuerzeichen (CR/LF – Carriage Return / Line Feed) interpretiert werden können. In der Standardeinstellung werten die COM-Ports in den Geräten diese Informationen aus, um den Datenfluss zu steuern. Mit dem “Binärmodus” kann ein COM-Port angewiesen werden, alle Daten binär weiterzuleiten und keine Anpassungen dieser Steuerzeichen vorzunehmen.

Mögliche Werte:

– Ja, nein.

Default:

– Nein.

▶ **Newline-Konversion**

Wählen Sie hier aus, welches Zeichen auf dem seriellen Port ausgegeben wird, wenn der Binär-Modus aktiviert ist.

Die Einstellung ist abhängig von der Anwendung, die über den seriellen Port kommunizieren wird. Wenn an den Port ein weiteres Gerät angeschlossen ist, können Sie hier entweder CRLF oder nur CR wählen, da die Outband-Schnittstelle dieser Geräte ein “Carriage Return” zur automatischen Bestimmung der Datenübertragungsgeschwindigkeit erwartet. Manche Unix-Anwendungen würden CRLF allerdings als unerlaubte doppelte Zeilenschaltung interpretieren, in diesem Fall wählen Sie CR oder LF.

Mögliche Werte:

– CRLF, CR, LF

Default:

– CRLF

Hinweis: Diese Einstellung wird nur ausgewertet, wenn für diesen seriellen Port der Binär-Modus **deaktiviert** ist.

▶ **TCP-Keepalive**

Der RFC 1122 definiert ein Verfahren, mit dem die Verfügbarkeit von TCP-Verbindungen geprüft werden kann (TCP-Keepalive). Ein inaktiver Transmitter sendet nach diesem Verfahren Anfragen nach dem Empfängerstatus an die Gegenstelle. Wenn die TCP-Sitzung zur Gegenstelle verfügbar ist, antwortet diese mit ihrem Empfängerstatus. Wenn die TCP-Sitzung zur Gegenstelle nicht verfügbar ist, wird die Anfrage in einem kürzeren Intervall solange wiederholt, bis die Gegenstelle mit ihrem Empfängerstatus antwortet (danach wird wieder ein längeres Intervall verwendet). Sofern die zugrunde liegende Verbindung funktioniert, die TCP-Sitzung zur Gegenstelle allerdings nicht verfügbar ist, sendet die Gegenstelle ein RST-Paket und löst so den Abbau der TCP-Sitzung bei der anfragenden Applikation aus.

Mögliche Werte:

- inaktiv: Der TCP-Keepalive wird nicht verwendet.
- aktiv: Der TCP-Keepalive ist aktiv, nur RST-Pakete führen zum Abbau von TCP-Sitzungen.
- proaktiv: Der TCP-Keepalive ist aktiv, wiederholt die Anfrage nach dem Empfängerstatus der Gegenstelle aber nur für den als “TCP-Wdh.-Zahl” eingestellten Wert. Sofern nach dieser Anzahl von Anfragen keine Antwort mit dem Empfängerstatus vorliegt, wird die TCP-Sitzung als “nicht verfügbar” eingestuft und an die Applikation gemeldet. Wird während der Wartezeit ein RST-Paket empfangen, so löst dieses vorzeitig den Abbau der TCP-Sitzung aus.

Default:

- inaktiv

Hinweis: Für Serverapplikationen wird die Einstellung “aktiv” empfohlen.

▶ **TCP-Keepalive-Intervall**

Dieser Wert gibt an, in welchen Intervallen die Anfragen nach dem Empfängerstatus versendet werden, wenn die erste Anfrage nicht erfolgreich beantwortet wurde. Der dazu gehörende Timeout wird gebildet als Intervall / 3 (maximal 75 Sekunden).

Mögliche Werte:

- maximal 10 Ziffern

Default:

– 0

Besondere Werte:

– 0: verwendet den Standardwert nach RFC 1122 (Intervall 7200 Sekunden, Timeout 75 Sekunden).

▶ **TCP-Wdh.-Timeout**

Maximale Zeit für den Retransmission-Timeout. Dieser Timeout gibt an, in welchen Intervallen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

– 0 bis 99 Sekunden.

Besondere Werte:

– 0 verwendet den Standardwert nach RFC 1122 (60 Sekunden).

Default:

– 0

Hinweis: Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

▶ **TCP-Wdh.-Zahl**

Maximale Anzahl der Versuche, mit denen der Zustand einer TCP-Verbindung geprüft und das Ergebnis an die Applikation gemeldet wird, welche die entsprechende TCP-Verbindung nutzt.

Mögliche Werte:

– 0 bis 9

Besondere Werte:

– 0 verwendet den Standardwert nach RFC 1122 (5 Versuche).

Default:

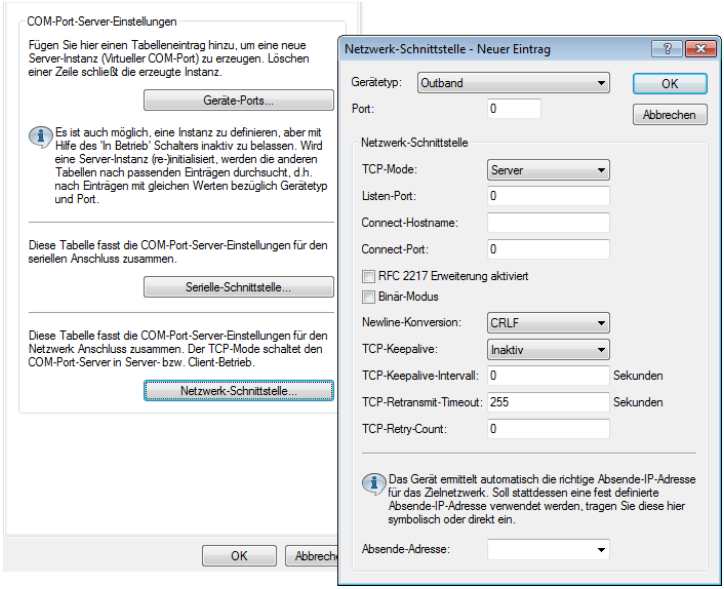
– 0

Hinweis: Die maximale Dauer der TCP-Verbindungsprüfung wird aus dem Produkt von TCP-Wdh.-Timeout und TCP-Wdh.-Zahl gebildet. Erst wenn der Timeout für alle Versuche abgelaufen ist, wird die entsprechende TCP-Anwendung informiert. Mit den Standardwerten von 60 Sekunden Timeout und maximal 5 Versuchen kann es bis zu 300 Sekunden dauern, bis eine nicht aktive TCP-Verbindung von der Applikation erkannt wird.

Netzwerk-Einstellungen

Diese Tabelle enthält alle Einstellungen, die das Verhalten des COM-Ports im Netzwerk definieren.

Hinweis: Bitte beachten Sie, dass alle diese Parameter durch die Gegenstelle überschrieben werden können, wenn die RFC2217-Verhandlung aktiviert ist; die aktuellen Einstellungen können im Status-Menü eingesehen werden.



LANconfig: COM-Ports / Server / Netzwerk-Schnittstelle

WEBconfig: Setup / COM-Ports / COM-Port-Server / Netzwerk-Einstellungen

- Device-Type

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Manche seriellen Geräte wie z. B. die CardBus haben mehr als einen seriellen Port. Tragen Sie hier die Nummer des Ports ein, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt werden soll.

- TCP-Modus

  Jede Instanz des COM-Port-Servers überwacht im Server-Modus den definierten Listen-Port auf eingehende TCP-Verbindungen. Pro Instanz ist nur eine aktive Verbindung erlaubt, alle anderen Verbindungsanfragen werden abgelehnt. Im Client-Modus versucht die Instanz eine TCP-Verbindung über einen definierten Port zur angegebenen Gegenstelle aufzubauen, sobald der Port bereit ist. Die TCP-Verbindung wird wieder geschlossen, sobald der Port nicht mehr bereit ist. In beiden Fällen schließt ein Gerät die offenen Verbindungen bei einem Neustart des Gerätes.

- Listen-Port

  Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

- Aufbau-Host-Name

  Zu diesem Host baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand “Bereit” befindet.

- Aufbau-Port

  Über diesen TCP-Port baut der COM-Port im TCP-Client-Modus eine Verbindung auf, sobald sich der Port im Zustand “Bereit” befindet.

- Loopback-Adresse

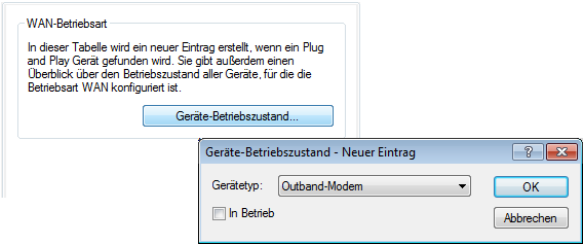
  Über diese Adresse kann der COM-Port angesprochen werden. Dies ist die eigene IP-Adresse, die als Quelladresse beim Verbindungsaufbau benutzt wird. Sie wird z. B. verwendet, um die IP-Route festzulegen, über die die Verbindung aufgebaut wird.

- RFC2217-Erweiterungen

  Die RFC2217-Erweiterungen können für beide TCP-Modi aktiviert werden. Wenn diese Erweiterungen eingeschaltet sind, signalisiert ein Gerät seine Bereitschaft, Telnet Steuerungssequenzen zu akzeptieren, mit der Sequenz IAC DO COM-PORT-OPTION. In der Folge werden auf dem COM-Port die entsprechenden Optionen verwendet, die konfigurierten Default-Werte werden überschrieben. Außerdem versucht der Port, für Telnet das lokale Echo und den Line Mode zu verhandeln. Die Verwendung der RFC2217-Erweiterungen ist auch bei nicht kompatibler Gegenstelle unkritisch, möglicherweise werden dann unerwartete Zeichen bei der Gegenstelle angezeigt. Als Nebeneffekt führt die Verwendung der RFC2217-Erweiterungen dazu, dass der Port einen regelmäßigen Alive-Check durchführt, indem Telnet-NOPs zur Gegenstelle gesendet werden.

6.18.5 Konfiguration der WAN-Geräte

Die Tabelle mit den WAN-Geräten dient nur als Status-Tabelle. Alle Hotplug-Geräte (über USB oder CardBus angeschlossen) tragen sich selbst in diese Tabelle ein.



LANconfig: COM-Ports / WAN / Geräte-Betriebszustand

WEBconfig: Setup / COM-Ports / WAN / Geraete

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Aktiv

  Status des angeschlossenen Gerätes:

6.18.6 Status-Informationen über die seriellen Verbindungen

Für jede Instanz des COM-Port-Servers werden verschiedene Statistiken und Zustandswerten erfasst. Der serielle Port, den die Instanz verwendet, wird in den beiden ersten Spalten der Tabelle angegeben – hier werden die bei der Konfiguration eingetragenen Werte für Device-Type und Port-Nummer angezeigt.

Netzwerk-Status

Telnet: Status / COM-Ports / COM-Port-Server / Netzwerk-Status

Diese Tabelle enthält alle Informationen über die aktuellen und die vorherigen TCP-Verbindungen.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Connection-Status

  Mögliche Werte:

  - Verbunden: Eine Verbindung ist aktiv (Server- oder Client-Modus).
  - Hoerend: Diese Instanz arbeitet im Server-Modus, derzeit ist keine TCP-Verbindung aktiv.
  - Nicht-hoerend: Im Server-Modus konnte der angegebene TCP-Port nicht für eingehende Verbindungen reserviert werden, z. B. weil er bereits von einer anderen Applikation belegt ist.
  - Leer: Diese Instanz arbeitet im Client-Modus und der Port ist nicht bereit, daher wird derzeit keine TCP-Verbindung aufgebaut.
  - Verbinden: Der Port hat den Zustand “Bereit” erreicht, es wird eine Verbindung aufgebaut.

- Last-Error

  Zeigt im Client-Modus den Grund für den letzten Verbindungsfehler an. Im Server-Modus hat dieser Wert keine Bedeutung.

- Remote-Address

  Zeigt die IP-Adresse der Gegenstelle bei einer erfolgreichen TCP-Verbindung an.

- Local-Port

  Zeigt den verwendeten lokalen TCP-Port bei einer erfolgreichen TCP-Verbindung an.

- Remote-Port

  Zeigt den verwendeten entfernten TCP-Port bei einer erfolgreichen TCP-Verbindung an.

COM-Port-Status

Diese Tabelle zeigt den Zustand des seriellen Ports und die auf diesem Port aktuell verwendeten Einstellungen.

- Device-Type

Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Port-Status

  Mögliche Werte:

  - Nicht-Vorhanden: Der serielle Port ist derzeit nicht für den COM-Port-Server verfügbar, z. B. weil der USB- oder CardBus-Adapter entfernt wurde oder weil die Schnittstelle von einer anderen Funktion des Geräts verwendet wird.
  - Nicht-Bereit: Der serielle Port ist prinzipiell für den COM-Port-Server verfügbar, derzeit aber nicht bereit für eine Datenübertragung, z. B. weil die DTR-Leitung nicht aktiv ist. Im Client-Zustand wird kein Verbindungsaufbau versucht, solange der Port in diesem Zustand ist.
  - Bereit: Der serielle Port ist verfügbar und bereit für eine Datenübertragung. Im Client-Zustand wird versucht, eine TCP-Verbindung aufzubauen, sobald der Port in diesem Zustand ist.

  Hinweis: Bitte beachten Sie, dass der Port-Status auch im Server-Modus von Bedeutung ist. Alle TCP-Verbindungsanfragen werden akzeptiert, allerdings wird die COM-Port-Instanz erst dann Daten zwischen dem seriellen Port und dem Netzwerk übertragen, wenn der serielle Port den Zustand “Bereit” erreicht hat. Die folgenden Spalten zeigen die Einstellungen, die auf dem seriellen Port aktuell verwendet werden. Sie entsprechen entweder den konfigurierten Werten oder den Werten, die bei der Verhandlung über die RFC2217-Erweiterungen ermittelt wurden.

- Bit-Rate

  Verwendete Bitrate auf dem COM-Port.

- Daten-Bits

  Anzahl der Daten-Bits.

- Paritaet

  Auf dem COM-Port verwendetes Prüfverfahren.

- Stop-Bits

  Anzahl der Stop-Bits.

- Handshake

  Auf dem COM-Port verwendete Datenflusskontrolle.

Byte-Counters

In dieser Tabelle werden die eingehenden und ausgehenden Datenpakete auf dem seriellen Port und der Netzwerk-Seite angezeigt.

Hinweis: Diese Werte werden nicht zurückgesetzt, wenn der entsprechende Anschluss geöffnet oder geschlossen wird.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Seriell-Tx

  Anzahl der auf der seriellen Schnittstelle gesendeten Bytes.

- Seriell-Rx

  Anzahl der auf der seriellen Schnittstelle empfangenen Bytes.

- Netzwerk-Tx

  Anzahl der auf der Netzwerkseite gesendeten Bytes.

- Netzwerk-Rx

  Anzahl der auf der Netzwerkseite empfangenen Bytes.

Port-Errors

In dieser Tabelle werden die Fehler auf dem seriellen Port angezeigt. Diese Fehler können auf ein fehlerhaftes Kabel oder auf Fehler in der Konfiguration hinweisen.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Paritaets-Fehler

  Anzahl der Fehler aufgrund einer nicht übereinstimmenden Prüfsumme.

- Rahmen-Fehler

  Anzahl der fehlerhaften Datenpakete.

Verbindungen

In dieser Tabelle werden die erfolgreichen und gescheiterten TCP-Verbindungen angezeigt, sowohl im Server wie auch im Client-Modus.

- Device-Type

  Liste der im Gerät verfügbaren seriellen Schnittstellen.

- Port-Nummer

  Nummer des Ports, der auf der seriellen Schnittstelle für den COM-Port-Server genutzt wird.

- Server-gestattet

  Anzahl der Verbindungen, die der COM-Port-Server gestattet hat.

- Server-abgelehnt

  Anzahl der Verbindungen, die der COM-Port-Server abgelehnt hat.

- Client-erfolgreich

Anzahl der Verbindungen, die der COM-Port-Client erfolgreich aufgebaut hat.

- Client-DNS-Fehler

  Anzahl der Verbindungen, die der COM-Port-Client aufgrund von DNS-Fehlern nicht aufbauen konnte.

- Client-TCP-Fehler

  Anzahl der Verbindungen, die der COM-Port-Client aufgrund von TCP-Fehlern nicht aufbauen konnte.

- Client-Gegenstelle-getrennt

  Anzahl der Verbindungen, bei denen der COM-Port-Client von der Gegenstelle getrennt wurde.

Delete-Values

Diese Aktion löscht alle Werte in den Status-Tabellen.

6.18.7 COM-Port-Adapter

Zum Anschluss von Geräten mit seriellen Schnittstellen an ein Geräten stehen folgende Möglichkeiten bereit:

Adapter	*Geräte*
COM-Port-Adapter	Alle mit serieller Konfigurationsschnittstelle
USB-Seriell-Adapter	Alle mit USB-Schnittstelle
CardBus-Seriell-Adapter	Alle mit CardBus-Einschub

Der COM-Port-Adapter muss als beidseitiger Sub-D Stecker mit folgender PIN-Belegung ausgeführt werden:

Pin	*Signal*	*Signal*	*Pin*
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5

Pin	*Signal*	*Signal*	*Pin*
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

6.19 IGMP Snooping

6.19.1 Einleitung

Alle Geräte mit WLAN-Schnittstellen verfügen über eine “LAN-Bridge”, die für die Übertragung der Daten zwischen den Ethernet-Ports und den WLAN-Schnittstellen sorgen. Die LAN-Bridge arbeitet dabei in vielen Aspekten wie ein Switch. Die zentrale Aufgabe eines Switches – im Gegensatz zu einem Hub – besteht darin, Pakete nur an den Port weiterzuleiten, an dem der Empfänger angeschlossen ist. Dazu bildet der Switch automatisch aus den eingehenden Datenpaketen eine Tabelle, in der die Absender-MAC-Adressen den Ports zugeordnet werden.

Wenn eine Ziel-Adresse eines eingehenden Pakets in dieser Tabelle gefunden wird, kann der Switch das Paket gezielt an den richtigen Port weiterleiten. Wird die Ziel-Adresse nicht gefunden, so leitet der Switch das Paket an alle Ports weiter. D.h. ein Switch kann ein Paket nur dann zielgerichtet weiterleiten, wenn die Zieladresse schon einmal als Absenderadresse eines Pakets über einen bestimmten Port bei ihm eingegangen ist. Broadcast- oder Multicast-Pakete können aber niemals als Absenderadresse in einem Paket eingetragen sein, darum werden diese Pakete immer auf alle Ports “geflutet”.

Während dieses Verhalten für Broadcasts die richtige Aktion ist (Broadcasts sollen schließlich alle möglichen Empfänger erreichen), ist es für Multicasts nicht unbedingt die gewünschte Lösung. Multicasts richten sich in der Regel an eine bestimmte Gruppe von Empfängern in einem Netzwerk, nicht aber an alle:

- Videostreams werden z. B. häufig als Multicast übertragen, aber nicht alle Stationen im Netzwerk sollen einen bestimmten Stream empfangen.

- Verschiedene Anwendungen im medizinischen Bereich nutzen Multicasts, um Daten an bestimmte Endgeräte zu übertragen, die nicht an allen Stationen eingesehen werden sollen.

Bei einer LAN-Bridge im Gerät wird es daher auch Ports geben, an denen kein einziger Empfänger des Multicasts angeschlossen ist. Das “überflüssige” Versenden der Multicasts auf Ports ohne Empfänger ist zwar kein Fehler, es führt aber zu Performance-Problemen:

- Viele Stationen können die unerwünschten Multicasts nicht in der Hardware der Netzwerkadapter aussortieren, sondern reichen die Pakete einfach an die höher gelegenen Protokollschichten weiter, was zu einer höheren Belastung der CPU führt.
- Gerade in WLANs kann die unnötige Aussendung der Multicasts zu einer deutlichen Einschränkung der verfügbaren Bandbreite führen, wenn keiner der angemeldeten WLAN-Clients Bedarf für den Multicast hat.

Mit dem Internet Group Management Protocol (IGMP) stellt die TCP/IP-Protokollfamilie ein Protokoll bereit, mit dem die Netzwerkstationen dem Router, an dem sie angeschlossen sind, das Interesse an bestimmten Multicasts mitteilen können. Dazu registrieren sich die Stationen bei den Routern für bestimmte Multicast-Gruppen, von denen Sie die entsprechenden Pakete beziehen wollen (Multicast-Registration). IGMP nutzt dazu spezielle Nachrichten zum Anmelden (Join-Messages) und Abmelden (Leave-Messages).

Hinweis: Die Information, in welchen Multicast-Gruppen sich eine Station registrieren kann oder soll, erhält die Station über andere Protokolle außerhalb von IGMP.

IGMP kann als Layer-3-Protokoll nur IP-Subnetze entsprechend der Anmeldungen an Multicast-Gruppen verwalten. Die in den Netzwerkstrukturen vorhandenen Geräte wie Bridges, Switches oder WLAN Access Points leiten die Pakete aber oft nur auf Layer 2 weiter, so dass IGMP zunächst keine Funktionen bietet, um die Pakete zielgerichtet durch diese Netzwerkstrukturen zu leiten. Die Bridges nutzen daher die Multicast-Registrierung zwischen Stationen und Routern, um zusätzliche Informationen über die zielgerichtete Verteilung der Multicasts zu erhalten. IP-Multicasts müssen nur an die Ports weitergeleitet werden, an denen sich ein Router befindet, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetzen weiterleiten kann. Dieses Verfahren wird als IGMP Snooping bezeichnet. Die Bridges, die eigentlich die Entschei-

dung für das Weiterleiten der Pakete anhand der MAC auf Layer 2 treffen, nutzen damit zusätzlich die Layer 3-Informationen der IP-Multicast-Pakete.

Für die weitere Beschreibung der Funktionen des IGMP Snooping im HiLCOS werden zwei wesentliche Begriffe unterschieden:

- Ein Port ist “Mitglied einer Multicast-Gruppe”, wenn mindestens eine daran angeschlossene Station Pakete für eine bestimmte Multicast-Adresse empfangen möchte. Diese Multicast-Registrierung kann sowohl dynamisch über IGMP Snooping gelernt wie auch manuell konfiguriert sein.
- Ein Port ist ein “Router-Port”, wenn daran ein Router angeschlossen ist, der Multicast-Routing beherrscht und die Pakete in bestimmte IP-Subnetzen weiterleiten kann.
- Eine Multicast-Gruppe ist “nicht registriert”, wenn kein Port der Bridge Mitglied dieser Multicast-Gruppe ist.

6.19.2 Ablauf des IGMP Snooping

Beim Empfang eines Pakets unterscheidet die Bridge zunächst, ob es sich um einen Broadcast, Multicast oder Unicast handelt. Broadcasts und Unicasts werden wie üblich weitergeleitet, d. h. entweder auf alle Ports oder nur auf den Port, an den entsprechend des Eintrags in der MAC-Tabelle der Empfänger angeschlossen ist.

Für die IP-Multicast-Pakete werden zwei Typen unterschieden (abgeschnittene Pakete oder Pakete mit ungültiger Prüfsumme werden dabei verworfen):

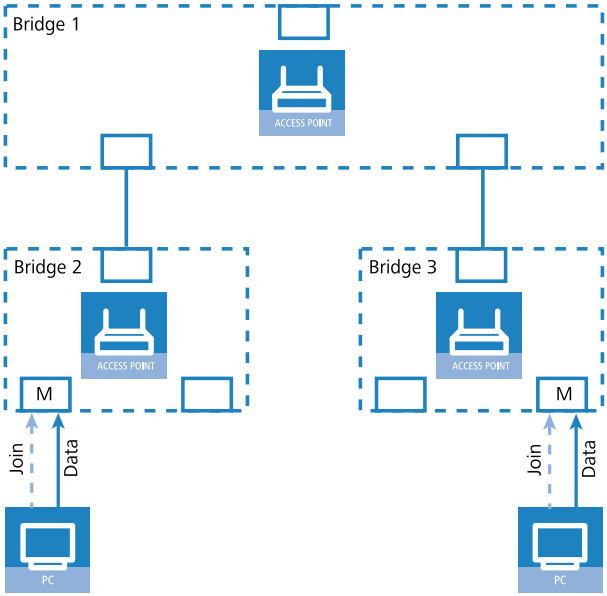
- IGMP-Nachrichten werden je nach Inhalt unterschiedlich behandelt:
  - Eine Join-Message führt dazu, dass der Port, über den das Paket eingeht, Mitglied der entsprechenden Multicast-Gruppe wird. Diese Nachricht wird nur an Router-Ports weitergeleitet.
  - Entsprechend führt eine Leave-Message dazu, dass der Port, über den das Paket eingeht, aus der entsprechenden Multicast-Gruppe entfernt wird. Auch diese Nachricht wird nur an Router-Ports weitergeleitet.
  - Eine eingehende IGMP-Anfrage macht den Port zu einem Router-Port. Diese Nachrichten werden an alle Ports weitergeleitet.
  - Alle anderen IGMP-Nachrichten werden an alle Ports weitergeleitet – dabei werden keine der Port-Eigenschaften geändert.
- Wenn es sich bei einem IP-Multicast-Paket nicht um eine IGMP-Nachricht handelt, wird die Ziel-Adresse ausgewertet. Pakete für die Zieladresse

“224.0.0.x“ werden dabei an alle Ports weitergeleitet, weil dieser “reservierte” Bereich von Protokollen ohne richtige IGMP-Registrierung verwendet wird. Für alle anderen Pakete wird die Zieladresse in der Tabelle der IGMP-Mitgliedschaften ermittelt:

- Wenn die Adresse gefunden wird, wird das Paket an die entsprechenden Ports weitergeleitet.
- Wenn die Adresse nicht gefunden wird, wird das Paket je nach Konfiguration entweder verworfen, an alle Ports oder ausschließlich an alle Router-Ports weitergeleitet.

6.19.3 IGMP Snooping über mehrere Bridges hinweg

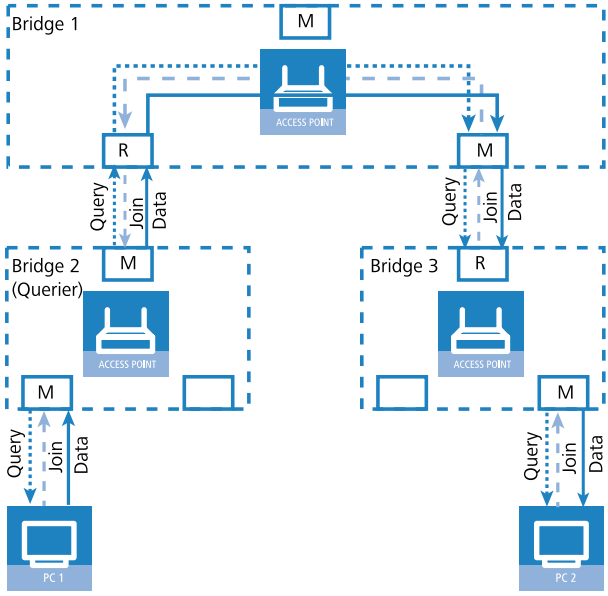
Wie beschrieben leitet IGMP Snooping eingehende Join- oder Leave-Nachrichten nur über Router-Ports weiter. In einer Struktur mehrerer Bridges sind zu Beginn alle Ports weder Router-Port noch Mitglied einer Multicast-Gruppe. Wenn sich die an den Bridges angeschlossenen Stationen für eine Multicast-Gruppe registrieren, wird der verwendete Port automatisch Mitglied dieser Gruppe. In dieser Phase ist allerdings keiner der Ports als Router-Port aktiviert, daher werden die Join-Nachrichten auch nicht an andere Bridges weitergeleitet. Die übergeordneten Bridges erfahren also nichts von der Mitgliedschaft des Ports in der gewünschten Multicast-Gruppe.



Die Bridges müssen also über Router-Ports verfügen, damit sich die Informationen über die Mitgliedschaften in Multicast-Gruppen verbreiten können. Da die Ports der Bridge nur durch IGMP-Anfragen zu Router-Ports werden können, muss einer der Multicast-fähigen Router im Netzwerk die Aufgabe übernehmen, die benötigten IGMP-Anfragen in Netzwerk zu streuen. Dieser Router wird auch als IGMP-Querier bezeichnet. Für den Fall, dass kein Multicast-Router im Netzwerk vorhanden ist, können die Access Points einen Querier simulieren. Um parallele Anfragen von unterschiedlichen Querier-Instanzen zu vermeiden, schaltet sich eine Querier-Instanz ab, wenn ein anderer Querier mit niedrigerer IP-Adresse gefunden wird. Die Verteilung der IGMP-Informationen durch den Querier lässt sich an folgendem Beispiel erklären:

1. Der Querier (im Beispiel Bridge 2) sendet in regelmäßigen Abständen IGMP-Anfragen über alle verfügbaren Ports aus (gepunktete Linien). Diese Anfragen kennzeichnen in der nächsten Bridge (Bridge 1) den Port, auf dem die Anfrage eingeht, als Router-Port (R). PC 1 antwortet auf diese Anfrage mit einer Join-Nachricht für alle Multicast-Gruppen (helle gestrichelte Linien), in welchen diese Station sich registrieren möchte. Der Port, an dem PC 1 an Bridge 2 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).

2. Außerdem versendet diese Bridge 1 die Anfragen über alle anderen Ports an angeschlossene Bridges und Stationen weiter unten in der Struktur. In Bridge 3 wird der Port, über den die Anfrage eingeht, dadurch zum Router-Port (R).
3. Auch die an Bridge 3 angeschlossene Station (PC 2) antwortet auf diese Anfrage mit einer Join-Nachricht für alle registrierten Multicast-Gruppen. Der Port, an dem PC 2 an Bridge 3 angeschlossen ist, wird damit Mitglied der entsprechenden Multicast-Gruppe(n).
4. Bridge 3 leitet diese Join-Nachricht über den Router-Port weiter an Bridge 1. Der empfangende Port von Bridge 1 wird damit auch Mitglied der Multicast-Gruppen, für die sich PC 2 registriert hat.
5. Im letzten Schritt leitet Bridge 1 die Join-Nachricht von PC 2 über den Router-Port weiter an Bridge 2, wo der empfangende Port ebenfalls Mitglied der Multicast-Gruppen von PC 2 wird.

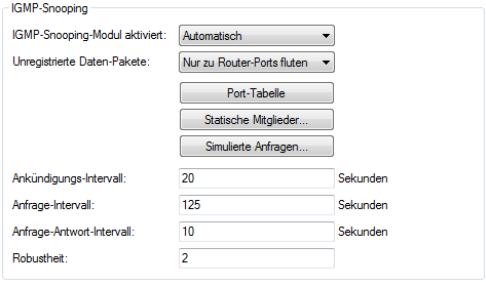


Wenn nun PC 1 einen Multicast aussendet für eine der von PC 2 registrierten Multicast-Gruppen, leiten alle Bridges (2, 1 und dann 3) die Pakete jeweils über den Mitglieds-Port weiter bis zu PC 2.

6.19.4 Konfiguration

Allgemeine Einstellungen

Die Konfiguration des IGMP-Snooping finden Sie im LANconfig unter **Schnittstellen** > **IGMP-Snooping**



IGMP-Snooping-Modul aktiviert

Aktiviert oder deaktiviert IGMP Snooping für das Gerät und alle definierten Querier-Instanzen. Ohne IGMP-Snooping verhält sich die Bridge wie ein einfacher Switch und sendet alle Multicasts auf alle Ports weiter.

Mögliche Werte:

- Ja
- Nein
- Automatisch

Default:

- Automatisch

In der Einstellung **Automatisch** aktiviert die Bridge das IGMP-Snooping nur, wenn auch Querier im Netz vorhanden sind.

Hinweis: Wenn diese Funktion deaktiviert ist, sendet die Bridge alle IP-Multicast-Pakete über alle Ports. Bei einer Änderung des Betriebszustandes setzt die Bridge die IGMP-Snooping-Funktion vollständig zurück, d. h. sie löscht alle dynamisch gelernten Werte (Mitgliedschaften, Router-Port-Eigenschaften).

Unregistrierte Datenpakete

Diese Option definiert die Verarbeitung von Multicast-Paketen mit Ziel-Adressen außerhalb des reservierten Adress-Bereiches `224.0.0.x`, für die weder dynamisch gelernte noch statisch konfigurierte Mitgliedschaften vorhanden sind.

Mögliche Werte:

- Nur zu Router-Ports fluten: Sendet diese Pakete an alle Router-Ports.
- Zu allen Ports fluten: Sendet diese Pakete an alle Ports.
- Verwerfen: Verwirft diese Pakete.

Default:

- Nur-Router-Ports

Ankündigungs-Intervall

Das Intervall in Sekunden, in dem die Geräte Pakete aussenden, mit denen sie sich als Multicast-fähige Router bekanntmachen. Aufgrund dieser Information können andere IGMP-Snooping-fähige Geräte schneller lernen, welche ihrer Ports Sie als Router-Ports verwenden sollen. Beim Aktivieren von Ports kann ein Switch z. B. eine entsprechende Anfrage nach Multicast-Routern versenden, die der Router mit einer solchen Bekanntmachung beantworten kann. Diese Methode ist je nach Situation ggf. deutlich schneller als die alternative Lernmöglichkeit über die IGMP-Anfragen.

Mögliche Werte:

- 4 bis 180 Sekunden

Default:

- 20

Anfrage-Intervall

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) IGMP-Anfragen an die Multicast-Adresse `224.0.0.1` schickt und damit Rückmeldungen der Stationen über die Mitgliedschaft in Multicast-Gruppen auslöst. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Bridge die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" lässt und löscht.

- Ein Querier sendet nach der Anfangsphase IGMP-Anfragen in diesem Intervall.
- Ein Querier kehrt zurück in den Querier-Status nach einer Zeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".
- Ein Router-Port verliert seine Eigenschaften nach einer Alterungszeit von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)".

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 125

Hinweis: Das Anfrage-Intervall muss größer als das Anfrage-Antwort-Intervall sein.

Anfrage-Antwort-Intervall

Intervall in Sekunden, beeinflusst das Timing zwischen den IGMP-Anfragen und dem Altern der Router-Ports bzw. Mitgliedschaften.

Intervall in Sekunden, in dem ein Multicast-fähiger Router (oder ein simulierter Querier) Antworten auf seine IGMP-Anfragen erwartet. Diese regelmäßigen Abfragen beeinflussen den Zeitpunkt, nach dem die Mitgliedschaft in bestimmten Multicast-Gruppen "altern" und gelöscht werden.

Mögliche Werte:

- Zahl aus 10 Ziffern größer als 0.

Default:

- 10

Hinweis: Das Anfrage-Antwort-Intervall muss kleiner als das Anfrage-Intervall sein.

Robustheit

Dieser Wert bestimmt die Robustheit des IGMP-Protokolls. Diese Option toleriert den Paketverlust von IGMP-Anfragen gegenüber den Join-Nachrichten.

Mögliche Werte:

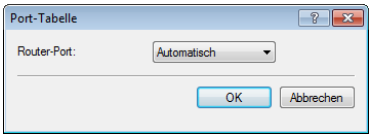
- Zahl aus 10 Ziffern größer als 0.

Default:

- 2

Port-Einstellungen

In dieser Tabelle können Sie die Port-bezogenen Einstellungen für IGMP Snooping vornehmen.



Port

Auf diesen Port geziehen sich die Einstellungen.

Mögliche Werte:

- Auswahl aus der Liste der im Gerät verfügbaren Ports.

Default:

- N/A

Router-Port

Diese Option definiert das Verhalten des Ports.

Mögliche Werte:

- Ja: Dieser Port verhält sich immer wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Nein: Dieser Port verhält sich nie wie ein Router-Port, unabhängig von den IGMP-Anfragen oder Router-Meldungen, die die Bridge auf diesem Port evtl. empfängt.
- Automatisch: Dieser Port verhält sich wie ein Router-Port, wenn eine IGMP-Anfragen oder Router-Meldung empfangen wurde. Der Port verliert diese Eigenschaft wieder, wenn die Bridge auf diesem Port für

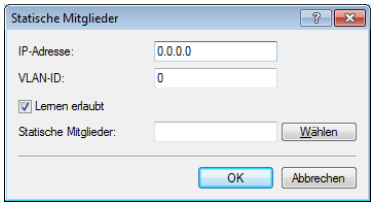
die Dauer von "Robustheit*Anfrage-Intervall+(Anfrage-Antwort-Intervall/2)" keine entsprechenden Pakete empfängt.

Default:

- Automatisch

Statische-Mitglieder

Diese Tabelle erlaubt die manuelle Definition von Mitgliedschaften, die z. B. nicht automatisch gelernt werden können oder sollen.



IP-Adresse

Die IP-Adresse der manuell definierten Multicast-Gruppe.

Mögliche Werte:

- Gültige IP-Multicast-Adresse.

Default:

- 0.0.0.0

VLAN-ID

Die VLAN-ID, auf welche die Bridge diese statische Mitgliedschaft anwenden soll. Für eine IP-Multicast-Adresse können Sie durchaus mehrere Einträge mit unterschiedlichen VLAN-IDs eintragen.

Mögliche Werte:

- 0 bis 4096.

Default:

- 0

Besondere Werte:

- Wenn “0” als VLAN gewählt wird, werden die IGMP-Anfragen ohne VLAN-Tag ausgegeben. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

Lernen erlaubt

Mit dieser Option aktivieren Sie das automatische Lernen von Mitgliedschaften für diese Multicast-Gruppe. Wenn das automatische Lernen deaktiviert ist, verschickt die Bridge die Pakete nur über die für die Multicast-Gruppe manuell definierten Ports.

Mögliche Werte:

- aktiviert
- deaktiviert

Default:

- Aktiviert

Statische Mitglieder

An diese Ports stellt die Bridge die Pakete mit der entsprechenden IP-Multicast-Adresse immer zu, unabhängig von empfangenen Join-Nachrichten.

Mögliche Werte:

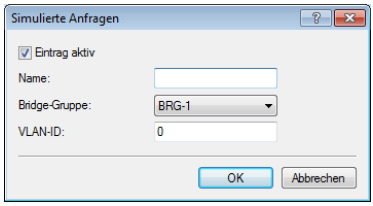
- Kommaseparierte Liste der gewünschten Ports, maximal 215 alphanumerische Zeichen.

Default:

- Leer

Simulierte-Anfrager

Diese Tabelle enthält alle im Gerät definierten simulierten Querier. Diese Einheiten werden eingesetzt, wenn kein Multicast-Router im Netzwerk vorhanden ist, aber dennoch die Funktionen des IGMP-Snooping benötigt werden. Um die Querier auf bestimmte Bridge-Gruppen oder VLANs einzuschränken, können Sie mehrere unabhängige Querier definieren, welche dann die entsprechenden VLAN-IDs nutzen.



Eintrag aktiv

Aktiviert oder deaktiviert die Querier-Instanz.

Mögliche Werte:

- Aktiviert
- Deaktiviert

Default:

- Aktiviert

Name

Name der Querier-Instanz.

Mögliche Werte:

- 8 alphanumerische Zeichen.

Default:

- Leer

Bridge-Gruppe

Schränkt die Querier-Instanz auf eine bestimmte Bridge-Gruppe ein.

Mögliche Werte:

- Auswahl aus der Liste der verfügbaren Bridge-Gruppen
- keine

Default:

- BRG-1

Besondere Werte:

- Ist "keine" Bridge-Gruppe gewählt, gibt die Bridge die IGMP-Anfragen auf allen Brigde-Gruppen aus.

VLAN-ID

Schränkt die Querier-Instanz auf ein bestimmtes VLAN ein.

Mögliche Werte:

- 0 bis 4096

Default:

- 0

Besondere Werte:

- Ist "0" als VLAN-ID gewählt, gibt die Bridge die IGMP-Anfragen ohne VLAN-Tag aus. Dieser Wert ist daher nur sinnvoll, wenn die Verwendung von VLAN generell deaktiviert ist.

6.19.5 IGMP Status

Allgemeine Statistiken

Die Status-Meldungen zu IGMP Snooping finden Sie auf folgenden Pfaden:

WEBconfig: HiLCOS-Menübaum / Status / LAN-Bridge-Statistiken / IGMP-Snooping

- In-Betrieb

  Zeigt an, ob das IGMP Snooping aktiviert oder deaktiviert ist.

- IPv4-Pakete

  Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

- Daten-Pakete

  Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf allen Ports empfangen wurden, und bei denen es sich nicht um IGMP-Pakete handelt.

- Steuer-Pakete

Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf allen Ports empfangen wurden.

- Defekte-Pakete

  Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-Pakete, die auf allen Ports empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.

  Hinweis: Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP/UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

- Werte-loeschen

  Diese Aktion löscht alle Statistik-Einträge.

Port-Status

Diese Tabelle zeigt alle Port-bezogenen Statistiken.

WEBconfig: HiLCOS-Menübaum / Status / LAN-Bridge-Statistiken / IGMP-Snooping / Port-Status

- Router-Port

  Zeigt an, ob der Port derzeit als Router-Port genutzt wird oder nicht, unabhängig davon, ob dieser Zustand statisch konfiguriert oder dynamisch gelernt wurde.

- IPv4-Pakete

  Zeigt die gesamte Anzahl der IPv4-Multicast-Pakete, die auf diesem Port empfangen wurden, unabhängig davon, ob es sich um IGMP-Pakete handelt oder nicht.

- Daten-Pakete

Zeigt die gesamte Anzahl der nicht beschädigten IPv4-Multicast-Pakete, die auf diesem Port empfangen wurdenund bei denen es sich nicht um IGMP-Pakete handelt.

- Steuer-Pakete

  Zeigt die gesamte Anzahl der nicht beschädigten IGMP-Pakete, die auf diesem Port empfangen wurden.

- Defekte-Pakete

  Zeigt die gesamte Anzahl der beschädigten Daten- oder IGMP-Pakete, die auf diesem Port empfangen wurden. Mögliche Ursachen für die Beschädigung der Pakete sind IP-Prüfsummenfehler oder abgeschnittene Pakete.

  Hinweis: Aus Performance-Gründen werden IP-Prüfsummen nur für IGMP-Pakete ausgewertet, nicht für den Datenteil der Multicast-Pakete. Daher werden Pakete mit einer fehlerhaften Prüfsumme im TCP/UDP- oder IP-Header nicht erkannt. Diese Pakete werden als Datenpakete gezählt.

Gruppen

Diese Tabelle zeigt alle dem Gerät bekannten Mitgliedschaften von Multicast-Gruppen, unabhängig davon, ob sie statisch konfiguriert oder dynamisch gelernt wurden. Wenn für eine Multicast-Gruppe sowohl statische als auch dynamische Mitgliedschaften existieren, werden diese in separaten Einträgen angezeigt.

WEBconfig: HiLCOS-Menübaum / Status / LAN-Bridge-Statistiken / IGMP-Snooping / Gruppen

- Adresse

  Zeigt die IP-Multicast-Adresse der Gruppe.

- VLAN-Id

  Zeigt die VLAN-ID, für welche dieser Eintrag gültig ist.

- Lernen-erlauben

Zeigt an, on für die Gruppe neue Mitgliedschaften dynamisch gelernt werden dürfen oder nicht.

- Statische-Mitglieder

  Zeigt die Liste der statisch für die Gruppe definierten Mitglieder.

- Dynamische-Mitglieder

  Zeigt die Liste der dynamisch für die Gruppe gelernten Mitglieder.

Simulierte-Anfrager

Die Tabelle zeigt den Status aller definierten und aktiven IGMP-Querier-Instanzen.

- Name

  Zeigt den Namen der Multicast-Gruppe.

- Bridge-Gruppe

  Zeigt die Bridge-Gruppe, für welche dieser Eintrag gültig ist.

- VLAN-Id

  Zeigt das VLAN, für welches dieser Eintrag gültig ist.

- Status

  Zeigt den Status des Eintrags.

  - Initial: Die Querier-Instanz wurde gerade gestartet und sendet IGMP-Anfragen in kurzen Intervallen (viermal schneller als das definierte Anfrage-Intervall).
  - Querier: Die Querier-Instanz betrachtet sich selbst als den aktiven Querier und sendet IGMP-Anfragen in den als Anfrage-Intervall definierten Abständen.
  - Non-Querier: Eine andere Querier-Instanz mit einer niedrigeren IP-Adresse wurde erkannt, die hier aufgeführte Instanz sendet keine IGMP-Anfragen.

6.20 Konfiguration des WWAN-Zugriffs

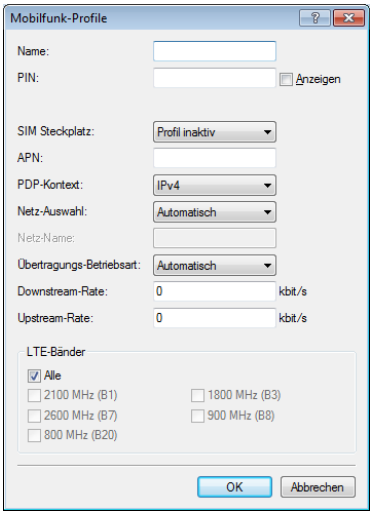
Das nachfolgende Tutorial zeigt Ihnen, wie Sie bei Geräten mit einem internen Mobilfunk-Modem manuell den WAN-Zugriff über das Mobilfunknetz (WWAN) konfigurieren. Dazu legen Sie für Ihren Provider zunächst ein Mobilfunk-Profil an oder verändern ein bereits vorkonfiguriertes Profil, und weisen dieses Profil anschließend der WAN-Schnittstelle des Gerätes zu.

Für einen einfacheren und schnelleren Konfigurationsweg steht Ihnen alternativ auch ein entsprechender Setup-Assistent (**Internet-Zugang einrichten**) zur Verfügung.

Hinweis: Hier haben Sie auch die Möglichkeit, für die Mobilfunk-Standards entsprechende Generationsbezeichnungen anzugeben und diese anzeigen zu lassen.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für Ihr Gerät und wechseln Sie in die Ansicht **Schnittstellen** > **WAN**.
2. Wählen Sie in der Tabelle **Mobilfunk-Profile** ein vorkonfiguriertes Profil zur Bearbeitung aus oder fügen Sie für Ihren Provider ein neues Profil hinzu.

   Der Vollständigkeit wegen beschreibt dieses Tutorial die Anlage eines neuen Profils.



3. Geben Sie unter **Name** eine eindeutige Bezeichnung für das Mobilfunk-Profil an.
4. Geben Sie unter **PIN** die 4-stellige PIN der verwendeten Mobilfunk-SIM-Karte ein. Das Gerät benötigt diese Information, um das Mobilfunk-Modem in Betrieb zu nehmen.

   Wichtig: Die SIM-Karte protokolliert jeden Fehlversuch mit einer ungeeigneten PIN. Die Anzahl dieser Fehlversuche bleibt auch dann erhalten, wenn das Gerät zwischenzeitlich vom Stromnetz getrennt ist. Nach 3 Fehlversuchen sperrt sich die SIM-Karte gegen weitere Zugangsversuche. In diesem Zustand benötigen Sie die in der Regel 8-stelligen PUK oder SuperPIN, um die Sperre aufzuheben.

5. Sofern Ihr Gerät mehrere SIM-Karten aufnehmen kann, wählen Sie über **SIM Steckplatz** die SIM-Karte aus, die Sie mit dem Profil verknüpfen wollen.

   Die Auswahl **Profil inaktiv** deaktiviert das Mobilfunk-Profil. Wählen Sie diese Option, falls Sie lediglich eine Profil-Vorlage anlegen und die Mobilfunk-Einrichtung zu einem späteren Zeitpunkt abschließen wollen.

   Hinweis: Nur aktivierte Profile sind in der Auswahl in LANmonitor sichtbar.

6. Geben Sie unter **APN** den Namen des Zugangs-Servers für die Datendienste Ihres Mobilfunk-Providers ein.
   Der APN (Access Point Name) ist spezifisch für jeden Mobilfunk-Provider. Sie finden diese Information normalerweise in den Unterlagen Ihres Mobilfunk-Vertrages.
7. Geben Sie unter **PDP-Kontext** den Typ des PDP-Kontextes für das Mobilfunk-Profil an.
   Der PDP-Kontext beschreibt die Unterstützung der Adressräume, welche das Backbone des betreffenden Mobilfunkanbieters für Verbindungen aus dem Mobilfunknetz ins Internet anbietet. Dies kann entweder IPv4 oder IPv6 allein, oder die Unterstützung für beide Adressräume umfassen (Dual-Stack). Clients, die den betreffenden Mobilfunkanbieter nutzen wollen, müssen mindestens einen der angegebenen Adressräume unterstützen.
8. Geben Sie den bevorzugten Modus für die **Netz-Auswahl** an:

   Automatisch
   Das Mobilfunk-Modem bucht sich automatisch in eines der verfügbaren und erlaubten Mobilfunk-Netze ein.

   Manuell
   Das Mobilfunk-Modem bucht sich ausschließlich in das spezifizierte Mobilfunk-Netz ein.

   Hinweis: Die manuelle Mobilfunk-Netzwahl eignet sich insbesondere dann, wenn Sie das Gerät stationär betreiben und Sie häufige Einbuchungsvorgänge in ein benachbartes oder funktechnisch stärkeres, mitunter aber unerwünschtes oder teureres Mobilfunk-Netz feststellen.

9. Sofern Sie die manuelle Netz-Auswahl gewählt haben, geben Sie unter **Netz-Name** die exakte Bezeichnung Ihres Heimnetzes an.
10. Geben Sie unter **Übertragungs-Betriebsart** die bevorzugte Übertragungsart innerhalb des Mobilfunknetzes an:

    Automatisch
    Automatische Wahl der Übertragungs-Betriebsart

    LTE(4G)+UMTS(3G)
    Kombinierter LTE-UMTS-Betrieb

    LTE(4G)+GPRS(2G)
    Kombinierter LTE-GPRS-Betrieb

LTE(4G)
Ausschließlicher LTE-Betrieb

UMTS(3G)+GPRS(2G)
Kombinierter UMTS-GPRS-Betrieb

UMTS(3G)
Ausschließlicher UMTS-Betrieb

GPRS(2G)
Ausschließlicher GPRS-Betrieb

11. Geben Sie unter **Downstream-Rate** und **Upstream-Rate** die Übertragungsraten des verwendeten Mobilfunk-Anschlusses an, damit die Quality-of-Service (QoS)-Funktionen der Firewall einwandfrei funktionieren.
Bei einem Wert von `0` gilt die Mobilfunk-Schnittstelle in der betreffenden Richtung als unbeschränkt und die QoS-Mechanismen greifen nicht.

12. Wenn aufgrund ungünstiger Umgebungsbedingungen der Router ständig zwischen zwei Frequenzbändern wechselt, kann das zu Instabilitäten bei der Übertragung führen. Mit der Auswahl im Abschnitt **LTE-Bänder** geben Sie dem Mobilfunk-Modem vor, welche Frequenzbänder verwendbar sind.

Alle
Alle Frequenzbänder sind aktiviert.

2100 MHz (B1)
2,1GHz-Band ist aktiviert.

1800 MHz (B3)
1,8GHz-Band ist aktiviert.

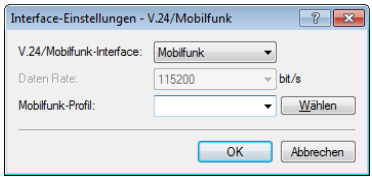
2600 MHz (B7)
2,6GHz-Band ist aktiviert.

900 MHz (B8)
900MHz-Band ist aktiviert.

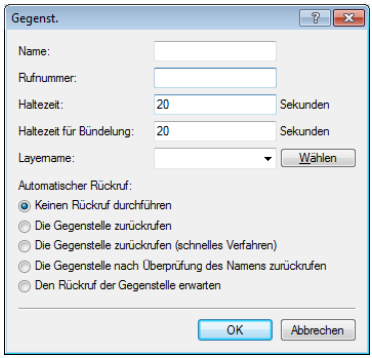
800 MHz (B20)
800MHz-Band ist aktiviert.

Hinweis: Diese Auswahl schränkt nur die Frequenzbänder bei der Übertragung im LTE-Standard ein. Für UMTS und GPRS bleiben grundsätzlich alle Bänder erlaubt.

13. Klicken Sie **OK**, um die Einstellungen zu speichern.
14. Klicken Sie in der Ansicht **Schnittstellen** > **WAN** auf **Interface-Einstellungen** und wählen Sie **V.24/Mobilfunk**.
15. Wählen Sie in der Liste **V.24/Mobilfunk-Interface** den Wert **Mobilfunk**.
16. Wählen Sie unter **Mobilfunk-Profil** das zuvor für Ihren Mobilfunk-Provider angelegte Profil aus.



17. Klicken Sie **OK**, um die Einstellungen zu speichern.
18. Klicken Sie in der Ansicht **Kommunikation** > **Gegenstellen** auf **Gegenst. (Mobilfunk/…)** und fügen Sie ein neues Profil hinzu.

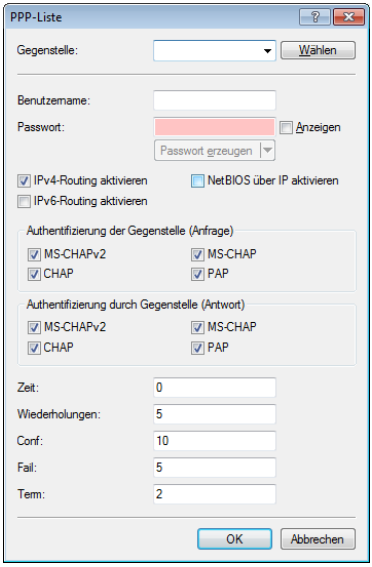


19. Tragen Sie unter **Name** eine eindeutige Bezeichnung für das Profil ein, z. B `WWAN`.
20. Tragen Sie unter **Rufnummer** die Einwahl-Rufnummer Ihres Mobilfunk-Providers ein. Sofern Ihr Provider Ihnen keine Einwahl-Rufnummer mitgeteilt hat, tragen Sie hier `*99#` ein.

21. Tragen Sie unter **Haltezeit** die Zeit ein, nach welcher das Gerät die Verbindung zur Gegenstelle trennt, wenn in dieser Zeit kein Datenpaket übertragen wird

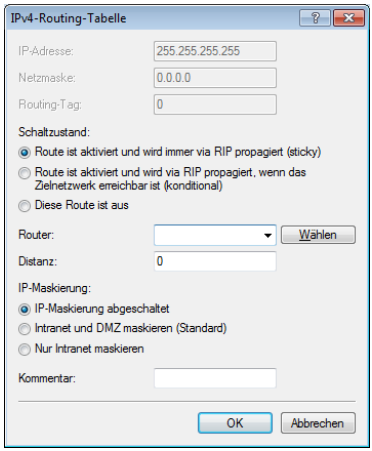
    Geben Sie z. B. einen Wert von `300` Sekunden ein, um einen akzeptablen Kompromiss zwischen Leerauf-Haltekosten und Kosten durch den Verbindungsaufbau zu wahren. Bei einem Wert von `0` hält das Gerät die Verbindung solange aufrecht, bis sie abgebrochen und beendet wird. Bei einem Wert von `9999` baut das Gerät die Verbindung automatisch immer wieder neu auf.

22. Wählen Sie als **Layernamen** den Vorgabewert `UMTS` aus.
23. Klicken Sie **OK**, um die Einstellungen zu speichern.
24. Klicken Sie in der Ansicht **Kommunikation** > **Protokolle** auf **PPP-Liste** und fügen Sie eine neue Gegenstelle hinzu.



25. Wählen Sie unter **Gegenstelle** das zuvor angelegte Gegenstellenprofil aus, z. B `WWAN`.
26. Wählen Sie unter **Authentifizierung der Gegenstelle (Anfrage)** jede Vorauswahl ab.
27. Klicken Sie **OK**, um die Einstellungen zu speichern.

28. Klicken Sie in der Ansicht **IP-Router** > **Routing** auf **IPv4-Routing-Tabelle-Liste** und fügen Sie die **Default-Route** (`255.255.255.255`) hinzu.



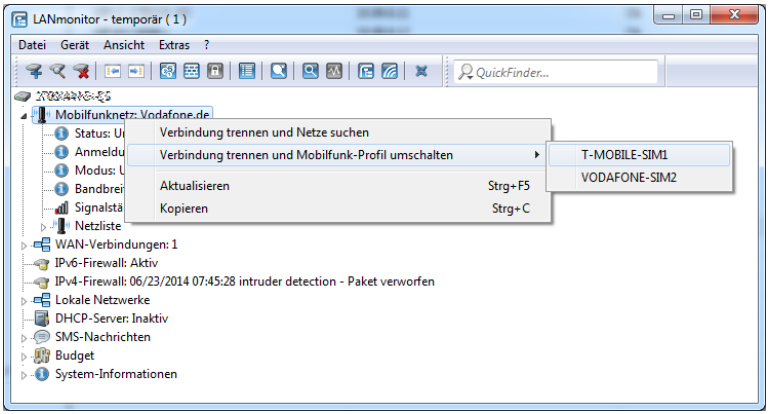
29. Geben Sie unter **Router** das zuvor unter **Gegenst. (Mobilfunk/…)** angelegte Profil an.
30. Setzen Sie die **IP-Maskierung** auf **Intranet und DMZ maskieren (Standard)**.
31. Klicken Sie **OK**, um die Einstellungen zu speichern.
32. Schreiben Sie die Änderungen zurück auf das Gerät.

Die Konfiguration des WWAN-Zugriffs ist damit abgeschlossen.

6.21 Umschalten zwischen Mobilfunk-Profilen oder SIM-Karten

Sofern Sie für eine SIM-Karte unterschiedliche Mobilfunk-Profile oder für mehrere SIM-Karten ein Mobilfunk-Profil angelegt haben, lässt sich mit LANmonitor zwischen diesen Profilen umschalten. Die nachfolgenden Schritte zeigen Ihnen, wie Sie im Betrieb ein alternatives Profil oder eine alternative SIM-Karte auswählen.

1. Wählen Sie im LANmonitor Ihr Gerät aus.
2. Öffnen Sie auf dem Eintrag **Mobilfunknetz** das Kontextmenü und wählen Sie **Verbindung trennen und Mobilfunk-Profil umschalten**.



3. Wählen Sie das Mobilfunk-Profil aus, auf das Sie umschalten wollen.

Das Gerät trennt daraufhin die Verbindung zum Mobilfunknetz und verbindet sich mit dem gewählten Mobilfunk-Profil erneut.

6.22 Route-Monitor

Der Route-Monitor überwacht Verbindungen zu Netzwerken verschiedener Provider und stellt im Fehlerfall eine Backup-Verbindung her. Die Überwachung geschieht über ein Trigger-Präfix, das der Provider in seinem Routing-Protokoll zur Verfügung stellt, z. B. beim Border Gateway Protokoll (BGP). Sobald die Route zu einem Provider-Netzwerk unerreichbar ist, erklärt der Route-Monitor das entsprechende Trigger-Präfix im eigenen Netzwerk für ungültig und öffnet eine Backup-Verbindung zum Provider-Netzwerk.

7 IPv6

7.1 IPv6-Grundlagen

IPv4 (Internet Protocol Version 4) ist ein Protokoll zur eindeutigen Adressierung von Teilnehmern in einem Netzwerk und definierte bislang alle weltweit vergebenen IP-Adressen. Da der so gebotene Adressraum Grenzen hat, tritt das IPv6 (Internet Protocol Version 6) in die Fußstapfen des bisherigen Standards. IPv6 bietet durch einen anderen IP-Adressaufbau ein breiteres Spektrum für IP-Adressen und vergrößert somit die möglich Anzahl an Teilnehmern in Netzwerken weltweit.

7.1.1 Warum IP-Adressen nach dem Standard IPv6?

Folgende Gründe führten zur einer Entwicklung des neuen IPv6-Standards:

- IPv4 deckt einen Adressraum von etwa vier Milliarden IP-Adressen ab, mit denen Teilnehmern in Netzwerken eindeutige Identitäten erhalten. Bei der Implementierung des IPv4-Standards in den 80er-Jahren galt dieser Adressraum als überaus ausreichend. Durch das enorme Wachstum des World Wide Web und der unvorhergesehenen Vielzahl an Rechnern und kommunizierenden Geräten entsteht eine Adressknappheit, die der IPv6-Standard überbrücken soll.
- Der größere Adressraum des IPv6 erschwert das Scannen von IP-Adressen durch Viren und Trojaner. Auf diese Weise bietet das breitere Spektrum einen größeren Schutz vor Angriffen.
- Das IPv6 wurde nach sicherheitstechnischen Anforderungen implementiert. So enthält es das Sicherheitsprotokoll IPSec (IP Security). Dieses sorgt für eine sichere Kommunikation im Netzwerk auf dem 3. Layer, während viele Sicherheitsmechanismen des IPv4 erst auf höheren Ebenen greifen.
- Durch einfachere und feste Bezeichnungen der Datenpakete sparen Router Rechenleistung und beschleunigen somit ihren Datendurchsatz.

- IPv6 ermöglicht eine einfachere und schnellere Übertragung von Daten in Echtzeit und eignet sich somit für Multi-Media-Anwendungen wie Internet-Telefonie oder Internet-TV.
- So genannte mobile IPs ermöglichen es, sich mit einer festen IP-Adresse in verschiedenen Netzwerken anzumelden. So kann man sich mit seinem Laptop im Heimnetzwerk, im Café oder am Arbeitsplatz mit derselben IP-Adresse anmelden.

7.1.2 Aufbau einer IP-Adresse nach IPv6-Standard

Die neuen IPv6-Adressen sind 128 Bit lang und decken somit einen Adressbereich von rund 340 Sextillionen möglichen Netzwerkteilnehmern ab. Sie bestehen aus 8 Blöcken zu je 16 Bit und werden als hexadezimale Zahl notiert. Das folgende Beispiel zeigt eine mögliche IPv6-Adresse:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

Um die Lesbarkeit solcher IP-Adressen zu verbessern, entfallen Nullen, die am Anfang eines Ziffernblocks stehen. Darüber hinaus kann eine einzige Gruppe von Blöcken entfallen, die komplett aus Nullen bestehen. Für das oben gezeigte Beispiel wäre eine möglich Darstellungsweise demnach die folgende:

2001:db8::54f3:dd6b:1/64

Eine IPv6-Adresse besteht aus zwei Komponenten: einem Präfix und einem Interface Identifier. Das Präfix bezeichnet die Zugehörigkeit der IP-Adresse zu einem Netzwerk, während der Interface Identifier z. B. im Fall der Autokonfiguration aus einer Link Layer Adresse erzeugt wird und somit zu einer Netzwerkkarte gehört. Das Gerät kann Interface Identifier auch mit Hilfe von Zufallszahlen generieren. Dies erhöht die Sicherheit. Auf diese Weise können mehrere IPv6-Adressen einem Teilnehmer zugeordnet werden.

Das Präfix beschreibt den ersten Teil der IP-Adresse. Die Länge des Präfix steht als Dezimalzahl hinter einem Schrägstrich. Für das hier genannte Beispiel lautet das Präfix:

2001:db8::/64

Der übrige Teil der IP-Adresse stellt den Interface Identifier dar. Dieser lautet für das angebene Beispiel:

::54f3:ddb6:1

Gegenüber den IP-Adressen nach dem Standard IPv4 ergeben sich für den Aufbau der neuen IPv6-Adressen einige Änderungen:

- Während IPv4-Adressen einen Adressraum von 32 Bit abdecken, entsteht durch die neue Länge von 128 Bit ein deutlich größerer Adressbereich von IPv6. IPv6-Adressen sind daher viermal so lang wie eine IPv4-Adresse.
- Eine Schnittstelle kann mehrere IPv6-Adressen haben, bedingt durch die mögliche Zuweisung mehrerer Präfixe zu einem Interface Identifier. Im IPv4-Standard besitzt jede Schnittstelle ausschließlich eine IP-Adresse.
- Die automatische Zuweisung von IPv4-Adressen erfolgt immer über einen DHCP-Server. IPv6 hingegen beherrscht eine Autokonfiguration, welche die Verwendung eines DHCP-Server überflüssig macht. Es besteht allerdings immer noch die Option, einen DHCP-Server einzusetzen oder die IP-Adressen statisch zu konfigurieren.

7.1.3 Migrationsstufen

IPv6 ist in Netzwerken auf verschiedene Arten verfügbar. Man unterscheidet bei IPv6-Umgebungen zwischen nativem IPv6 und IPv6, das über einen Tunnel entsteht.

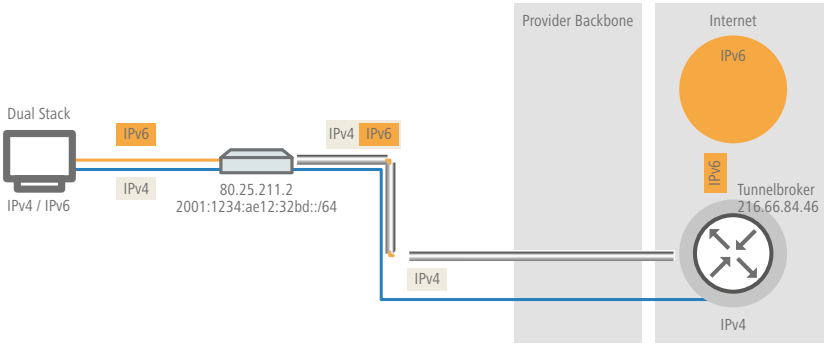
- **Reines (oder natives) IPv6:** Reines IPv6 bezeichnet ein Netzwerk, das nach Außen über IPv6 kommuniziert. Auf dieses können Teilnehmer mit IPv4-Internetzugang nur zugreifen, wenn der Router eine der unten beschriebenen Tunneltechnologien einsetzt.
- **IPv6 via Dual Stack:** Dual Stack bezeichnet den parallelen Betrieb von IPv4 und IPv6 in einem Netzwerk.
- **IPv6 Tunneling:** Wenn ein Router keinen nativen IPv6-Internetzugang hat, besteht die Möglichkeit, mit Hilfe eines Tunnels auf IPv6-Netzwerke zuzugreifen.

7.2 IPv6-Tunneltechnologien

7.2.1 6in4-Tunnel

6in4 Tunnel dienen der Verbindung zweier Hosts, Router oder der Verbindung zwischen Host und Router. 6in4 Tunnel können somit zwei IPv6 Netzwerke über ein IPv4 Netzwerk verbinden. Die Abbildung zeigt einen statischen 6in4-

Tunnel zwischen dem lokalen Router und einem 6in4-Gateway eines Tunnelbrokers.



Im Gegensatz zu 6to4 handelt es sich hierbei im einen dedizierten, bekannten Dienst und Betreiber. Die Endpunkte sind festgelegt und der Tunnelbroker weist ein statisches Präfix zu. Die Vorteile einer 6in4 Lösung sind also sowohl feste 6in4-Gateways als auch das Wissen um den Betreiber. Das feste Präfix des Tunnelbrokers bestimmt darüber hinaus die Anzahl der möglichen Subnetze, die genutzt werden können. Ein 64 Bit Präfix (z. B. 2001:db8::/64) erlaubt die Nutzung eines Subnetzes. Bei einem 48 Bit Präfix stehen sogar 16 Bit des 64 Bit Präfix-Anteils zur Verfügung. Damit lassen sich bis zu 65536 Subnetze realisieren.

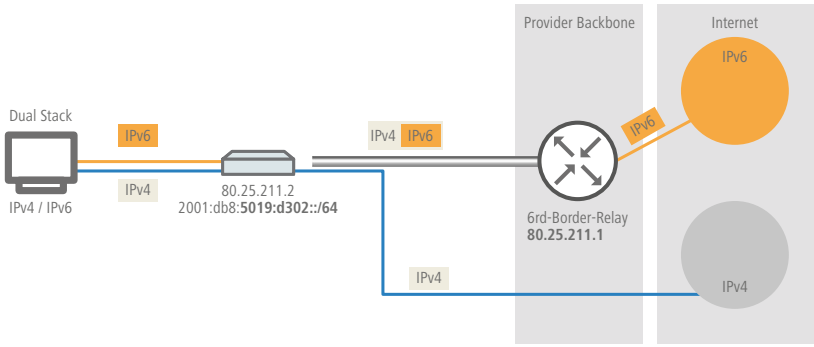
Der Nachteil der 6in4-Technologie ist der höhere Administrationsaufwand. Eine Anmeldung beim gewählten Tunnelbroker ist notwendig. Hinzu kommt die statische Konfiguration der Tunnelendpunkte. Im Falle einer dynamisch bezogenen IPv4-Adresse müssen die Daten regelmäßig aktualisiert werden. Letzteres kann allerdings von einem Router, beispielsweise mit Hilfe eines Skriptes, automatisch erledigt werden.

6in4 stellt eine vergleichsweise sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Technologie ist somit auch zum Betrieb von Webservern geeignet, die über IPv6 erreicht werden sollen. Der Nachteil ist lediglich der erhöhte adminstrative Aufwand. Diese Technologie ist somit auch für den professionellen Einsatz geeignet.

7.2.2 6rd-Tunnel

6rd (rapid deployment) ist eine Weiterentwicklung von 6to4. Die zugrunde liegende Funktionsweise ist identisch. Der Unterschied besteht darin, dass

ein spezifisches Relay genutzt wird, welches der Provider betreibt. Dies löst die zwei grundlegenden Probleme der 6to4- Technologie, die mangelnde Sicherheit und Stabilität. Das Präfix wird bei 6rd entweder manuell konfiguriert oder über DHCP (IPv4) übermittelt, was den Konfigurationsauswand weiter reduziert. Die Abbildung zeigt eine schematische Darstellung eines 6rd Szenarios.



Der Provider weist dem Router ein Präfix (2001:db8::/32) zu, welches vom Router durch die IPv4-Adresse ergänzt wird. Die somit erzeugte IPv6-Adresse hat die Form: 2001:db8:5019:d302::/64. 6rd ist somit aus zwei Perspektiven interessant. Es ermöglicht dem Provider auf einfache Art und Weise seinen Kunden das IPv6 Internet zugänglich zu machen. Zusätzlich vereinfacht es die Nutzung für die Kunden erheblich. Sie müssen weder die Sicherheitsrisiken von 6to4 hinnehmen noch den Konfigurationsaufwand von 6in4 investieren.

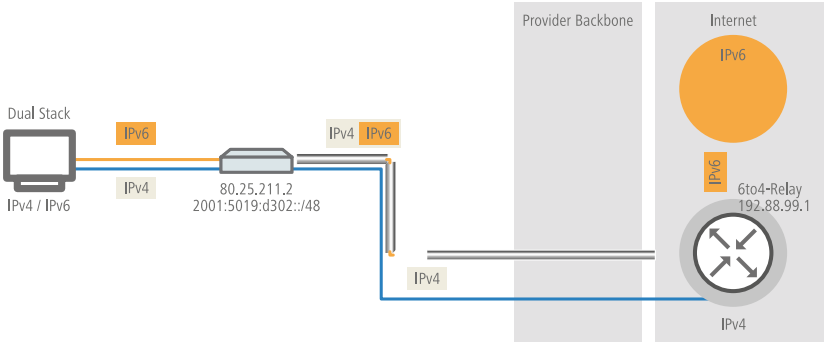
7.2.3 6to4-Tunnel

Mit dem 6to4-Tunneling haben Sie die Möglichkeit auf einfache Weise eine Verbindung zwischen zwei IPv6-Netzwerken über ein IPv4-Netzwerk herzustellen. Dazu wird ein so genannter 6to4-Tunnel erstellt:

- Ein Router zwischen lokalen IPv6-Netzwerk und einem IPv4-Netzwerk dient als Vermittler zwischen den Netzwerken.
- Der Router hat sowohl eine öffentliche IPv4-Adresse, als auch eine IPv6-Adresse. Die IPv6-Adresse setzt sich aus einem IPv6-Präfix und der IPv4-Adresse in hexadezimaler Schreibweise zusammen. Hat ein Router z. B. die IPv4-Adresse 80.25.211.2 , so wird diese zunächst in hexadezimale Schreibweise umgerechnet: 5019:d302. Ergänzend dazu kommt ein IPv6-

Präfix (z. B. 2002::/16), so dass die IPv6-Adresse für den Router wie folgt aussieht: 2002:5019:d302::/48.

- Schickt ein Gerät aus dem IPv6-Netzwerk Datenpakete über den Router an eine IPv6-Zieladresse, dann schachtelt der Router die IPv6-Pakete zunächst in ein Paket mit einem IPv4-Header. Das geschachtelte Paket leitet der Router anschließend an ein 6to4-Relay weiter. Das 6to4-Relay entpackt das Paket und leitet es an das gewünschte Ziel weiter. Die folgende Abbildung zeigt das Funktionsprinzip des 6to4-Tunneling:



6to4-Tunnel stellen eine dynamische Verbindung zwischen IPv6- und IPv4-Netzwerken her: die Antwortpakete werden möglicherweise über ein anderes 6to4-Relay zurückgeleitet, als auf dem Hinweg. Daher handelt es sich beim 6to4-Tunnel nicht um eine Punkt zu Punkt-Verbindung. Der Router sucht für jede neue Verbindung stets das nächstgelegene öffentliche 6to4-Relay. Dies geschieht über die Anycast-Adresse 192.88.99.1. Dieser Aspekt ist zum einen ein Vorteil des 6to4-Tunneling, stellt aber gleichzeitig auch einen Nachteil dar. Öffentliche 6to4-Relays benötigen keine Anmeldung und sind frei zugänglich. Desweiteren benötigt die dynamische Verbindung wenig Konfigurationsaufwand. Auf diese Weise ist es für jeden Nutzer möglich, einfach und schnell einen 6to4-Tunnel über ein öffentliches Relay zu erzeugen.

Andererseits führt die dynamische Verbindung dazu, dass der Nutzer keinen Einfluss auf die Wahl der 6to4-Relays hat. Daher besteht vom Provider des Relays die Möglichkeit, Daten mitzuschneiden oder zu manipulieren.

7.2.4 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, kurz DS-Lite, dient dazu, dass Internet-Provider ihren Kunden über eine IPv6-Verbindung Zugang zu IPv4-Servern verschaffen können. Das

ist z. B. dann erforderlich, wenn der Kunde weiterhin IPv4-Geräte verwendet, der Internet-Provider allerdings aufgrund knapper IPv4-Adressen dem Kunden nur eine IPv6-Adresse vergeben kann. Im Gegensatz zu den anderen drei IPv6-Tunnelverfahren "6in4", "6rd" und "6to4" dient DS-Lite also dazu, IPv4-Pakete über eine IPv6-Verbindung zu übertragen (IPv4-über-IPv6-Tunnel).

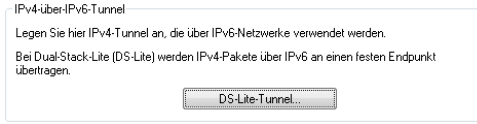
Der Router verpackt dazu die IPv4-Pakete in einen IPv4-in-IPv6-Tunnel und übermittelt sie unmaskiert an den Provider. Der führt anschließend eine NAT mit einer seiner eigenen verbliebenen IPv4-Adressen durch.

Zur Definition eines DS-Lite-Tunnels benötigt der Router nur die IPv6-Adresse des Tunnel-Endpunkts sowie das Routing-Tag, über das er diese Adresse erreichen kann.

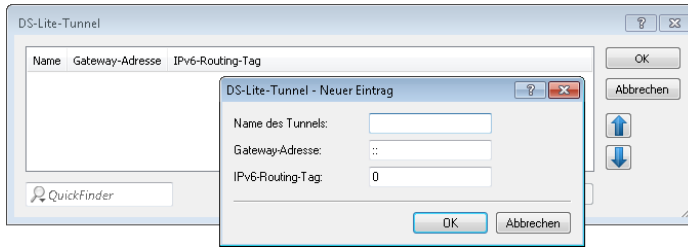
Standardmäßig verwendet der Router die IPv4-Adresse des entsprechenden internen Netzes, z. B. vom "INTRANET". Möchte man stattdessen eine andere IP-Adresse (z. B. 192.0.0.2) vorgeben, muss diese zusammen mit dem Gegenstellennamen des DS-Lite-Tunnels in der IP-Parameter-Liste angelegt sein.

Die Angabe eines IPv4-DNS-Servers ist für einen DS-Lite-Tunnel nicht ratsam, da dessen Einträge die NAT-Tabelle des Internet-Providers unnötig füllen würden.

Einen DS-Lite-Tunnel richten Sie in LANconfig ein über **IPv4** > **Tunnel** mit einem Klick auf **DS-Lite-Tunnel**.



Klicken Sie anschließend auf **Hinzufügen** und geben Sie die Bezeichnung des Tunnels, die IPv6-Adresse des Gateways und das Routing-Tag ein.



Name des Tunnels

Dieser Eintrag bestimmt den Namen des IPv4-über-IPv6-Tunnels.

Gateway-Adresse

Dieser Eintrag definiert die Adresse des DS-Lite-Gateways, den sogenannten Address Family Transition Router (AFTR).

Die folgenden Werte sind möglich:

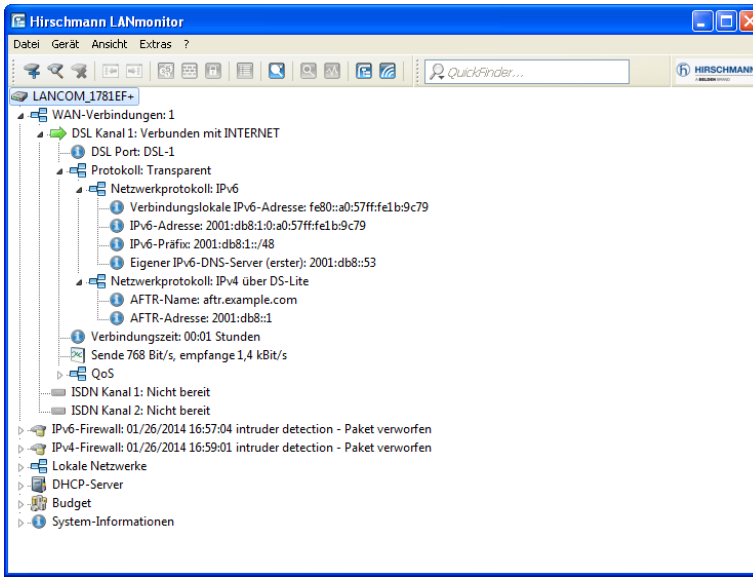
- Eine IPv6-Adresse, z. B. 2001:db8::1
- Ein per DNS auflösbarer FQDN (Fully Qualified Domain Name), z. B. aftr.example.com
- Die IPv6 Unspecified Address "::" bestimmt, dass das Gerät die Adresse des AFTRs per DHCPv6 beziehen soll (Werkseinstellung).
- Ein leeres Feld verhält sich wie bei der Eingabe von "::".

IPv6-Routing-Tag

Das Routing-Tag spezifiziert eindeutig die Route zum DS-Lite-Gateway.

Hinweis: Da bei DS-Lite das NAT durch den Provider erfolgt, ist die Funktion vieler Anwendungen von den Einstellungen des Provider-NATs abhängig (z. B. SIP, H.323, IRC oder IPSec). PPTP funktioniert über DS-Lite gar nicht. Wenn der Provider kein Portforwarding eingerichtet hat, funktionieren auch IPv4-Serverdienste nicht mehr.

Über den LANmonitor lassen sich die Status-Tabelle und die Anzahl der aktuellen DS-Lite-Verbindungen darstellen:



7.3 DHCPv6

Im Vergleich zu IPv4 benötigen Clients in einem IPv6-Netzwerk wegen der Autokonfiguration keine automatischen Adresszuweisungen über einen entsprechenden DHCP-Server. Da aber bestimmte Informationen wie DNS-Server-Adressen nicht per Autokonfiguration übertragen werden, ist es in bestimmten Anwendungsszenarien sinnvoll, auch bei IPv6 einen DHCP-Dienst im Netzwerk zur Verfügung zu stellen.

7.3.1 DHCPv6-Server

Die Verwendung eines DHCPv6-Servers ist bei IPv6 optional. Grundsätzlich unterstützt ein DHCPv6-Server zwei Betriebsarten:

- **Stateless**: Der DHCPv6-Server verteilt keine Adressen, sondern nur Informationen, z. B. DNS-Server-Adressen. Bei dieser Methode generiert sich ein Client seine IPv6-Adresse durch die 'Stateless Address Autokonfiguration (SLAAC)'. Dieses Verfahren ist besonders attraktiv u. a. für kleine Netzwerke, um den Verwaltungsaufwand möglichst gering zu halten.

- **Stateful**: Der DHCPv6-Server verteilt IPv6-Adressen, ähnlich wie bei IPv4. Dieses Verfahren ist deutlich aufwändiger, da ein DHCPv6-Server die Adressen vergeben und verwalten muss.

Ein DHCPv6-Server verteilt nur die Optionen, die ein IPv6-Client explizit bei ihm anfragt, d. h., der Server vergibt einem Client nur dann eine Adresse, wenn dieser explizit eine Adresse anfordert.

Zusätzlich kann der DHCPv6-Server Präfixe zur weiteren Verteilung an Router weitergeben. Dieses Verfahren wird als 'Präfix-Delegierung' bezeichnet. Ein DHCPv6-Client muss allerdings ebenfalls dieses Präfix explizit angefragt haben.

7.3.2 DHCPv6-Client

Durch die Autokonfiguration in IPv6-Netzwerken gestaltet sich die Konfiguration der angeschlossenen Clients sehr einfach und komfortabel.

Damit ein Client jedoch auch Informationen z. B. über DNS-Server erhalten kann, müssen Sie das Gerät so konfigurieren, dass es bei Bedarf den DHCPv6-Client aktiviert.

Die Einstellungen für den DHCPv6-Client sorgen dafür, dass das Gerät beim Empfang bestimmter Flags im Router-Advertisment den DHCPv6-Client startet, um spezielle Anfragen beim zuständigen DHCPv6-Server zu stellen:

- **M-Flag**: Erhält ein entsprechend konfiguriertes Gerät ein Router-Advertisment mit gesetztem 'M-Flag', dann fordert der DHCPv6-Client eine IPv6-Adresse sowie andere Informationen wie DNS-Server, SIP-Server oder NTP-Server beim DHCPv6-Server an.
- **O-Flag**: Bei einem 'O-Flag' fragt DHCPv6-Client beim DHCPv6-Server nur nach Informationen wie DNS-Server, SIP-Server oder NTP-Server, nicht jedoch nach einer IPv6-Adresse.

  Hinweis: Wenn das 'M-Flag' gesetzt ist, muss nicht zwingend auch das 'O-Flag' gesetzt sein.

Hinweis: Bei IPv6 wird die Default-Route nicht über DHCPv6 verteilt, sondern über Router-Advertisements.

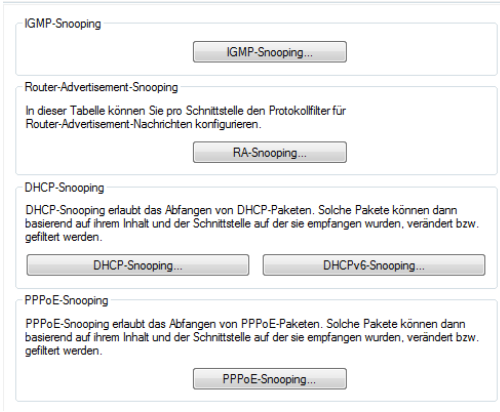
7.3.3 Lightweight-DHCPv6-Relay-Agent (LDRA)

Im Gegensatz zu einem DHCPv6-Relay-Agent, der über alle IPv6-Funktionen (wie z. B. ICMPv6) verfügt und Datenpakete im Netz routen kann (Layer-3), ermöglicht ein Lightweight-DHCPv6-Relay-Agent nach RFC 6221 nur die Erzeugung und Weitergabe von Relay-Agent-Informationen zwischen DHCPv6-Clients und DHCPv6-Servern (Layer-2).

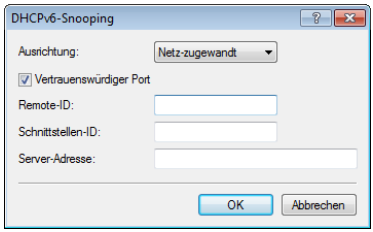
Anders als beim DHCPv4-Snooping fügt der LDRA den DHCPv6-Paketen nicht einfach Informationen zum Relay-Agent an, sondern er verpackt die Nachricht des Clients in eine eigene Option, stellt seinen Relay-Agent-Header voran und schickt erst anschließend dieses DCHPv6-Paket mit zusätzlichen Informationen an den DHCPv6-Server weiter (Relay Forward Message).

Der DHCPv6-Server wertet dieses Datenpaket aus und schickt eine gleichermaßen verpackte Antwort an den Relay-Agent. Der extrahiert die Nachricht und sendet sie an den anfragenden Client (Relay Reply Message).

Im LANconfig können Sie das DHCPv6-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCPv6-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Ausrichtung

Hier aktivieren bzw. deaktivieren Sie das DHCPv6-Snooping. Die folgende Auswahl ist möglich:

- **netz-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit einem DHCPv6-Server.
- **client-zugewandt**: Über diese Schnittstelle kommuniziert der LDRA mit den ans Netz angeschlossenen DHCPv6-Clients.

In der Werkseinstellung **netz-zugewandt** ist der LDRA deaktiviert.

Vertrauenswürdiger Port

Der LDRA leitet sowohl DHCP-Anfragen von Clients als auch DHCP-Antworten von DHCP-Servern weiter, wenn diese Option aktiviert ist. Ist diese Schnittstelle als nicht vertrauenswürdig eingestuft, verwirft der LDRA DHCPv6-Anfragen an dieser Schnittstelle. DHCPv6-Antworten, die nicht die korrekte Interface-ID enthalten, leitet der LDRA ebenfalls nicht an den Client weiter.

Remote-Id

Die Remote-ID nach RFC 4649 kennzeichnet eindeutig den Client, der eine DHCPv6-Anfrage stellt.

Schnittstellen-Id

Die Interface-ID kennzeichnet eindeutig die Schnittstelle, über die ein Client eine DHCPv6-Anfrage stellt.

Server-Adresse

Hier können Sie die IPv6-Adresse eines DHCPv6-Servers festlegen.

Hinweis: Lassen Sie dieses Feld leer, wenn Sie Antworten von allen DHCPv6-Servern im Netz erhalten wollen. Ansonsten reagiert der LDRA

nur auf DHCPv6-Antworten des Servers, dessen Adresse Sie angegeben haben. Antworten von anderen DHCPv6-Servern verwirft der LDRA in diesem Fall.

Sie können für **Remote-Id** und **Schnittstellen-Id** die folgenden Variablen verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- %n: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- %v: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.
- %s: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

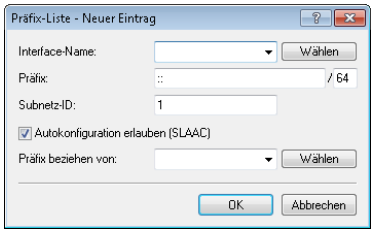
7.3.4 Präfix-Exclude-Option für DHCPv6-Präfix-Delegation

Der DHCPv6-Client des Gerätes unterstützt bei der Präfix-Delegation den Ausschluss von delegierten IPv6-Präfixen nach RFC 6603 (Prefix Exclude Option for DHCPv6-based Prefix Delegation).

Diesen Mechanismus verwenden Provider bei der DHCPv6 Präfix-Delegation, um ein Präfix aus dem delegierten Präfix für die Verwendung auf dem Kunden-LAN auszuschließen. Damit benötigt das Gerät für die WAN-Verbindung kein zusätzliches Präfix, sondern verwendet dafür das ausgeschlossene Präfix

aus dem delegierten DHCPv6-Präfix. Dieses Präfix steht nicht mehr für das LAN auf der Kundenseite zur Verfügung.

Sollte im Gerät das ausgeschlossene Präfix für das LAN konfiguriert sein, erfolgt eine Syslog-Meldung und das Präfix wird im LAN nicht angekündigt. In diesem Fall konfigurieren Sie unter **IPv6** > **Router-Advertisement** > **Präfix-Liste** manuell eine andere Subnetz-ID für dieses LAN, um den Konflikt aufzulösen.

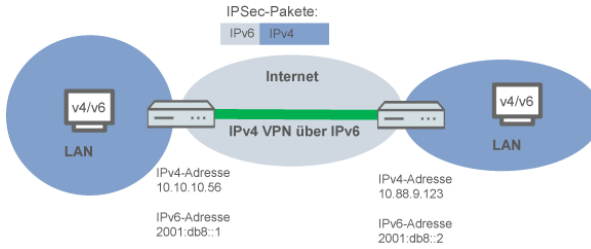


7.4 IPv4-VPN-Tunnel über IPv6

Bisher war es nicht möglich, zwei Gegenstellen über VPN zu verbinden, die für den Internetzugang private IPv4-Adressen verwenden (z. B. Mobilfunk).

Mit IPv6 ist diese Einschränkung nicht mehr vorhanden, da jedes IPv6-Gerät eine öffentliche IPv6-Adresse erhält. Somit kann über IPv6 ein IPv4-VPN-Tunnel eingerichtet werden, der zwei entfernte IPv4-Netzwerke verbindet, unabhängig von den IPv4-WAN-Adressen der entsprechenden Gegenstellen.

Im dargestellten Beispiel werden zwei lokale IPv4-Netzwerke über einen IPv4-VPN-Tunnel verbunden, welcher über eine IPv6-Internet-Verbindung aufgebaut wurde. Hierbei werden über die IPv6-Internetverbindung (nativ oder über Tunnelbroker) die IPv4-VPN-Pakete mit einem IPv6-Header an die Gegenstelle gesendet.



7.4.1 Setup-Assistent - IPv4-VPN-Verbindung über IPv6 einrichten

Der Setup-Assistent zur Verbindung zweier lokaler Netze unterstützt Sie bei der Einrichtung einer VPN-Verbindung.

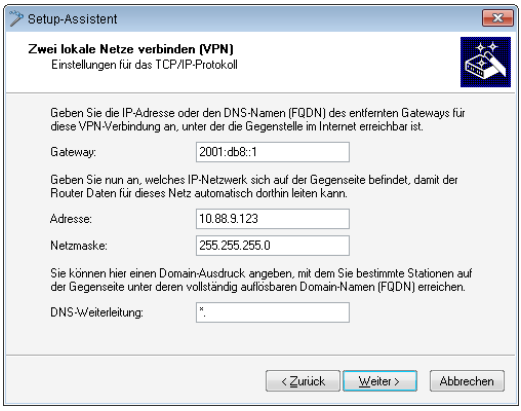
1. Starten Sie LANconfig.

   LANconfig sucht nun automatisch im lokalen Netz nach Geräten. Sobald LANconfig mit der Suche fertig ist, zeigt es in der Liste alle gefundenen Geräte mit Namen, evtl. einer Beschreibung, der IP-Adresse und dem Status an.

2. Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** > **Setup Assistent**.

   LANconfig liest zunächst die Gerätekonfiguration aus und zeigt das Auswahlfenster der möglichen Anwendungen.

3. Wählen Sie die Aktion **Zwei lokale Netze verbinden** .
4. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.
5. Geben Sie als Gateway-Adresse die IPv6-Adresse des Gateways ein.



6. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.

   Der Setup-Assistent schreibt die Konfiguration in das Gerät.

7.5 IPv6-Firewall

7.5.1 Funktion

Während die IPv4-Firewall ausschließlich das Forwarding der IP-Daten kontrolliert, regelt die IPv6-Firewall auch die Funktionen der Access-Listen aller IPv6-Server-Dienste. Die IPv6-Firewall entspricht damit eher dem klassischen Design von Firewalls, die die Inbound- und Outbound-Kommunikation sowie das Forwarding separat unterstützen. Da im Gerät dessen Konfiguration gezielt die Kommunikation steuert, verzichtet das Gerät auf eine Outbound-Firewall.

7.5.2 Konfiguration

Die Konfiguration der IPv6-Firewall entspricht weitgehend der Konfiguration der IPv4-Firewall, erfolgt jedoch getrennt von dieser.

Die Inbound- und Forwarding-Firewall verfügen jeweils über eine eigene Regeltabelle, die sich in Umfang und Aufbau an die entsprechende Regelstruktur der IPv4-Firewall anlehnen.

Die Regeln sind nach absteigender Priorität sortiert, d. h., die Regel mit der höchsten Priorität steht in der Liste oben. Bei gleicher Priorität erfolgt eine Sortierung anhand der Genauigkeit analog zur Verfahrensweise bei IPv4. Falls die Regel vorgibt, weitere Regeln zu beachten, führt die Firewall der Reihe nach auch die nachfolgenden Filterregeln aus. Ansonsten beendet die Firewall die Filterung, nachdem sie die aktuell zutreffende Regel angewendet hat.

7.5.3 Default-Einträge für die IPv6-Firewall-Regeln

Die IPv6-Firewall besitzt standardmäßig eine Reihe von Filterregeln, die sie auf eingehende Datenströme anwendet.

Default-Einträge für die Inbound-Regeln

Diese Übersicht enthält die Regeln, die die Firewall bei Inbound-Verbindungen anwenden soll. Standardmäßig sind bereits die folgenden Regeln für die wichtigsten Anwendungsfälle vorgegeben:

ALLOW-ICMP, ACCEPT
Erlaube alle Verbindungen über ICMPV6.

ALLOW-DHCP-CLIENT, ACCEPT
Erlaube die Kommunikation mit dem DHCPv6-Client.

ALLOW-DHCP-SERVER, ACCEPT
Erlaube die Kommunikation mit dem DHCPv6-Server.

ALLOW-CONFIG-LOCALNET, ACCEPT
Erlaube die Konfiguration im lokalen Netzwerk über HTTP, HTTPS, SNMP, SSH, TELNET, TFTP.

ALLOW-CONFIG-VPN, ACCEPT-VPN
Erlaube die HTTP, HTTPS, SNMP, SSH, TELNET und TFTP-Kommunikation über VPN.

ALLOW-DNS-SERVER, ACCEPT
Erlaube die Kommunikation mit dem internen DNS-Server aus dem lokalen Netz.

ALLOW-DNS-SERVER-VPN, ACCEPT-VPN
Erlaube die Kommunikation mit dem internen DNS-Server über VPN.

DENY-ALL, REJECT-SNMP
Blockiere die gesamte Kommunikation und informiere den Admin über SNMP.

ALLOW-CONFIG-WAN, ACCEPT
Erlaube die Kommunikation über die WAN-Schnittstelle über HTTPS, SSH. (deaktiviert)

ALLOW-IPSEC, ACCEPT
Erlaube die gesamte VPN-Kommunikation über IPSEC. (deaktiviert)

ALLOW-IPSEC-HTTPS-ENCAPSULTION, ACCEPT
Erlaube die Nutzung von IPSec über HTTPS. (deaktiviert)

Default-Einträge für die Forwarding-Regeln

Diese Tabelle enthält die Regeln, die die Firewall beim Forwarding von Daten anwenden soll. Standardmäßig sind bereits die folgenden Regeln für die wichtigsten Anwendungsfälle vorgegeben:

ALLOW-VPN, ACCEPT-VPN
Erlaube alle Verbindungen über IPSEC.

DENY-ALL, REJECT-SNMP
Blockiere die gesamte Kommunikation über SNMP.

ALLOW-OUTBOUND, ACCEPT-VPN
Erlaube die gesamte ausgehende Kommunikation.

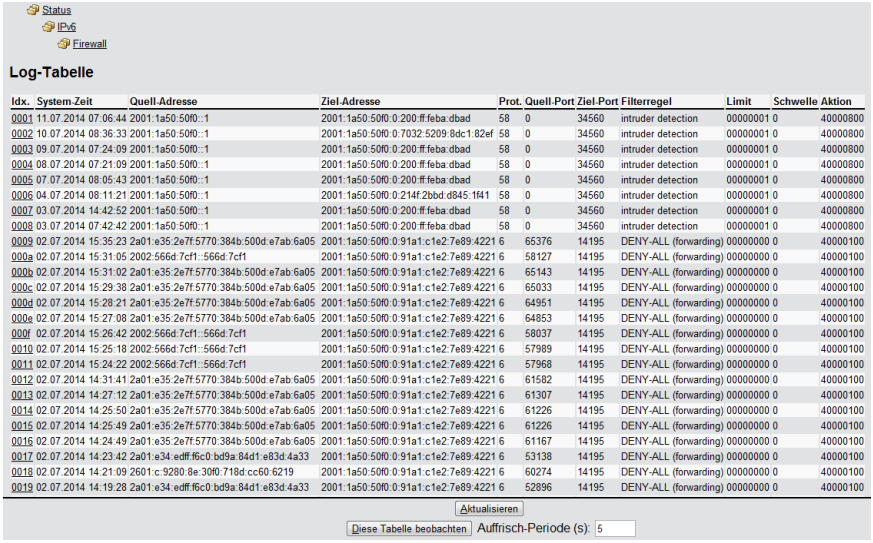
7.5.4 IPv6-Firewall-Log-Tabelle

Die IPv6-Firewall stellt analog zur IPv4-Firewall eine Log-Tabelle für Ereignisse im IPv6-Umfeld bereit.

Die Syntax dieser Log-Tabelle entspricht der IPv4-Log-Tabelle mit Ausnahme des IP-Adressformats (IPv6-Adressen liegen in hexadezimaler, IPv4-Adressen in dezimaler Form vor).

IPv6-Firewall-Log-Tabelle über WEBconfig auswerten

Sie können die IPv6-Log-Tabelle im WEBconfig über **HiLCOS-Menübaum** > **Status** > **IPv6** > **Firewall** > **Log-Tabelle** öffnen.



Die Einträge haben folgende Bedeutung:

- **Idx.**: Fortlaufender Index. Darüber lässt sich die Tabelle auch über SNMP abfragen.
- **System-Zeit**: System-Zeit in UTC-Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt).
- **Quell-Adresse**: Quell-Adresse des gefilterten Pakets.
- **Ziel-Adresse**: Ziel-Adresse des gefilterten Pakets.
- **Prot.**: Protokoll (TCP, UDP etc.) des gefilterten Pakets.
- **Quell-Port**: Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Ziel-Port**: Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen).
- **Filterregel**: Name der Regel, die den Eintrag erzeugt hat. Erfolgt die Filterung auf Grund mehrerer Regeln, listet die Spalte alle entsprechenden Regeln auf. Falls der Platz nicht ausreicht, erscheint das Kürzel '...'.

- **Limit**: Bitfeld, das das überschrittene Limit beschreibt, durch das die Firewall den Filter angewendet hat. Es sind zur Zeit folgende Werte definiert:
  - 0x01: Absolute Anzahl
  - 0x02: Anzahl pro Sekunde
  - 0x04: Anzahl pro Minute
  - 0x08: Anzahl pro Stunde
  - 0x10: globales Limit
  - 0x20: Byte-Limit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit)
  - 0x40: Limit gilt nur in Empfangsrichtung
  - 0x80: Limit gilt nur in Senderichtung
- **Schwelle**: überschrittener Grenzwert des auslösenden Limits.
- **Aktion**: Bitfeld, das alle ausgeführten Aktionen aufführt. Es sind zur Zeit folgende Werte definiert:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Aufbaufilter
  - 0x00000400: Internet-(Defaultrouten-)Filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Quell-Adresse sperren
  - 0x00020000: Ziel-Adresse und -Port sperren
  - 0x20000000: Sende SYSLOG-Benachrichtigung
  - 0x40000000: Sende SNMP-Trap
  - 0x80000000: Sende E-Mail

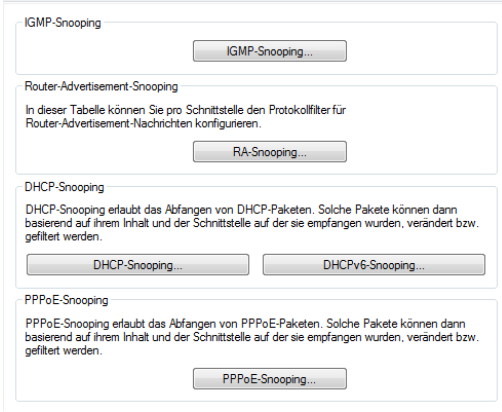
Hinweis: Alle Firewall-Aktionen erscheinen ebenfalls im IP-Router-Trace.

7.6 Router-Advertisement-Snooping

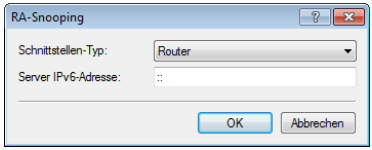
In einem IPv6-Netz senden Router periodisch oder auf Anfrage Router-Advertisments, um sich angeschlossenen Clients als Gateway zu präsentieren. Diesen Mechanismus können Angreifer wie beim DHCPv4 nutzen, um anfragenden Clients eine fehlerhafte oder schadhafte Netzkonfiguration zu übermitteln.

Beim RA-Snooping vermittelt das Gerät nur Router-Advertisements von Routern, nicht aber von Clients. Über die Angabe einer Router-Adresse lassen sich die Router-Advertisments auf einen bestimmten Router als Sender einschränken.

Im LANconfig können Sie das RA-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **RA-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



Schnittstellen-Typ

Bestimmen Sie hier den bevorzugten Schnittstellen-Typ. Die folgende Auswahl ist möglich:

- **Router**: Das Gerät vermittelt alle RAs, die an dieser Schnittstelle ankommen (Default).
- **Client**: Das Gerät verwirft alle RAs, die an dieser Schnittstelle ankommen.

Router-Adresse

Sofern Sie den Schnittstellen-Typ **Router** gewählt haben, geben Sie hier eine optionale Router-Adresse an. Bei Angabe einer Router-Adresse vermittelt das Gerät nur RAs des entsprechenden Routers.

Unter dem Schnittstellen-Typ **Client** ignoriert das Gerät dieses Eingabefeld.

7.7 IPv6-Konfigurationsmenü

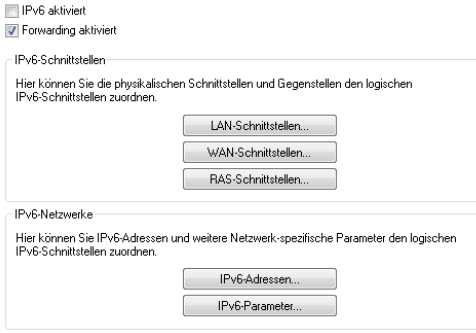
Im Gegensatz zu früheren Versionen von LANconfig, in denen es im Konfigurationsmenü die Konfigurationsmöglichkeit **TCP/IP** für IPv4 gab, finden Sie nun an dieser Stelle die Optionen **IPv4** und **IPv6**.

Klicken Sie auf **IPv6**, um die Einstellungen für dieses Protokoll vorzunehmen. Die Konfiguration **IPv6** ist unterteilt in die Optionen **Allgemein**, **Router-Advertisement**, **DHCPv6** und **Tunnel**. Standardmäßig befinden Sie sich nach dem Klick auf **IPv6** in der Ansicht *Allgemein* auf Seite 642.

7.7.1 Allgemein

Hier nehmen Sie die Grundeinstellungen vor.

- **IPv6 aktiviert:** Sie haben die Möglichkeit, IPv6 im Gerät zu aktivieren oder zu deaktivieren.
- **Forwarding aktiviert:** Forwarding dient der Paketweiterleitung zwischen IPv6-Schnittstellen. Diese Option ist standardmäßig aktiviert.



IPv6-Schnittstellen

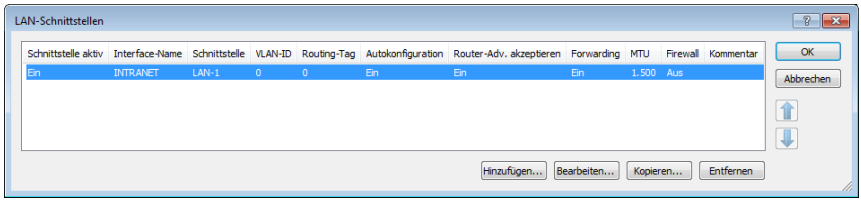
Über die Schaltflächen **LAN-Schnittstellen**, **WAN-Schnittstellen** und **RAS-Schnittstellen** gelangen Sie zu den Tabellen, die Ihnen die Möglichkeiten bieten, neue Schnittstellen hinzuzufügen sowie bestehende Schnittstellen zu konfigurieren oder zu löschen.

IPv6-Netzwerke

Die Schaltflächen **IPv6-Adressen** und **IPv6-Parameter** dienen dazu, den Schnittstellen IPv6-Adressen zuzuordnen sowie die Parameter der Schnittstellen (Gateway-Adresse, erster und zweiter DNS) zu konfigurieren. Über die Schaltfläche **Loopback-Adressen** lassen sich IPv6-Loopback-Adressen definieren, die das Gerät als zusätzliche Absenderadresse ansieht.

LAN-Schnittstellen

Für jedes existierende IPv4-Netzwerk müssen Sie zusätzlich unter **LAN-Schnittstellen** ein äquivalentes IPv6-Netzwerk anlegen. Dabei müssen die Einstellungen zu Schnittstellen-Bindung, Routing-Tag und VLAN-ID zu den Einstellungen des jeweiligen IPv4-Netzwerks passen. Da ein Gerät beliebig viele IPv6-Adressen haben kann, müssen Sie unter **IPv6-Adressen** statisch konfigurierte IPv6-Adressen hinzufügen.



Die Einträge in der Tabelle **LAN-Schnittstellen** haben folgende Bedeutung:

- **Schnittstelle aktiv**: Aktiviert bzw. deaktiviert diese LAN-Schnittstelle.
- **Interface-Name** bzw. **Netzwerkname**: Benennen Sie das logische IPv6-Interface, für das das physikalische Interface (Schnittstellen-Zuordnung) und die VLAN-ID gelten sollen.
- **Schnittstelle**: Wählen Sie die physikalische Schnittstelle aus, die zusammen mit der VLAN-ID das logische IPv6-Interface bilden soll. Eine Zuordnung "beliebig" wie bei IPv4 ist bei IPv6 nicht mehr möglich.
- **VLAN-ID**: Wählen Sie die VLAN-ID aus, die zusammen mit der physikalischen Schnittstelle das logische IPv6-Interface bilden soll.
- **Schnittstellen-Tag**: Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.
- **Autokonfiguration**: Aktivieren bzw. deaktivieren Sie die automatische Konfiguration von Adressen (SLAAC oder DHCPv6) in der Client-Rolle für dieses Interface.

  Hinweis: Falls das Gerät selbst auf diesem Interface Router-Advertisements versendet, erzeugt es auch bei aktivierter Autokonfiguration keine IPv6-Adressen aus empfangenen Router-Advertisements von anderen Routern.

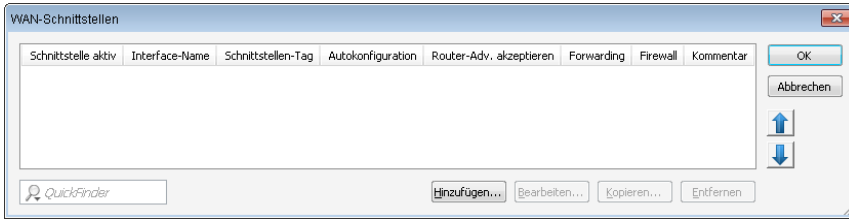
- **Router Advertisements akzeptieren**: Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten. Bei deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.
- **Forwarding**: Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces. Wenn Sie das Forwarding deaktivieren,

überträgt das Gerät auch keine Router-Advertisements über dieses Interface.

- **MTU**: Bestimmen Sie die gültige MTU auf dem entsprechenden Link.
- **Firewall**: Hier haben Sie die Möglichkeit, die Firewall für das Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist.
- **Kommentar**: Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

WAN-Schnittstellen

Für jede existierende Gegenstelle, auf der Sie IPv6 benutzen wollen, müssen Sie zusätzlich unter **WAN-Schnittstellen** eine äquivalente logische IPv6-WAN-Schnittstelle anlegen. Dabei muss der Name der IPv6-WAN-Schnittstelle dem Namen der IPv4-Gegenstelle entsprechen.



Die Einträge in der Tabelle **WAN-Schnittstellen** haben folgende Bedeutung:

- **Schnittstelle aktiv**: Aktiviert bzw. deaktiviert diese WAN-Schnittstelle.
- **Interface-Name**: Benennen Sie das logische IPv6-Interface analog zur zugehörigen IPv4-Gegenstelle.
- **Schnittstellen-Tag**: Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.
- **Autokonfiguration**: Aktivieren bzw. deaktivieren Sie die automatische Konfiguration von Adressen (SLAAC oder DHCPv6) in der Client-Rolle für dieses Interface.
- **Router Advertisements akzeptieren**: Aktivieren bzw. deaktivieren Sie die Auswertung empfangener Router-Advertisement-Nachrichten. Bei

deaktivierter Auswertung übergeht das Gerät die über Router-Advertisements empfangenen Präfix-, DNS- und Router-Informationen.

- **Forwarding**: Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces. Wenn Sie das Forwarding deaktivieren, überträgt das Gerät auch keine Router-Advertisements über dieses Interface.
- **Firewall**: Hier haben Sie die Möglichkeit, die Firewall für das Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist.
- **Kommentar**: Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

RAS-Schnittstellen

Grundsätzlich existieren zwei Wege, um die Konfiguration von RAS-Gegenstellen zu verwalten:

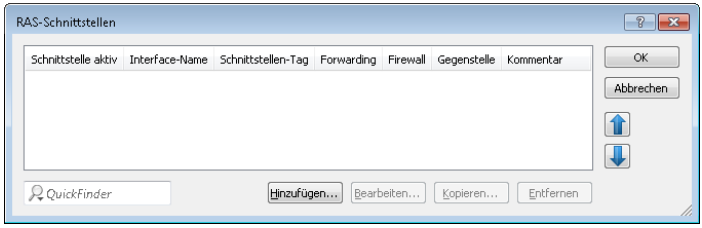
Die Benutzerdaten bzw. die Konfigurationen sind lokal im Gerät gespeichert.

Der Vorteil dieser Variante ist, dass man auf einen RADIUS-Server verzichtet und damit Verwaltung und Kosten der Netzinfrastruktur gering hält.

Die Benutzerdaten bzw. die Konfigurationen sind auf einen externen RADIUS-Server ausgelagert.

Der Vorteil dieser Variante liegt in der zentralen Benutzerverwaltung bei umfangreichen verteilten Netzwerk-Szenarien.

Für RAS-Zugänge über IPv6 müssen Sie zusätzlich unter **RAS-Schnittstellen** die entsprechende RAS-Schnittstelle einrichten.



Die Einträge in der Tabelle **RAS-Schnittstellen** haben folgende Bedeutung:

- **Schnittstelle aktiv**: Aktivieren oder deaktivieren Sie hier diese Schnittstelle.
- **Interface-Name**: Definieren Sie hier den Namen der RAS-Schnittstelle, über die die IPv6-Gegenstellen zugreifen.
- **Schnittstellen-Tag**: Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.
- **Forwarding**: Aktivieren bzw. deaktivieren Sie die Weiterleitung von Datenpaketen an andere Interfaces.
- **Firewall**: Hier haben Sie die Möglichkeit, die Firewall für jedes Interface einzeln zu deaktivieren, wenn die globale Firewall für IPv6-Schnittstellen aktiv ist. Um die Firewall für alle Schnittstellen global zu aktivieren, markieren Sie unter **Firewall/QoS** > **Allgemein** die Option **IPv6-Firewall/QoS aktiviert**.

  Achtung: Wenn Sie die globale Firewall deaktivieren, dann ist auch die Firewall einer einzelnen Schnittstelle inaktiv. Das gilt auch dann, wenn Sie diese mit dieser Option aktiviert haben.

- **Gegenstelle**: Bestimmen Sie hier eine Gegenstelle oder eine Liste von Gegenstellen für RAS-Einwahl-Benutzer.

  Die folgenden Werte sind möglich:

  - Eine einzelne Gegenstelle aus den Tabellen unter **Setup** > **WAN** > **PPTP-Gegenstellen**, **Setup** > **WAN** > **L2TP-Gegenstellen** oder **Setup** > **PPPoE-Server** > **Namenliste**.
  - Dem Platzhalter "*", der bewirkt, dass diese Schnittstelle für alle PPTP-, PPPoE- und L2TP-Gegenstellen gilt.
  - Dem Platzhalter "*" als Suffix oder Präfix von Gegenstellen, z. B. "FIRMA*" oder "*TUNNEL".

  Durch den Platzhalter-Mechanismus bilden Sie bei IPv6-RAS-Diensten mehrere Gegenstellen auf sogenannte Template-Schnittstellen ab. Diese Template-Schnittstellen sind als normale Schnittstellen bei IPv6-Diensten wie DHCPv6-Server oder Router Advertisements einsetzbar. Darüber lässt sich z. B. eine Gruppe von RAS-Schnittstellen aus einem IPv6-Präfix-Pool bedienen.

- **Kommentar**: Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

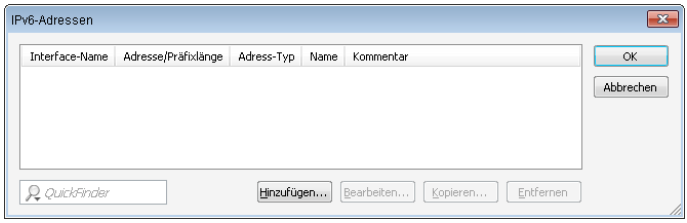
Informationen zu den RADIUS-Attributen für IPv6-RAS-Dienste finden Sie unter *Erweiterung der RADIUS-Attribute für IPv6-RAS-Dienste*.

Hinweis: Wenn RAS-Clients einen IPv6-DNS-Server zugewiesen oder per Präfix-Delegation Präfixe delegiert bekommen sollen, so müssen Sie unter **IPv6** > **DHCPv6** einen entsprechenden Eintrag in der Tabelle **DHCPv6-Netzwerke** anlegen.

Hinweis: Wollen Sie einen Benutzer anhand der PPP-Liste authentifizieren, so müssen Sie unter **Kommunikation** > **Protokolle** > **PPP-Liste** bei diesem Benutzer die Option **IPv6-Routing** aktivieren.

IPv6-Adressen

In der Tabelle **IPv6-Adressen** können Sie sowohl IPv6-Adressen für LAN-Schnitsttellen als auch für WAN-Schnittstellen anlegen.



Die Einträge in der Tabelle **IPv6-Adressen** haben folgende Bedeutung:

- **Interface-Name**: Benennen Sie das Interface, dem Sie das IPv6-Netz zuordnen wollen.
- **Adresse/Präfixlänge**: Vergeben Sie eine IPv6-Adresse inklusive Präfixlänge für dieses Interface.

  Die Präfixlänge beträgt standardmäßig 64 Bit ("/64"). Verwenden Sie für die IPv6-Adresse möglichst keine längeren Präfixe, da zahlreiche IPv6-Mechanismen (z. B. die Autokonfiguration) von maximal 64 Bit Länge ausgehen.

Beispiel:

- Global Unicast Adresse: "2001:db8::1/64"
- Unique Local Adresse: "fd00::1/64"

Hinweis: Verbindungslokale Adressen sind pro Interface fest vorgegeben und nicht konfigurierbar.

- **Adress-Typ**: Bestimmen Sie den Typ der IPv6-Adresse.

  Mögliche Optionen:

  - Unicast
  - Anycast
  - EUI-64

  Beim Adresstyp EUI-64 entspricht die IPv6-Adresse der IEEE-Norm "EUI-64". Die MAC-Adresse der Schnittstelle stellt damit einen eindeutig identifizierbaren Bestandteil der IPv6-Adresse dar. Ein korrektes Eingabeformat für eine IPv6-Adresse inkl. Präfixlänge nach EUI-64 würde lauten: "2001:db8:1::/64". "EUI-64" ignoriert einen eventuell konfigurierten Interface Identifier der jeweiligen IPv6-Adresse und ersetzt ihn durch einen Interface Identifier nach "EUI-64". Die Präfixlänge bei "EUI-64" muss zwingend "/64" sein.

  Beim Adresstyp Unicast können sie eine vollständige IPv6-Adresse im Feld **Adresse/Präfixlänge** inkl. Interface-Identifier angeben, z. B. "2001:db8::1234/64".

  Beim Adresstyp Anycast können sie ebenfalls eine vollständige IPv6-Adresse im Feld **Adresse/Präfixlänge** inkl. Interface-Identifier abgeben, z. B. "2001:db8::1234/64". Intern behandelt das Gerät diese Adresse als Anycast-Adresse.

- **Name**: Vergeben Sie einen aussagekräftigen Namen für diese Kombination aus IPv6-Adresse und Präfix.
- **Kommentar**: Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

IPv6-Parameter

In der Tabelle **IPv6-Parameter** können Sie statische Parameter für LAN- oder WAN-Schnittstellen wie IPv6-DNS-Server oder IPv6-Gateway manuell konfigurieren, falls Sie keine Autokonfiguration oder DHCPv6 verwenden.

Die Einträge in der Tabelle **IPv6-Parameter** haben folgende Bedeutung:

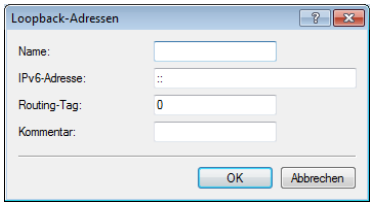
- **Interface-Name**: Benennen Sie das Interface, für Sie die IPv6-Parameter konfigurieren wollen.
- **Gateway-Adresse**: Bestimmen Sie das verwendete IPv6-Gateway für dieses Interface.

  Hinweis: Dieser Parameter überschreibt Gateway-Informationen, die das Gerät beispielsweise über Router-Advertisements empfängt.

- **Erster DNS**: Bestimmen Sie den ersten IPv6-DNS-Server für dieses Interface.
- **Zweiter DNS**: Bestimmen Sie den zweiten IPv6-DNS-Server für dieses Interface.

Loopback-Adressen

In der Tabelle **Loopback-Adressen** lassen sich IPv6-Loopback-Adressen festlegen. Das Gerät sieht jede dieser Adressen als eigene Adresse an, die auch dann verfügbar ist, wenn z. B eine physikalische Schnittstelle deaktiviert ist.



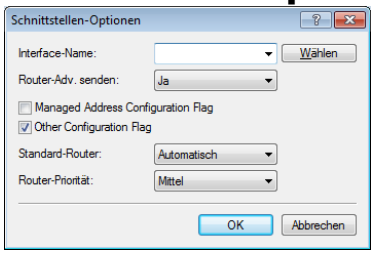
Die Einträge in der Tabelle **Loopback-Adressen** haben folgende Bedeutung:

- **Name**: Vergeben Sie hier einen eindeutigen Namen für diese Loopback-Adresse.
- **IPv6-Adresse**: Geben Sie hier eine gültige IPv6-Adresse ein.
- **Routing-Tag**: Geben Sie hier das Routing-Tag des Netzes an, zu dem die Loopback-Adresse gehört. Nur die Pakete mit dem entsprechenden Routing-Tag erreichen diese Adresse.
- **Kommentar**: Tragen Sie hier einen optionalen Kommentar ein.

7.7.2 Router-Advertisement

In der Konfiguration **Router-Advertisement** bieten sich Ihnen mehrer Schaltflächen mit Optionen zu Einstellungen des Neighbor Discovery Protocol (NDP), falls das Gerät als IPv6-Router arbeiten soll:

Schnittstellen-Optionen



Hier aktivieren oder deaktivieren Sie die folgenden Funktionen von Schnittstellen:

Router-Adv. senden

reguliert periodisches Senden von Router-Advertisements und das Antworten auf Router Solicitations.

Managed-Flag

wenn diese Funktion aktiv ist, konfiguriert ein Client, der dieses Router-Advertisement empfängt, Adressen durch Stateful Autoconfiguration (DHCPv6). Clients beziehen dann auch automatisch andere Informationen, wie z. B. DNS-Server.

Other Flag

wenn diese Funktion aktiv ist, versucht ein Client, zusätzliche Informationen, z. B. DNS-Server-Adressen, über DHCPv6 zu beziehen. Ob ein Client Adressen durch Autokonfiguration bilden soll, können Sie pro Präfix in der **Präfix-Liste** unter **Autokonfiguration erlauben (SLAAC)** bestimmen.

Standard-Router

definiert das Verhalten, wie sich das Gerät als Standardgateway bzw. Router ankündigen soll. Die Parameter haben folgende Funktionen:

- "Automatisch": Solange eine WAN-Verbindung besteht, setzt das Gerät eine positive Router-Lifetime in den Router-Advertisement-Nachrichten. Das führt dazu, dass ein Client diesen Router als Standard-Gateway verwendet.

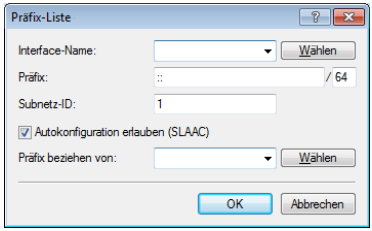
Besteht die WAN-Verbindung nicht mehr, so setzt der Router die Router-Lifetime auf "0". Ein Client verwendet dann diesen Router nicht mehr als Standard-Gateway.

- "Immer": Die Router-Lifetime ist unabhängig vom Status der WAN-Verbindung immer positiv, d. h. größer "0".
- "Nie": Die Router-Lifetime ist immer "0".

Router-Priorität

definiert die Präferenz dieses Routers. Clients tragen diese Präferenz in ihre lokale Routing-Tabelle ein.

Präfix-Liste



Setzen Sie die Präfix-Optionen verwendeter Schnittstellen. Möglich sind folgende Einstellungen:

Präfix

Tragen Sie hier ein Präfix ein, das in Router-Advertisements angekündigt wird, z. B. 2001:db8::/64. Die Präfixlänge muss immer exakt "/64" sein, da es sonst für Clients unmöglich ist, Adressen durch Hinzufügen ihrer Interface-Identifier (mit Länge 64 Bit) zu generieren. Soll ein vom Provider delegiertes Präfix automatisch weiter propagiert werden, so setzen Sie hier "::/64" und den Namen des entsprechenden WAN-Interfaces unter dem Parameter **Präfix beziehen von** ein.

Subnetz-ID

Tragen Sie hier die Subnetz-ID ein, die mit dem vom Provider delegierten Präfix kombiniert werden soll. Weist der Provider z. B. das Präfix "2001:db8:a::/48" zu und ist die Subnetz-ID "0001" oder kurz "1", so enthält das Router-Advertisement auf diesem Interface das Präfix "2001:db8:a:0001::/64". Die maximale Subnetzlänge bei einem 48 Bit langen delegierten Präfix ist 16 Bit (65.536 Subnetze), d. h. mögliche

Subnetz-IDs von "0000" bis "FFFF". Bei einem delegierten Präfix von "/56" ist die maximale Subnetzlänge 8 Bit (256 Subnetze), d. h. Subnetz-IDs von "00" bis "FF". In der Regel wird die Subnetz-ID "0" zur automatischen Bildung der WAN-IPv6-Adresse verwendet. Deshalb starten Subnetz-IDs für LANs bei "1". Die Default-Einstellung ist "1".

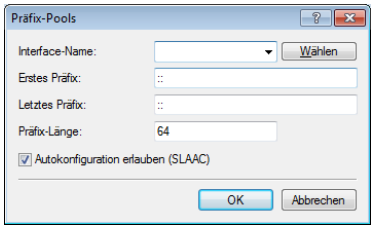
Autokonfiguration erlauben (SLAAC)

Gibt an, ob der Client das Präfix für die Stateless Address Autoconfiguration (SLAAC) verwenden soll. Die Default-Einstellung ist "aktiviert".

Präfix beziehen von

Definiert den Namen des Interfaces, auf dem ein Präfix über DHCPv6-Präfix-Delegation oder Tunnel empfangen wird. Aus diesem Präfix kann pro Interface ein Subnetz abgeleitet und propagiert werden.

Präfix-Pools



Diese Tabelle enthält Präfix-Pools, aus denen RAS-Benutzer einen Präfix bei der Einwahl über IPv6 erhalten. Möglich sind folgende Einstellungen:

Interface-Name

Bestimmt den Namen der RAS-Schnittstelle, für die dieser Präfix-Pool gelten soll.

Erster Präfix

Definiert das erste Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db8::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Letzter Präfix

Definiert das letzte Präfix des Pools, das der Einwahl-Benutzer durch Router-Advertisement zugeteilt bekommt, z. B. '2001:db9:FFFF::'. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool.

Präfix-Länge

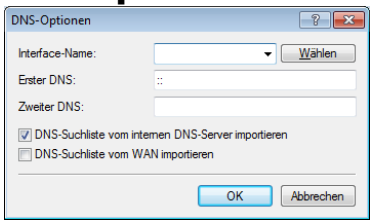
Definiert die Länge des Präfixes, das der Einwahl-Benutzer per Router-Advertisement zugewiesen bekommt. Die Größe des Einwahl-Pools richtet sich nur nach dem ersten und letzen Präfix. Jeder Benutzer erhält dabei genau ein /64-Präfix aus dem Pool zugewiesen.

Achtung: Damit ein Client aus dem Präfix per Autokonfiguration eine IPv6-Adresse bilden kann, muss die Präfix-Länge immer 64 Bit betragen.

SLAAC

Gibt an, ob der Client das Präfix für eine Stateless Address Autoconfiguration (SLAAC) verwenden kann.

DNS-Optionen



Definiert die DNS-Informationen in Router-Advertisements nach RFC 6106. Möglich sind folgende Einstellungen:

Interface-Name

Name des Interfaces, auf dem der IPv6-DNS-Server Informationen in Router-Advertisements ankündigt.

Erster DNS

IPv6-Adresse des ersten IPv6-DNS-Servers (Recursive DNS-Server, RDNSS, nach RFC 6106) für dieses Interface.

Zweiter DNS

IPv6-Adresse des zweiten IPv6-DNS-Servers für dieses Interface.

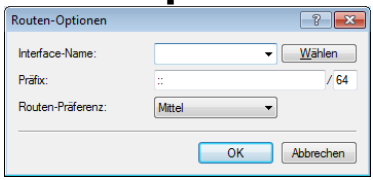
DNS-Suchliste vom internen DNS-Server importieren

Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. "intern". Die eigene Domäne ist unter **IPv4** > **DNS** > **Allgemeine Einstellungen** konfigurierbar. Die Default-Einstellung ist "aktiviert".

DNS-Suchliste vom WAN inportieren

Gibt an, ob die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Diese Funktion steht nur dann zur Verfügung, wenn in der Präfix-Liste das entsprechende WAN-Interface unter **Präfix beziehen von** verknüpft ist.

Routen-Optionen



Definiert die Routen-Option in Router-Advertisements nach RFC 4191 (Route Information Option). Möglich sind folgende Einstellungen:

Interface-Name

Definiert den Namen des logischen Interfaces, auf dem Router-Advertisements mit dieser Routen-Option gesendet werden sollen.

Präfix

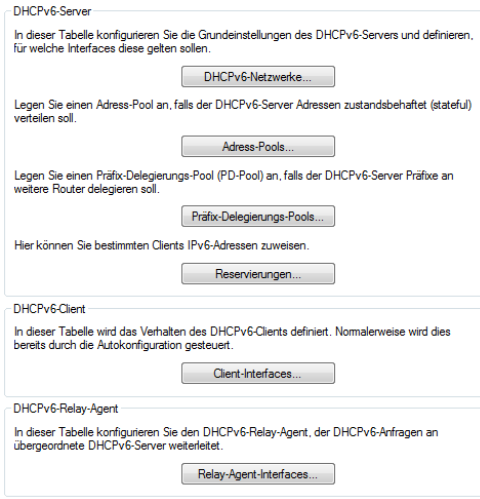
Präfix der Routen-Option, z. B. "2001:db8::/32".

Routen-Präferenz

Präferenz der Route. Mögliche Werte sind "Hoch", "Mittel" (Default) und "Niedrig".

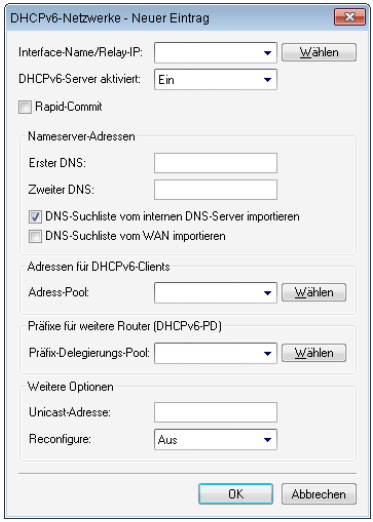
7.7.3 DHCPv6

Hier konfigurieren Sie DHCPv6-Server, den DHCPv6-Client und den DHCPv6-Relay-Agent.



DHCPv6-Netzwerke

In dieser Tabelle konfigurieren Sie die Grundeinstellungen des DHCPv6-Servers und definieren, für welche Interfaces diese gelten sollen.



Interface-Name-or-Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ hinterlegen Sie hier die IPv6-Adresse des entfernten DHCPv6 Relay-Agenten.

DHCPv6-Server aktiviert

Aktiviert bzw. deaktiviert den Eintrag.

Rapid-Commit

Bei aktiviertem Rapid-Commit antwortet der DHCPv6-Server direkt auf eine Solicit-Anfrage mit einer Reply-Nachricht.

Hinweis: Der Client muss explizit die Rapid-Commit-Option in seiner Anfrage setzen.

Erster DNS

IPv6-Adresse des ersten DNS-Servers.

Zweiter DNS

IPv6-Adresse des zweiten DNS-Servers.

DNS-Suchliste vom internen DNS-Server importieren

Gibt an, ob die DNS-Suchliste (DNS Search List) bzw. die eigene Domäne für dieses logische Netzwerk vom internen DNS-Server eingefügt werden soll, z. B. "intern". Die eigene Domäne ist unter **IPv4** > **DNS** > **Allgemeine Einstellungen** konfigurierbar. Die Default-Einstellung ist "aktiviert".

DNS-Suchliste vom WAN importieren

Gibt an, ob die vom Provider übertragende DNS-Suchliste (z. B. provider-xy.de) in diesem logischen Netzwerk angekündigt werden soll. Die Default-Einstellung ist "deaktiviert".

Adress-Pool

Name des für dieses Interface verwendeten Adress-Pools.

Hinweis: Verteilt der DHCPv6-Server seine Adressen 'stateful', müssen Sie entsprechende Adressen in die Tabelle **Adress-Pools** eintragen.

Präfix-Delegierungs-Pool

Name des Präfix-Pools, den der DHCPv6-Server verwenden soll.

Hinweis: Soll der DHCPv6-Server Präfixe an weitere Router delegieren, müssen Sie entsprechende Präfixe in der Tabelle **Präfix-Delegierungs-Pools** eintragen.

Unicast-Adresse

Standardmäßig reagiert der DHCPv6-Server ausschließlich auf Multicast-Anfragen. Wenn der DHCPv6-Server auf eine Unicast-Anfragen reagieren soll, so kann hier diese IPv6-Adresse konfiguriert werden. In der Regel reicht Multicast zur Kommunikation aus.

Reconfigure

Jede IPv6-Adresse bzw. jedes IPv6-Präfix hat eine vom Server vorgegebene Lebenszeit. In gewissen Intervallen fragt ein Client beim Server an, um seine Adresse zu verlängern (sogenannte Renew/Rebind-Zeiten).

Ändert sich aber z. B. durch Trennung und Wiederaufbau der Internetverbindung oder Anforderung eines neuen Präfixes (Telekom-Privcay-Funktion) das WAN-Präfix, so hat der Server keine Möglichkeit, die Netzwerkgeräte darüber zu informieren, dass sich Präfix bzw. Adresse geändert haben. Das bedeutet, dass ein Client noch eine alte Adresse oder ein altes Präfix verwendet und damit nicht mehr mit dem Internet kommunizieren kann.

Die Reconfigure-Funktion ermöglicht dem DHCPv6-Server, die Clients im Netzwerk zu einer Erneuerung der Leases/Bindings aufzufordern. Wenn der Client mit dem Server beim ersten Kontakt erfolgreich ein Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten *Reconfigure Key* geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so verwirft der Client diese Aufforderung zur Re-Konfiguration.

Unterstützt wird das *Reconfigure Key Authentication Protocol* nach RFC 3315 für die Optionen *Renew* und *Information-Request*, sowie *Rebind* nach RFC 6644. Das Auslösen der Rekonfiguration erfolgt auf der Konsole des Gerätes durch einen do-Befehl im Status-Baum:

```
do /Status/IPv6/DHCPv6/Server/Reconfigure
```

Die Reconfigure-Funktion erwartet im Anschluss folgende Parameter:

- `renew`: (optional, Default) Fordert den Client auf, ein Renew für seine Adresse und/oder sein Präfix durchzuführen.
- `rebind`: (optional) Fordert den Client auf, ein Rebind für seine Adresse und/oder sein Präfix durchzuführen.
- `info`: (optional) Fordert den Client auf, ein Information-Request zu senden, um z. B. seinen DNS-Server zu aktualisieren.
- `-c <Client-ID>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Client-ID.
- `-b <Adresse/Präfix>`: Die Reconfigure-Funktion gilt für den Client mit der angegebenen Adresse bzw. dem angegebenen Präfix.
- `-i <Interface/Relay>`: Die Reconfigure-Funktion gilt allen Clients, die am angegebenen Interface bzw. Relay angeschlossen sind.
- `-a`: Die Reconfigure-Funktion gilt für alle Clients.

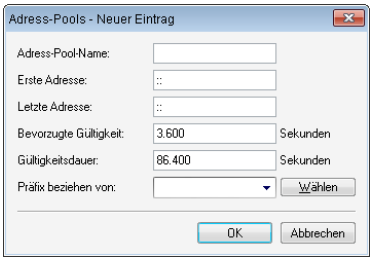
Hinweis: Den Status eines Clients in Bezug auf Reconfigure finden Sie unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Clients**.

In LANconfig stehen Ihnen folgende Einstellungen für das Reconfigure zur Auswahl:

- **Aus**: Deaktiviert die Reconfigure-Funktion.
- **Zurückweisen**: Clients, die die Reconfigure-Option in Anfragen gesetzt haben, werden vom Server abgelehnt und erhalten keine Adressen, Präfixe oder andere Optionen.
- **Erlauben**: Hat ein Client die Reconfigure-Option in Anfragen gesetzt, so verhandelt der Server mit dem Client die nötigen Parameter, um zu einem späteren Zeitpunkt ein Reconfigure zu starten.
- **Erforden**: Clients müssen die Reconfigure-Option in ihren Anfragen setzen, sonst lehnt der Server diese Clients ab. Dieser Modus ist dann sinnvoll, wenn Sie sichergehen wollen, dass der Server ausschließlich Clients bedient, die Reconfigure unterstützen. Dadurch ist gewährleistet, dass alle Clients zu einem späteren Zeitpunkt erfolgreich durch Reconfigure ihre Adressen, Präfixe oder weiteren Informationen aktualisieren können.

Adress-Pools

In dieser Tabelle definieren Sie einen Adress-Pool, falls der DHCPv6-Server Adressen stateful verteilen soll:



Adress-Pool-Name

Name des Adress-Pools

Erste Adresse

Erste Adresse des Pools, z. B. "2001:db8::1"

Letzte Adresse

Letzte Adresse des Pools, z. B. "2001:db8::9"

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'gültig' verwenden soll.

Hinweis: Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Mit diesem Parameter können Sie den Netzwerk-Clients Adressen aus dem Präfix zuteilen, das der Router vom WAN-Interface per

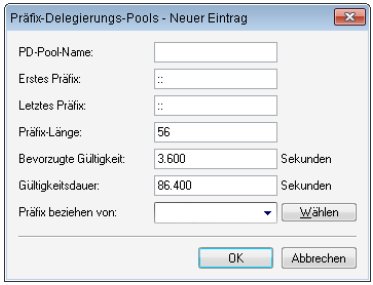
DHCPv6-Präfix-Delegation vom Provider bezogen hat. Wählen Sie hier das entsprechende WAN-Interface aus. Hat der Provider beispielsweise das Präfix "2001:db8::/64" zugewiesen, dann können Sie beim Parameter **Erste Adresse** den Wert "::1" und bei **Letzte Adresse** den Wert "::9" eingeben. Zusammen mit dem vom Provider delegierten Präfix "2001:db8::/64" erhalten Clients dann Adressen aus dem Pool "2001:db8::1" bis "2001:db8::9". Ist das Provider-Präfix größer als "/64", z. B. "/48" oder "56", so müssen Sie das Subnetting für das logische Netzwerk in den Adressen berücksichtigen. **Beispiel:**

- Zugewiesenes Provider-Präfix: "2001:db8:abcd:aa::/56"
- "/64" als Präfix des logischen Netzwerks (Subnetzt-ID 1): "2001:db8:abcd:aa01::/64"
- Erste Adresse: "0:0:0:0001::1"
- Letzte Adresse: "0:0:0:0001::9"

Hinweis: Sie sollten diesen Mechanismus nur verwenden, wenn der Provider ein festes Präfix zuweist. Ansonsten kann es passieren, dass der Provider dem Router ein neues Präfix delegiert hat, aber der Client noch eine Adresse aus dem Pool mit dem alten Präfix besitzt. Dazu muss der Client seine Adresse beim Server aktualisieren.

Präfix-Delegierungs-Pools

In dieser Tabelle bestimmen Sie Präfixe, die der DHCPv6-Server an weitere Router delegieren soll:



PD-Pool-Name

Name des PD-Pools

Erstes Präfix

Erstes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:1100::"

Letztes Präfix

Letztes zu delegierendes Präfix im PD-Pool, z. B. "2001:db8:FF00::"

Präfix-Länge

Länge der Präfixe im PD-Pool, z. B. "56" oder "60"

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client dieses Präfix als 'gültig' verwenden soll.

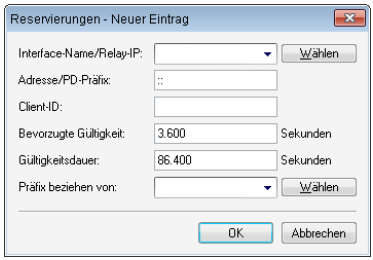
Hinweis: Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Reservierungen

Wenn Sie Clients feste IPv6-Adressen oder Routern feste Präfixe zuweisen wollen, können Sie in dieser Tabelle pro Client eine Reservierung vornehmen:



Interface-Name-oder Relay

Name des Interfaces, auf dem der DHCPv6-Server arbeitet, z. B. "INTRANET". Alternativ können Sie auch die IPv6-Adresse des entfernten Relay-Agenten eintragen.

Adresse/PD-Präfix

IPv6-Adresse oder PD-Präfix, das Sie statisch zuweisen wollen.

Client-ID

DHCPv6-Unique-Identifier (DUID) des Clients.

Bei DHCPv6 lassen sich Clients nicht mehr wie bei DHCPv4 anhand ihrer MAC-Adresse, sondern anhand der DUID identifizieren. Die DUID lässt sich auf dem jeweiligen Client auslesen, unter Windows beispielsweise mit dem Kommandozeilen-Befehl `show dhcpv6-client` oder im WEBconfig unter **Status** > **IPv6** > **DHCPv6** > **Client** > **Client-ID**.

Arbeitet das Gerät als DHCPv6-Server, finden sich die Client-IDs der Clients mit aktuellem Bezug von IPv6-Adressen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **Adress-Zuteilungen**, bzw. mit aktuellem Bezug von IPv6-Präfixen unter **Status** > **IPv6** > **DHCPv6** > **Server** > **PD-Zuteilungen**.

Der LANmonitor zeigt die Client-IDs der Clients unter **DHCPv6-Server** an.

Bevorzugte Gültigkeit

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'bevorzugt' verwenden soll. Nach Ablauf dieser Zeit führt ein Client diese Adresse als 'deprecated'.

Gültigkeitsdauer

Bestimmen Sie hier die Zeit in Sekunden, die der Client diese Adresse als 'gültig' verwenden soll.

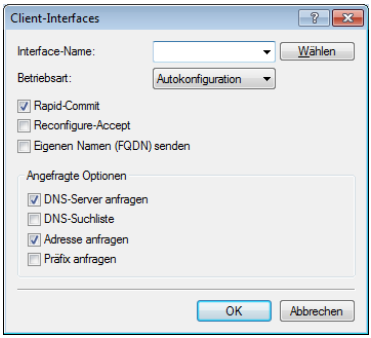
Hinweis: Wenn Sie ein Präfix eines WAN-Interfaces zu dynamischen Bildung der Adressen verwenden, ist das Konfigurieren der Werte `Bevorzugte Gültigkeit` und `Gültigkeitsdauer` gesperrt. In diesem Fall ermittelt das Gerät diese Werte automatisch aus den vorgegebenen Werte des delegierten Präfixes des Providers.

Präfix beziehen von

Name des WAN-Interfaces, von dem der Client das Präfix zur Adress- bzw. Präfixbildung verwenden soll.

Client-Interfaces

Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Clients.



Hinweis: Normalerweise steuert bereits die Autokonfiguration das Client-Verhalten. Deshalb sind in dieser Tabelle nur Einträge nötig, falls Sie den Client 'Standalone' betreiben oder bestimmte Optionen, die von den Standard-Einstellungen abweichen, verwenden wollen.

Interface-Name

Name des Interfaces, auf dem der DHCPv6-Client arbeitet Dies können LAN-Interfaces oder WAN-Interfaces (Gegenstellen) sein, z. B. "INTRANET" oder "INTERNET".

Betriebsart

Bestimmt, wie und ob das Gerät den Client aktiviert. Mögliche Werte sind:

- "Autokonfiguration": Das Gerät wartet auf Router-Advertisements und startet dann den DHCPv6-Client. Diese Option ist die Standardeinstellung.
- "Ja:": Das Gerät startet den DHCPv6-Client sofort, sobald die Schnittstelle aktiv wird, ohne auf Router-Advertisements zu warten. Dabei ignoriert das Gerät die Vorgaben aus Router-Advertisements.
- "Nein:": Der DHCPv6-Client ist auf diesem Interface deaktiviert. Auch, wenn das Gerät Router-Advertisements empfängt, startet es den Client nicht.

Rapid-Comment

Bei aktiviertem Rapid-Commit versucht der Client, mit nur zwei Nachrichten vom DHCPv6-Server eine IPv6-Adresse zu erhalten. Ist der DHCPv6-Server entsprechend konfiguriert, antwortet er auf diese Solicit-Anfrage sofort mit einer Reply-Nachricht.

Reconfigure-Accept

Wenn der Client mit dem Server beim ersten Kontakt erfolgreich ein Re-Konfiguration (Reconfigure) ausgehandelt hat, dann kann der Server den Client jederzeit auffordern, seine Adresse oder andere Informationen zu aktualisieren. Der Mechanismus wird durch den sogenannten 'Reconfigure Key' geschützt, so dass nur der ursprüngliche Server mit dem richtigen Schlüssel den Client auffordern kann. Erhält der Client eine Reconfigure-Nachricht ohne gültigen Reconfigure-Key, so verwirft der Client diese Aufforderung zur Re-Konfiguration. Der Client unterstützt dazu das 'Reconfigure Key Authentication Protocol' nach RFC 3315 für die Optionen 'Renew' und 'Information-Request', sowie 'Rebind' nach RFC 6644.

Für WAN-Interfaces ist diese Option standardmäßig aktiviert.

Eigenen Namen (FQDN) senden

Der Client sendet den eigenen Hostnamen (Fully Qualified Domain Name). Diese Option ist standardmäßig auf LAN-Interfaces aktiv.

DNS-Server anfragen

Legt fest, ob der Client beim DHCPv6-Server nach DNS-Servern fragen soll.

Hinweis: Sie müssen diese Option aktivieren, damit das Gerät Informationen über einen DNS-Server erhält.

DNS-Suchliste

Der Client fragt die DNS-Suchliste an.

Adresse anfragen

Legt fest, ob der Client beim DHCPv6-Server nach einer IPv6-Adresse fragen soll.

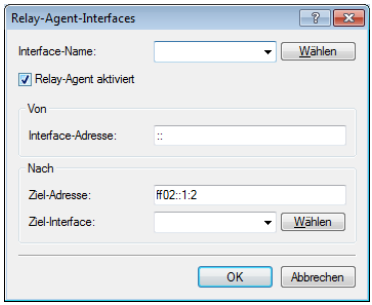
Hinweis: Diese Option sollten Sie nur dann aktivieren, wenn der DHCPv6-Server die Adressen über dieses Interface stateful, d. h. nicht durch 'SLAAC', verteilt.

Präfix anfragen

Legt fest, ob der Client beim DHCPv6-Server nach einem IPv6-Präfix anfragen soll. Eine Aktivierung dieser Option ist nur dann sinnvoll, wenn das Gerät selber als Router arbeitet und Präfixe weiterverteilt. Auf WAN-Interfaces ist diese Option standardmäßig aktiviert, damit der DHCPv6-Client ein Präfix beim Provider anfragt, das er ins lokale Netzwerk weiterverteilen kann. Auf LAN-Interfaces ist diese Option standardmäßig deaktiviert, weil ein Gerät im lokalen Netzwerk eher als Client und nicht als Router arbeitet.

Relay-Agent-Interfaces

Ein DHCPv6-Relay-Agent leitet DHCP-Nachrichten zwischen DHCPv6-Clients und DHCPv6-Servern weiter, die sich in unterschiedlichen Netzwerken befinden. Definieren Sie in dieser Tabelle das Verhalten des DHCPv6-Relay-Agents.



Interface-Name

Name des Interfaces, auf dem der Relay-Agent Anfragen von DHCPv6-Clients entgegennimmt, z. B. "INTRANET".

Relay-Agent aktiviert

Bestimmt, wie und ob das Gerät den Relay-Agent aktiviert. Mögliche Werte sind:

- "Ja:" Relay-Agent ist aktiviert. Diese Option ist die Standardeinstellung.
- "Nein:" Relay-Agent ist nicht aktiviert.

Interface-Adresse

Eigene IPv6-Adresse des Relay-Agents auf dem Interface, das unter Interface-Name konfiguriert ist. Diese IPv6-Adresse wird als Absenderadresse in den weitergeleiteten DHCP-Nachrichten verwendet. Über diese Absenderadresse kann ein DHCPv6-Server einen Relay-Agenten eindeutig identifizieren. Die explizite Angabe der Interface-Adresse ist nötig, da ein IPv6-Host durchaus mehrere IPv6-Adressen pro Schnittstelle haben kann.

Ziel-Adresse

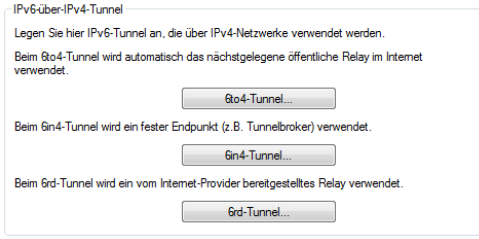
IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder Linklokale Multicast-Adresse sein. Bei Verwendung einer Linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der Linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

Ziel-Interface

Das Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine Linklokale Multicast-Adresse konfiguriert wird, da Linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

7.7.4 Tunnel

In der Konfiguration **Tunnel** legen Sie über 3 Schaltflächen IPv6-Tunnel an, die über IPv4-Netzwerke verwendet werden. Dies benötigen Sie, um den Zugang zum IPv6-Internet über eine IPv4-Verbindung herzustellen.



- **6to4-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6to4-Tunneln.

  Hinweis: Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Geräts hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen über einen 6to4-Tunnel **ausschließlich für Testzwecke** geeignet. Vermeiden Sie insbesondere Datenverbindungen über einen 6to4-Tunnel für den Einsatz in Produktivsystemen oder die Übertragung sensibler Daten.

- **6in4-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6in4-Tunneln.

  Hinweis: 6in4-Tunnel haben einen höheren administrativen Aufwand, stellen aber eine sichere und stabile Technologie für einen IPv6-Internetzugang dar. Diese Möglichkeit ist auch für den professionellen Einsatz geeignet.

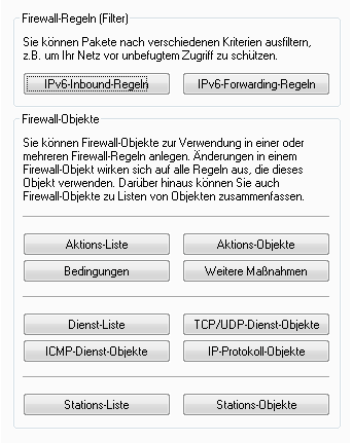
- **6rd-Tunnel**: Diese Schaltfläche öffnet die Einstellung von 6rd-Tunneln.

  Hinweis: 6rd-Tunnel sind sowohl für Endanwender als auch für den professionellen Einsatz geeignet, da es nicht den Konfigurationsaufwand von 6in4-Tunneln erfordert, aber dennoch nicht die Sicherheitsrisiken von 6to4-Tunneln hat.

7.8 Tutorials

7.8.1 Konfiguration der IPv6-Firewall-Regeln

Mit LANconfig können Sie die Firewall-Regeln unter **Firewall/QoS** > **IPv6-Regeln** festlegen.



Standardmäßig sind bereits einige Objekte und Listen für die wichtigsten Anwendungsfälle vorgegeben.

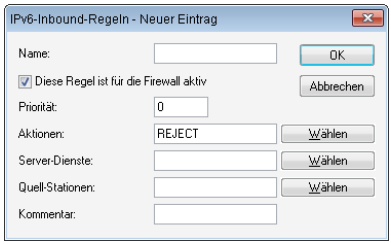
Hinweis: Sie können Listen oder Objekte nicht löschen, wenn die Firewall diese in einer Forwarding- oder Inbound-Regel verwendet.

IPv6-Inbound-Regeln

Über die Schaltfläche **IPv6-Inbound-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den ankommenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

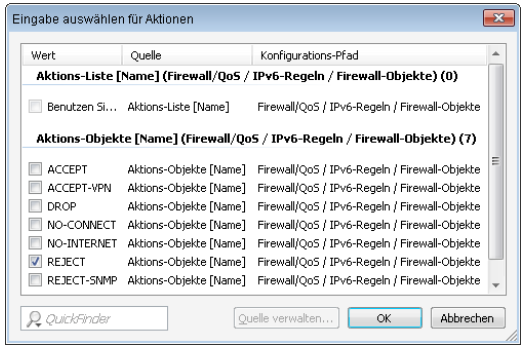
Aktiviert die Regel.

Priorität

Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken

anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Server-Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

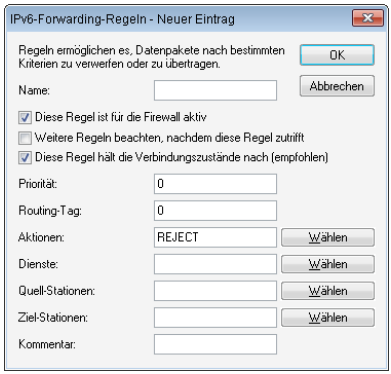
IPv6-Forwarding-Regeln

Über die Schaltfläche **IPv6-Forwarding-Regeln** legen Sie Regeln fest, nach denen die IPv6-Firewall den weiterzuleitenden Datenverkehr behandeln soll.

Standardmäßig sind bereits einige Regeln für die wichtigsten Anwendungsfälle vorgegeben.

Um die Reihenfolge der Regeln zu ändern, markieren Sie in der Tabelle die entsprechende Regel und verschieben diese über einen Klick auf eine Pfeil-Schaltfläche nach oben oder unten in der Tabelle. Die Firewall wendet die Regel nacheinander von oben nach unten an.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen der Regel.

Diese Regel ist für die Firewall aktiv

Aktiviert die Regel.

Weitere Regeln beachten, nachdem diese Regel zutrifft

Wenn Sie diese Option aktivieren, führt die Firewall zusätzlich die nachfolgenden Regeln der Liste aus. Das ist dann sinnvoll, wenn die Firewall z. B. zunächst eine Gruppen-Regel und anschließend jeweils eine Regel für die einzelnen Gruppen-Objekte anwenden soll.

Diese Regel hält die Verbindungszustände nach (empfohlen)

Aktivieren Sie diese Option, wenn die Regel die TCP-Verbindungszustände nachhalten soll.

Priorität

Bestimmt die Priorität der Regel: Je höher der Wert, desto höher die Priorität.

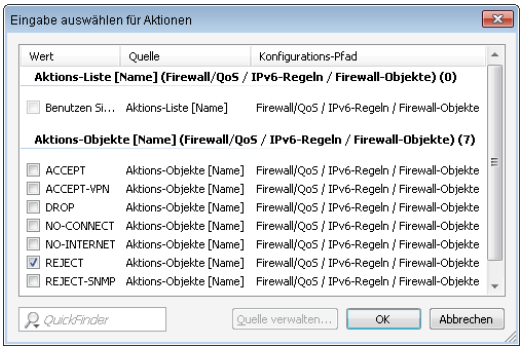
Routing-Tag

Tragen Sie hier als Schnittstellen-Tag einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, die das Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnitt-

stellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen.

Aktionen

Bestimmt die Aktion, die die Firewall bei gültiger Regel ausführen soll. Über **Wählen** können Sie aus einer Liste eine Aktion oder eine Aktions-Liste auswählen.



Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Server-Dienste

Bestimmt die Dienste, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Dienst oder eine Dienste-Liste auswählen.

Quell-Stationen

Bestimmt die Quell-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

Ziel-Stationen

Bestimmt die Ziel-Stationen, auf die die Firewall die Regel anwenden soll. Über **Wählen** können Sie aus einer Liste einen Station oder eine Stations-Liste auswählen.

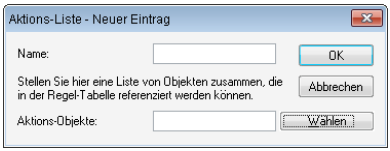
Kommentar

Vergeben Sie hier eine aussagefähige Beschreibung der Filterregel.

Aktions-Liste

Über die Schaltfläche **Aktions-Liste** können Sie Aktionen zu Gruppen zusammenfassen. Die Aktionen definieren Sie vorher unter **Aktions-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Regel festzulegen.



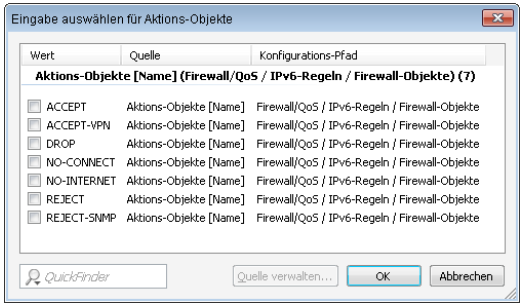
Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Aktions-Objekte

Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.



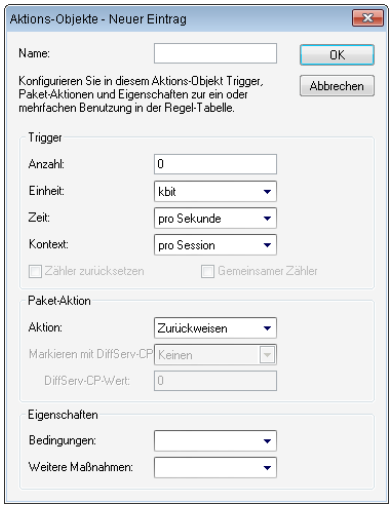
Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen

Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Aktions-Objekte

Über die Schaltfläche **Aktions-Objekte** definieren Sie Aktionen, die die IPv6-Firewall bei gültiger Filterregel ausführen kann.

Klicken Sie auf **Hinzufügen...**, um eine neue Aktion festzulegen.



Sie können die folgenden Eigenschaften des Objektes bestimmen:

Name

Bestimmt den Namen des Objektes.

Anzahl

Bestimmt das Limit, bei dessen Überschreiten die Firewall die Aktion ausführt.

Einheit

Bestimmt die Einheit des Limits. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zeit

Bestimmt, für welchen Messzeitraum die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Kontext

Bestimmt, in welchem Kontext die Firewall das Limit ansetzt. Wählen Sie im Drop-Down-Menü den entsprechenden Wert aus.

Zähler zurücksetzen

Wenn Sie diese Option aktivieren, setzt die Firewall den Zähler nach Ausführen der Aktion wieder zurück.

Hinweis: Diese Option können Sie nur aktivieren, wenn Sie unter **Zeit** den Wert "absolut" ausgewählt haben.

Gemeinsamer Zähler

Wenn Sie diese Option aktivieren, zählt die Firewall alle Aktions-Trigger gemeinsam.

Hinweis: Diese Option können Sie nur aktivieren, wenn Sie unter **Kontext** die Werte "pro Station" oder "global" ausgewählt haben.

Aktion

Bestimmt die Aktion, die die Firewall bei Erreichen des Limits ausführt.

Die folgende Auswahl ist möglich:

- **Zurückweisen**: Die Firewall weist das Datenpaket zurück und sendet einen entsprechenden Hinweis an den Absender.
- **Verwerfen**: Die Firewall verwirft das Datenpaket ohne Benachrichtigung.
- **Übertragen**: Die Firewall akzeptiert das Datenpaket.

Markieren mit DiffServ-CP

Bestimmt die Priorität der Datenpakete (Differentiated Services, DiffServ), mit der die Firewall die Datenpakete übertragen soll.

Hinweis: Diese Option können Sie nur festlegen, wenn Sie unter **Aktion** den Wert "Übertragen" ausgewählt haben.

Hinweis: Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

Hinweis: Diese Option können Sie nur festlegen, wenn Sie unter **Markieren mit DiffServ-CP** den Wert "Wert" ausgewählt haben.

Bedingungen

Bestimmt, welche Bedingung zusätzlich zur Ausführung der Aktion erfüllt sein müssen. Die Bedingungen können Sie unter **Bedingungen** definieren.

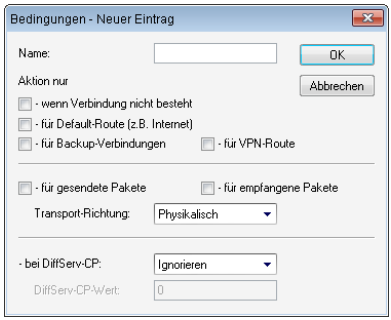
Weitere Maßnahmen

Bestimmt, welche Trigger-Aktionen die Firewall zusätzlich zur Filterung der Datenpakete starten soll. Die Trigger-Aktionen können Sie unter **Weitere Maßnahmen** definieren.

Bedingungen

Über die Schaltfläche **Bedingungen** definieren Sie Bedingungen, die zum Anwenden der Forwarding- und Inbound-Regeln erfüllt sein müssen.

Klicken Sie auf **Hinzufügen...**, um eine neue Bedingung festzulegen.



Sie können die folgenden Eigenschaften der Bedingung bestimmen:

Name

Bestimmt den Namen des Objektes.

Aktion nur - wenn Verbindung nicht besteht

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn keine Verbindung besteht.

Aktion nur - für Default-Route (z. B. Internet)

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn die Verbindung über die Default-Route besteht.

Aktion nur - für Backup-Verbindungen

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine Backup-Verbindung handelt.

Aktion nur - für VPN-Route

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um eine VPN-Verbindung handelt.

Aktion nur - für gesendete Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um gesendete Datenpakete handelt.

Aktion nur - für empfangene Pakete

Aktivieren Sie diese Option, wenn die Firewall die Aktion nur ausführen soll, wenn es sich um empfangene Datenpakete handelt.

Transport-Richtung

Bestimmt, ob die Transportrichtung sich auf den logischen Verbindungsaufbau oder die physikalische Datenübertragung über das jeweilige Interface bezieht.

Aktion nur - bei DiffServ-CP

Bestimmt, welche Priorität die Datenpakete (Differentiated Services, DiffServ) besitzen müssen, damit die Bedingung erfüllt ist.

Hinweis: Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

DiffServ-CP-Wert

Bestimmt den Wert für den Differentiated Services Code Point (DSCP).

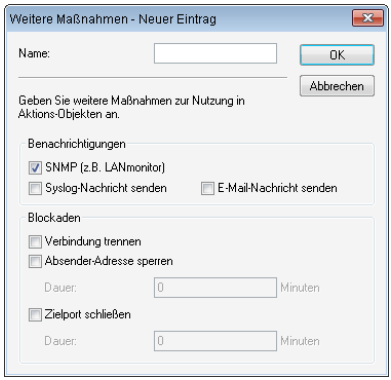
Geben Sie hier einen Wert ein, wenn Sie im Feld **- bei DiffServ-CP** die Option "Wert" ausgewählt haben.

Hinweis: Weitere Informationen zu den DiffServ-CodePoints finden Sie im Referenzhandbuch im Kapitel “QoS”.

Weitere Maßnahmen

Über die Schaltfläche **Weitere Maßnahmen** definieren Sie weitere Maßnahmen, die die Firewall nach Anwenden der Forwarding- und Inbound-Regeln ausführen kann.

Klicken Sie auf **Hinzufügen...**, um eine neue Maßnahme festzulegen.



Sie können die folgenden Eigenschaften der Trigger-Aktion bestimmen:

Name

Bestimmt den Namen des Objektes.

SNMP (z. B. LANmonitor)

Aktivieren Sie diese Option, wenn die Firewall eine Benachrichtigung über SNMP versenden soll. Diese Benachrichtigung können Sie z. B. mit LANmonitor empfangen.

SYSLOG-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine SYSLOG-Nachricht versenden soll.

Hinweis: Weitere Informationen zu SYSLOG finden Sie im Referenzhandbuch im Kapitel "Diagnose" im Abschnitt "SYSLOG".

E-Mail-Nachricht senden

Aktivieren Sie diese Option, wenn die Firewall eine E-Mail-Nachricht versenden soll.

Hinweis: Wenn Sie eine Benachrichtigung per E-Mail erhalten möchten, müssen Sie unter **Firewall/QoS** > **Allgemein** > **Administrator E-Mail** eine entsprechende E-Mail-Adresse angeben.

Verbindung trennen

Aktivieren Sie diese Option, wenn die Firewall die Verbindung trennen soll.

Absender-Adresse sperren

Aktivieren Sie diese Option, wenn die Firewall die Absender-Adresse sperren soll. Die Firewall trägt die gesperrte IP-Adresse, die Sperrzeit sowie die zugrunde liegende Regel in die **Hostsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

Dauer

Wenn die Firewall den Absender sperren soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert "0" deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Zielport schließen

Aktivieren Sie diese Option, wenn die Firewall den Ziel-Port sperren soll. Die Firewall trägt die gesperrte Ziel-IP-Adresse, das Protokoll, den Ziel-Port, die Sperrzeit sowie die zugrunde liegende Regel in die **Portsperrliste** unter **Status** > **IPv6** > **Firewall** ein.

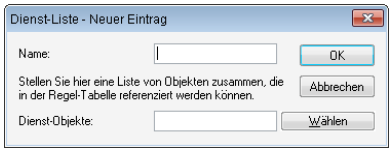
Dauer

Wenn die Firewall den Zielport schließen soll, können Sie hier die Dauer der Sperrung in Minuten festlegen. Der Wert "0" deaktiviert die Sperre, da die Sperrzeit praktisch nach 0 Minuten abläuft.

Dienst-Liste

Über die Schaltfläche **Dienst-Liste** können Sie Dienste zu Gruppen zusammenfassen. Die Dienste definieren Sie vorher unter **TCP/UDP-Dienst-Objekte**, **ICMP-Dienst-Objekte** und **IP-Protokoll-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Dienst-Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Dienst-Objekte

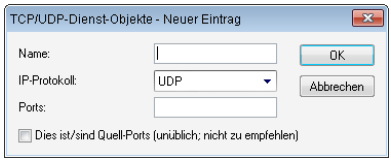
Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

TCP/UDP-Dienst-Objekte

Über die Schaltfläche **TCP/UDP-Dienst-Objekte** definieren Sie TCP/UDP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen...**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

IP-Protokoll

Bestimmt das Protokoll des Dienstes

Ports

Bestimmt die Ports des Dienstes. Trennen Sie mehrere Ports jeweils durch ein Komma.

Hinweis: Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Dies ist/sind Quell-Ports

Bestimmt, ob es sich bei den angegebenen Ports um Quell-Ports handelt.

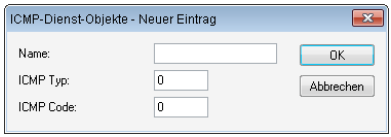
Hinweis: In bestimmten Szenarien kann es sinnvoll sein, einen Quell-Port anzugeben. Normalerweise ist es aber unüblich, so dass die Auswahl "nein" zu empfehlen ist.

ICMP-Dienst-Objekte

Über die Schaltfläche **ICMP-Dienst-Objekte** definieren Sie ICMP-Dienste, die die IPv6-Firewall für Filterregeln verwenden kann.

Hinweis: Listen mit den offiziellen ICMP-Typen und -Codes finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen...**, um einen neuen Dienst festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

ICMP Typ

Bestimmt den Typ des ICMP-Dienstes.

ICMP Code

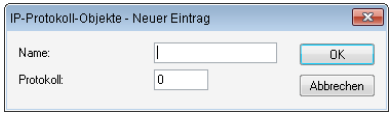
Bestimmt den Code des ICMP-Dienstes.

IP-Protokoll-Objekte

Über die Schaltfläche **IP-Protokoll-Objekte** definieren Sie Internet-Protokoll-Objekte, die die IPv6-Firewall für Filterregeln verwenden kann.

Hinweis: Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter *www.iana.org*.

Klicken Sie auf **Hinzufügen...**, um ein neues Objekt festzulegen.



Sie können die folgenden Eigenschaften der Regel bestimmen:

Name

Bestimmt den Namen des Objektes.

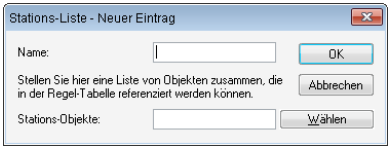
Protokoll

Bestimmt die Protokoll-Nummer.

Stations-Liste

Über die Schaltfläche **Stations-Liste** können Sie Stationen zu Gruppen zusammenfassen. Die Stationen definieren Sie vorher unter **Stations-Objekte**.

Klicken Sie auf **Hinzufügen...**, um eine neue Liste festzulegen.



Sie können die folgenden Eigenschaften einer Liste festlegen:

Name

Bestimmt den Namen der Liste.

Stations-Objekte

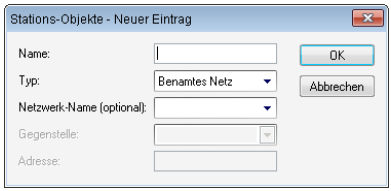
Bestimmt die Objekte, die sie in dieser Liste zusammenfassen möchten. Über **Wählen** können Sie aus einer Liste ein oder mehrere Objekte auswählen.

Wenn Sie hier einen neuen Eintrag eingeben, taucht dieser zunächst unter **Unbekannte Quelle** auf. Markieren Sie anschließend den Eintrag einer Quelle, der Sie den neuen Eintrag zuordnen möchten und klicken anschließend auf **Quelle verwalten**. Bestimmen Sie die Werte für diesen Eintrag, und speichern Sie das neue Objekt. Der neue Eintrag taucht nun als neues Objekt in der Liste der entsprechenden Quelle auf.

Stations-Objekte

Über die Schaltfläche **Stations-Objekte** definieren Sie Stationen, die die IPv6-Firewall für Filterregeln verwenden kann.

Klicken Sie auf **Hinzufügen...**, um ein neues Objekt anzulegen.



Sie können die folgenden Eigenschaften der Objekte festlegen:

Name

Bestimmt den Namen des Objektes.

Typ

Bestimmt den Stationstyp.

Netzwerk-Name

Geben Sie hier den Namen des Netzwerkes ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Hinweis: Die Angabe eines Netzwerk-Namens ist optional.

Gegenstelle

Geben Sie hier den Namen der Gegenstelle ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

Adresse

Geben Sie hier die Adresse der Gegenstelle ein, wenn Sie im Feld **Typ** die entsprechende Option ausgewählt haben.

7.8.2 Einrichtung eines IPv6-Internetzugangs

Sie haben die Möglichkeit einen Zugang zu einem IPv6-Netz einrichten, wenn

- Sie ein IPv6-fähiges Gerät besitzen,
- eine Tunneltechnologie benutzen und
- Ihr Provider ein natives IPv6-Netz unterstützt oder Sie einen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

IPv6-Zugang über den Setup-Assistenten von LANconfig

Der Setup-Assistent unterstützt Sie bei der Konfiguration des IPv6-Zugangs für Ihre Geräte.

Folgende Optionen stehen Ihnen im Assistenten zur Verfügung:

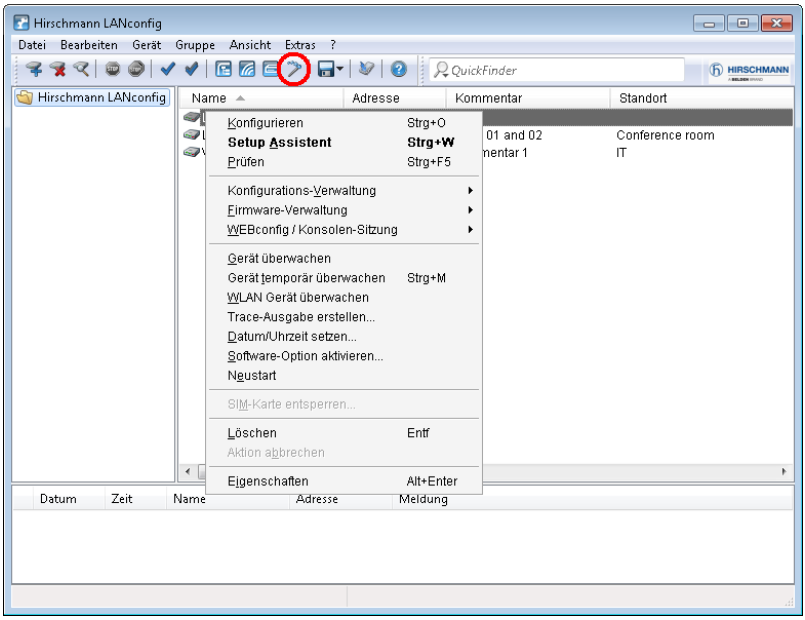
- *Den IPv6-Zugang bei einem neuen, unkonfigurierten Gerät einrichten.*
- *Bei einem bestehenden Gerät einen IPv6-Zugang zusätzlich zum bestehenden IPv4-Zugang einrichten.*

Setup-Assistent - IPv6 bei einem neuen Gerät einrichten

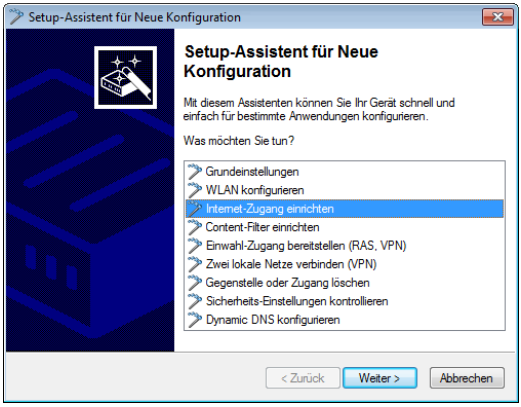
Wenn Sie ein neues Gerät angeschlossen, aber noch nicht konfiguriert haben, haben Sie die Möglichkeit per Setup-Assistent IPv4- und IPv6-Verbindungen herzustellen.

Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie nun entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste.



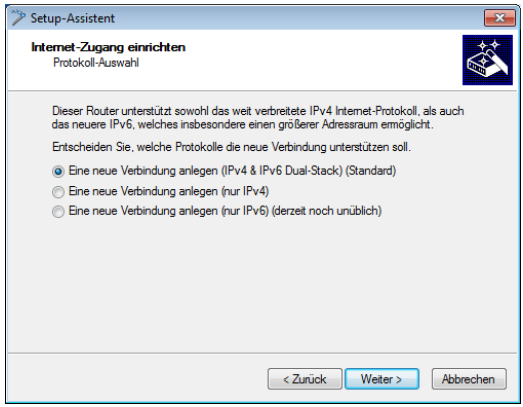
2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**.



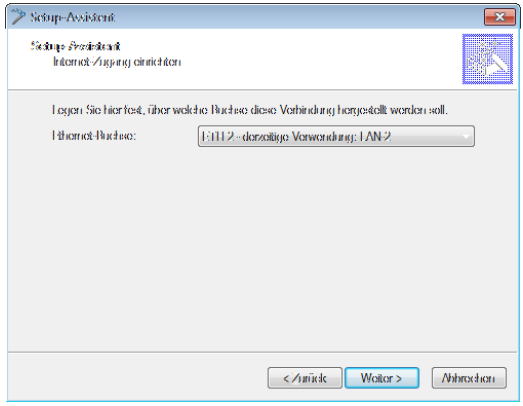
3. Sie haben die Möglichkeit, zwischen den folgenden Optionen zu wählen:

- Eine Dual-Stack-Verbindung herstellen. Diese ist IPv4- und IPv6-tauglich und daher derzeit für ein neues Gerät die empfohlene Option.
- Eine reine IPv4-Verbindung herstellen.
- Eine reine IPv6-Verbindung herstellen.

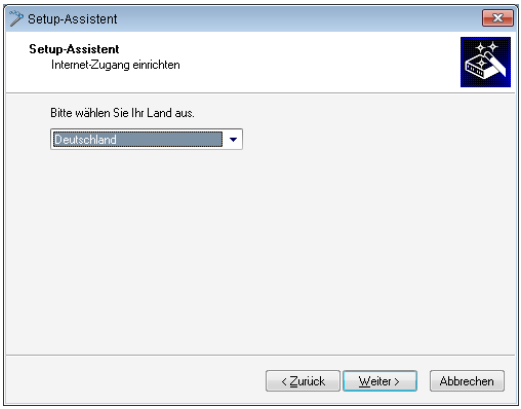
Nachfolgend führen wir Sie durch die Einrichtung einer Dual-Stack-Verbindung. Aktivieren Sie die entsprechende Auswahl.



4. Bestimmen Sie die Schnittstelle, über die Sie die Verbindung herstellen wollen.



5. Wählen Sie aus der Liste Ihr Land aus.

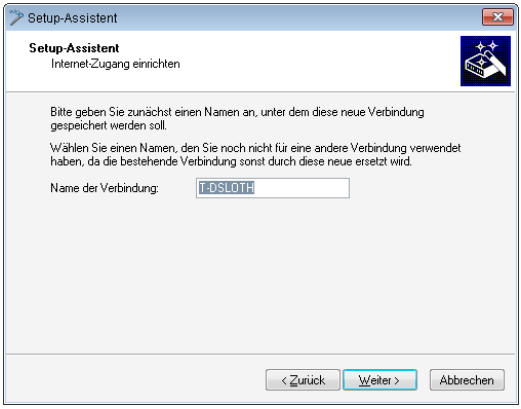


6. Wählen Sie Ihren Internet-Provider aus.

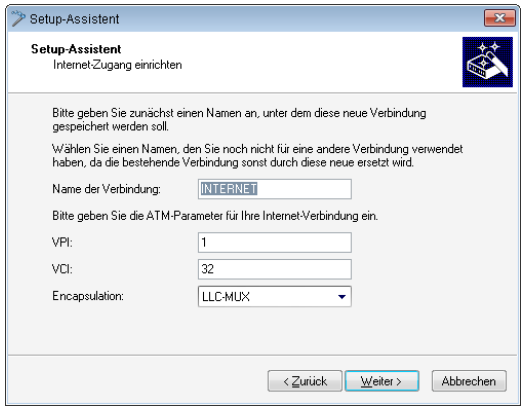
Sie haben folgende Einträge zur Auswahl:

- Eine Auswahl relevanter Internet-Provider
- Internet-Zugang über PPP over Ethernet
- Internet-Zugang über Plain IP
- Internet-Zugang über PPTP
- Internet-Zugang über Plain Ethernet

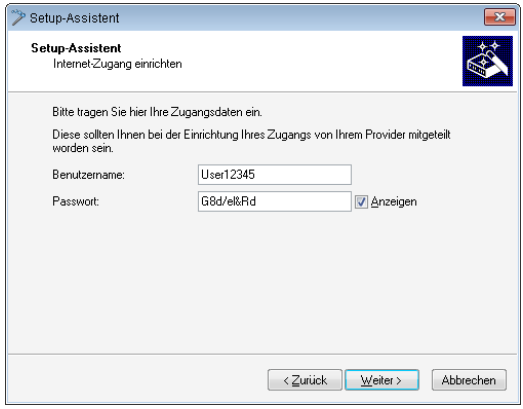
7. Definieren Sie einen Namen für diese Verbindung.



Wenn Sie den Internet-Zugang alternativ z. B. über eine PPPoE-Verbindung einrichten wollen, geben Sie zusätzlich noch die entsprechenden ATM-Parameter ein.

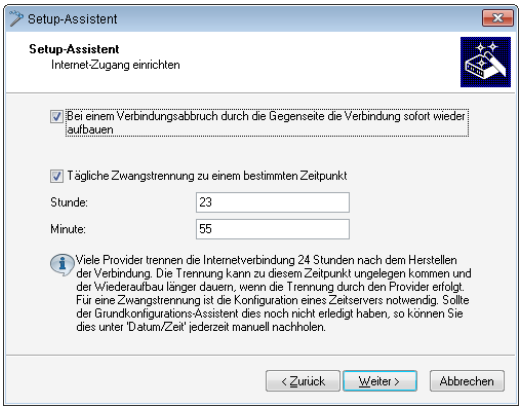


8. Tragen Sie die Zugangsdaten ein, die Ihnen Ihr Provider bei der Errichtung Ihres Internetzugangs mitgeteilt hat.

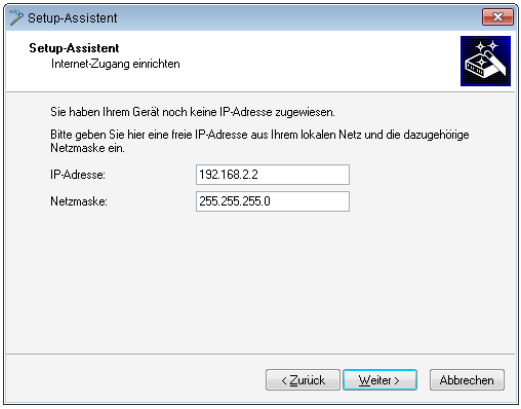


Hinweis: Je nach Provider können sich Art und Anzahl der Felder unterscheiden.

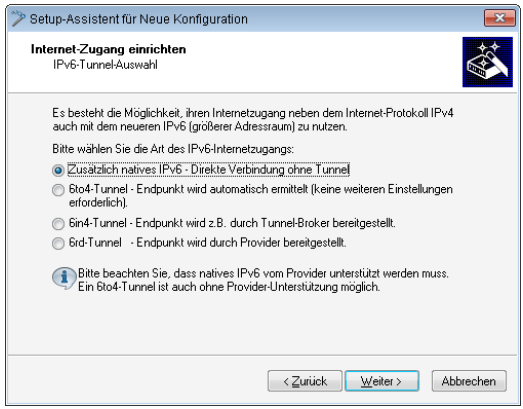
9. Legen Sie fest, wie sich das Gerät bei einem Verbindungsabbruch verhalten soll. Außerdem können Sie angeben, ob und wann das Gerät die Internetverbindung zwangsweise trennen soll.



10. Falls Ihr Gerät noch keine IP-Adresse besitzt, tragen Sie eine neue IP-Adresse sowie die entsprechende Netzmaske ein.



11. Wählen Sie die Art des IPv6-Internet-Zugangs.

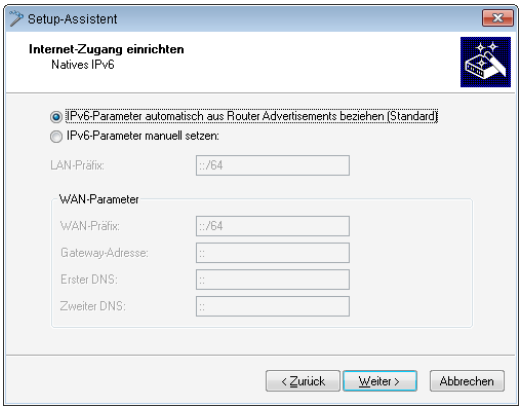


Sie haben folgende Optionen zur Auswahl:

- **Zusätzlich natives IPv6**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
- **6to4-Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-Tunnels.
- **6in4-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6in4-Tunnel.
- **6rd-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6rd-Tunnel.

Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

12. Übernehmen Sie die Default-Einstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



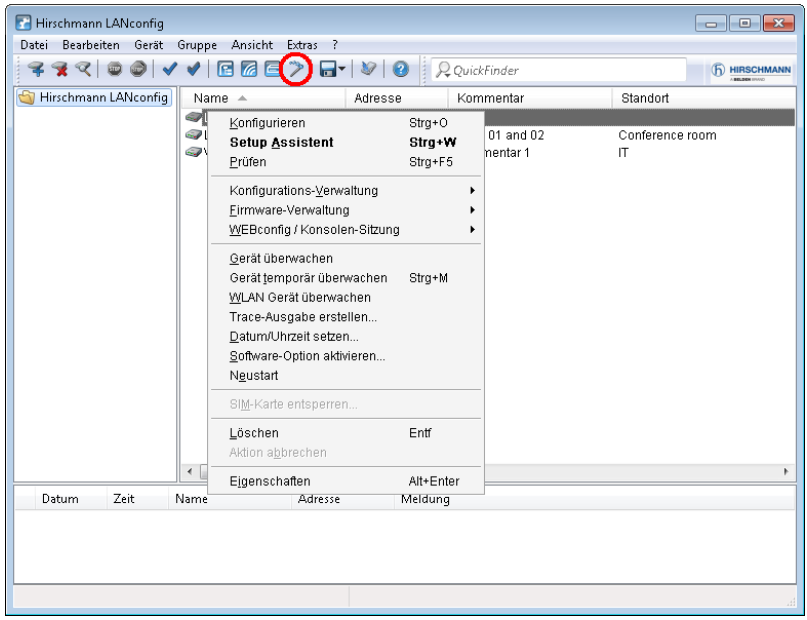
13. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

Setup-Assistent - IPv6 bei einem bestehenden Gerät einrichten

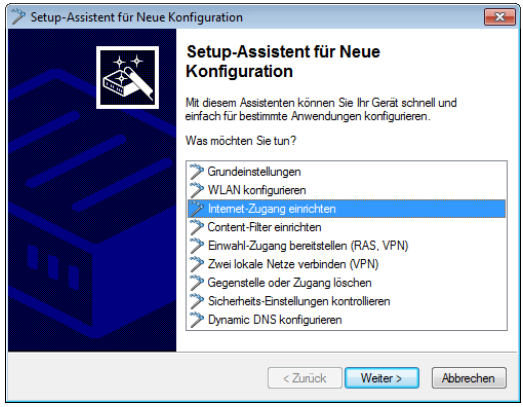
Wenn Sie ein Gerät für IPv4 konfiguriert haben und zusätzliche eine IPv6-Verbindung einrichten wollen, haben Sie die Möglichkeit, diese IPv6-Verbindungen über den Setup-Assistenten herzustellen.

Um Ihre Eingaben zu übernehmen und zum nächsten Dialog zu gelangen, klicken Sie jeweils auf **Weiter**.

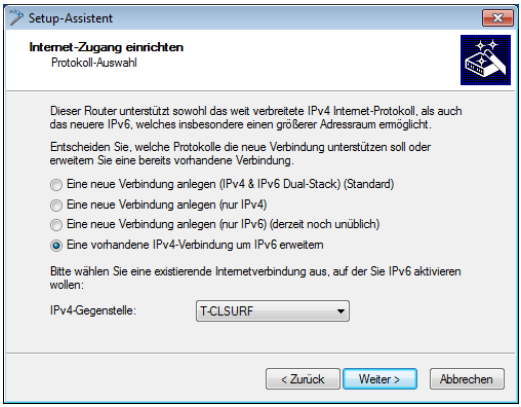
1. Starten Sie den Setup-Assistenten in LANconfig. Markieren Sie dazu das zu konfigurierende Gerät. Den Setup-Assistenten starten Sie entweder per Rechtsklick im sich öffnenden Menü oder per Zauberstab-Icon in der Symbolleiste



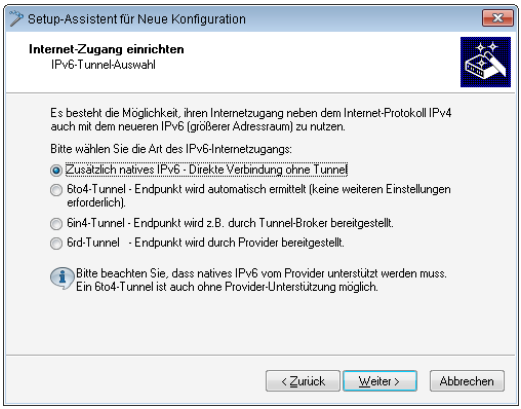
2. Wählen Sie im Setup-Assistenten die Option **Internet-Zugang einrichten**. Klicken Sie anschließend auf **Weiter**.



3. Da ihr Gerät bereits für IPv4 beherrscht, bietet der Setup-Assistent Ihnen die Möglichkeit, diese existierende Einstellung um IPv6 zu erweitern. Wählen Sie diese Option und klicken Sie anschließend auf **Weiter**.



4. Wählen Sie die Art des IPv6-Internet-Zugangs.

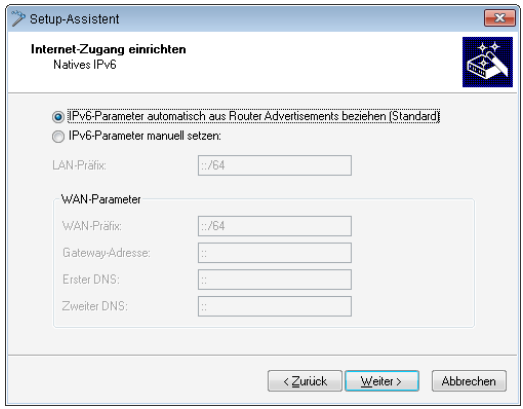


Sie haben folgende Optionen zur Auswahl:

- **Zusätzlich natives IPv6**: Konfigurieren Sie eine direkte Verbindung ohne Tunnel.
- **6to4-Tunnel**: Starten Sie den Assistenten zur Konfiguration eines 6to4-Tunnels.
- **6in4-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6in4-Tunnel.
- **6rd-Tunnel**: Bestimmen Sie in der Eingabemaske die Parameter für den 6rd-Tunnel.

Aktivieren Sie die Option für die Einrichtung einer nativen IPv6-Internet-Verbindung.

5. Übernehmen Sie die Default-Einstellung **IPv6-Parameter automatisch aus Router-Advertisements beziehen.**



6. Sie haben die Einrichtung des nativen IPv6-Internetzugangs abgeschlossen. Klicken Sie abschließend auf **Fertig stellen**, damit der Assistent Ihre Eingaben im Gerät speichern kann.

7.8.3 Einrichtung eines 6to4-Tunnels

Die Verwendung eines 6to4-Tunnels bietet sich an, wenn

- Ihr Gerät IPv6-fähig ist und Sie auf IPv6-Dienste zugreifen möchten,
- Ihr Provider jedoch kein natives IPv6-Netz unterstützt und
- Sie keinen Zugang zu einem so genannten Tunnelbroker haben, der Ihre IPv6-Datenpakete vermittelt.

Bei der Verwendung eines 6to4-Tunnels erhält das Gerät keine IPv6-Adresse bzw. kein IPv6-Präfix des Providers, da dieser keine IPv6-Funktionalität anbietet.

Das Gerät berechnet ein eigenes, eindeutiges Präfix aus "2002::/16" und der Hexadezimal-Darstellung der eigenen, öffentlichen IPv4-Adresse, die der Provider liefert. Diese Anwendung funktioniert daher ausschließlich dann, wenn das Gerät tatsächlich eine öffentliche IPv4-Adresse besitzt. Das Gerät erhält z. B. keine öffentlich gültige IPv4-Adresse, sondern nur eine IPv4-Adresse aus einem privaten Adressbereich, wenn

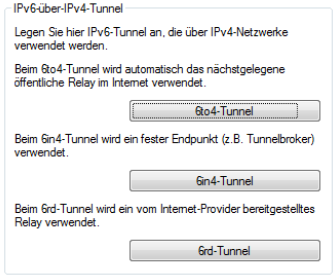
- das Gerät selbst nicht den Zugang zum Internet herstellt, sondern "hinter" einem anderen Router steht.

Hinweis: Verbindungen über einen 6to4-Tunnel nutzen Relays, die der Backbone des IPv4-Internet-Providers auswählt. Der Administrator des Geräts hat keinen Einfluss auf die Auswahl des Relays. Darüber hinaus kann sich das verwendete Relay ohne das Wissen des Administrators ändern. Aus diesem Grund sind Verbindungen über einen 6to4-Tunnel **ausschließlich für Testzwecke** geeignet. Vermeiden Sie insbesondere Datenverbindungen über einen 6to4-Tunnel für den Einsatz in Produktivsystemen oder die Übertragung sensibler Daten.

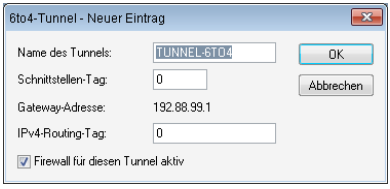
Verwendung von LANconfig

Um einen 6to4-Tunnel über LANconfig einzurichten, gehen Sie wie folgt vor:

1. Starten Sie LANconfig. LANconfig sucht nun automatisch im lokalen Netz nach Geräten.
2. Wählen Sie das Gerät aus, für das Sie den 6to4-Tunnel einrichten wollen. Markieren Sie es mit einem Links-Klick und starten Sie die Konfiguration in der Menüleiste über **Gerät** > **Konfigurieren**.
3. Wechseln Sie im Konfigurationsdialog in die Ansicht **IPv6** > **Tunnel** und klicken Sie auf **6to4-Tunnel**.



4. Klicken Sie auf **Hinzufügen**, um einen neuen 6to4-Tunnel anzulegen.

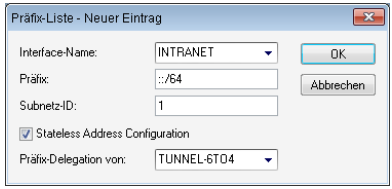


5. Vergeben Sie den Namen des 6to4-Tunnels.

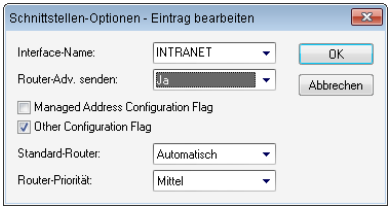
6. Tragen Sie als **Schnittstellen-Tag** einen Wert ein, der das Netzwerk eindeutig spezifiziert. Alle Pakete, welche dieses Gerät auf diesem Netzwerk empfängt, erhalten intern eine Markierung mit diesem Tag. Das Schnittstellen-Tag ermöglicht eine Trennung der für dieses Netzwerk gültigen Routen auch ohne explizite Firewall-Regel.
7. Die **Gateway-Adresse** ist per Default vorbelegt mit der Anycast-Adresse "192.88.99.1". Diese Adresse können Sie nur über WEBconfig bzw. Telnet ändern.
8. Bestimmen Sie hier das Routing-Tag, mit dem das Gerät die Route zum zugehörigen entfernten Gateway ermittelt. Das **IPv4-Routing-Tag** gibt an, über welche getaggte IPv4-Route die Datenpakete ihre Zieladresse erreichen.
9. Als Default-Wert ist die Firewall dieses Tunnels aktiv.

   Wenn Sie die globale Firewall deaktivieren, deaktivieren Sie ebenfalls die Firewall für den Tunnel.
10. Übernehmen Sie Ihre Eingaben mit **OK**.
11. Wechseln Sie in das Verzeichnis **IPv6** > **Router-Advertisements**.

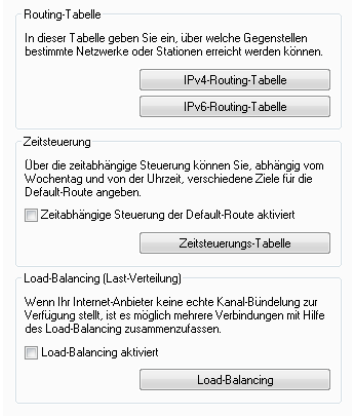
12. Öffnen Sie die **Präfix-Liste** und klicken Sie auf **Hinzufügen**.



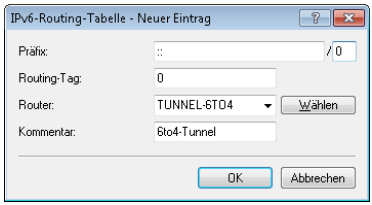
13. Vergeben Sie einen Namen für das Interface, das den 6to4-Tunnel verwenden wird, z. B. "INTRANET".
14. Bestimmen Sie als **Präfix** den Wert "::/64", um das vom Provider vergebene Präfix automatisch und in voller Länge zu übernehmen.
15. Übernehmen Sie die Default-Wert "1" für die **Subnetz-ID**.
16. Übernehmen Sie die aktivierte Option **Stateless Address Configuration**.
17. Übernehmen Sie im Feld **Präfix-Delegation von** aus der Liste den Namen des Tunnels, den Sie zuvor definiert haben, im Beispiel oben "TUNNEL-6TO4".
18. Übernehmen Sie Ihre Eingaben mit **OK**.
19. Im Verzeichnis **IPv6** > **Router-Advertisements** öffnen Sie die **Schnittstellen-Optionen** und klicken auf **Bearbeiten** für den Eintrag INTRANET.
20. Wählen Sie im Drop-Down-Menü **Router Advertisements senden** die Option "Ja".



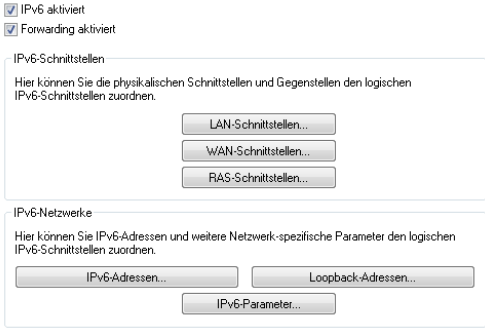
21. Übernehmen Sie alle weiteren Default-Werte unverändert.
22. Speichern Sie die Eingaben mit **OK**.
23. Wechseln Sie in das Verzeichnis **IP-Router** > **Routing**.



24. Öffnen Sie die **IPv6-Routing-Tabelle** und klicken auf **Hinzufügen**.



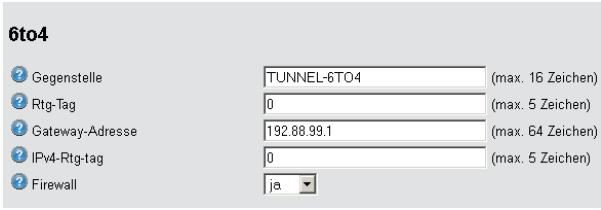
25. Vergeben Sie als **Präfix** den Wert "::/0".
26. Übernehmen Sie für **Routing-Tag** den Default-Wert "0".
27. Im Feld **Router** wählen Sie aus der Liste den Namen des Tunnels aus, den Sie definiert haben, im Beispiel oben "TUNNEL-6TO4".
28. Vergeben Sie einen aussagekräftigen **Kommentar** für diesen Eintrag.
29. Speichern Sie die Eingaben mit **OK**.
30. Wechseln Sie in das Verzeichnis **IPv6** > **Allgemein** und aktivieren Sie den IPv6-Stack.



Verwendung von WEBconfig

Um einen 6to4-Tunnel über WEBconfig einzurichten, gehen Sie wie folgt vor:

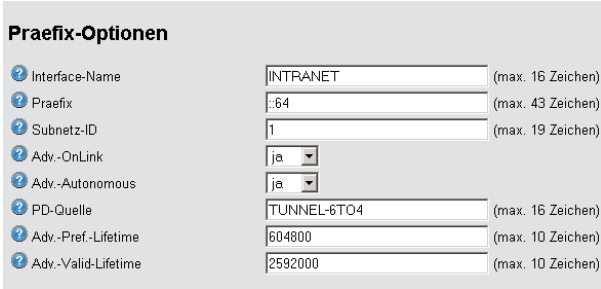
1. Geben Sie in der Adresszeile Ihres Browsers die Adresse des Gerätes ein, für das Sie den 6to4-Tunnel einrichten wollen.
2. Wechseln Sie in das Verzeichnis **HiLCOS-Menübaum** > **Setup** > **IPv6** > **Tunnel** > **6to4** und klicken Sie auf **Hinzufügen**.



3. Vergeben Sie den Namen der Gegenstelle, z. B. "TUNNEL-6TO4".
4. Das **Routing-Tag** lassen Sie unverändert auf dem Default-Wert "0".
5. Als **Gateway-Adresse** können Sie den Default-Wert "192.88.99.1" übernehmen. Das ist die Standard-Anycast-Adresse für 6to4-Relays, mit denen sich Ihr Gerät verbindet.

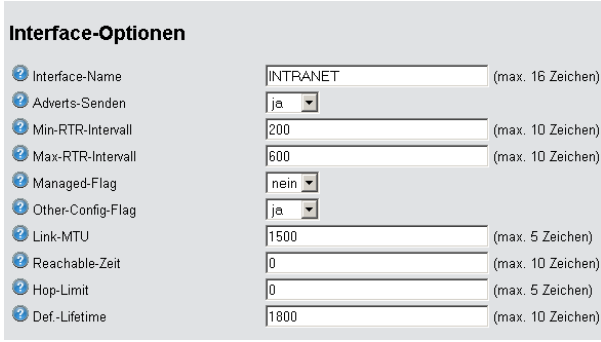
   Diese Adresse ist der Grund dafür, dass ein 6to4-Tunnel instabil und unsicher ist. Weder ist sichergestellt, dass überhaupt ein 6to4-Relay verfügbar ist, noch können Sie jedem verfügbaren 6to4-Relay vertrauen. Es gibt keine Garantie dafür, dass das verbundene Relay keine Aufzeichnung Ihres Datenverkehrs vornimmt.
6. Übernehmen Sie im Feld **IPv4-Rtg-tag** den Default-Wert "0"
7. Aktivieren Sie die **Firewall** für diesen Tunnel.

   Wenn Sie die globale Firewall deaktivieren, deaktivieren Sie ebenfalls die Firewall für den Tunnel.
8. Speichern Sie die Eingaben mit **Setzen**.
9. Wechseln Sie in das Verzeichnis **HiLCOS-Menübaum** > **Setup** > **IPv6** > **Router-Advertisement**, öffnen Sie die Tabelle **Praefix-Optionen** und klicken Sie auf **Hinzufügen**.

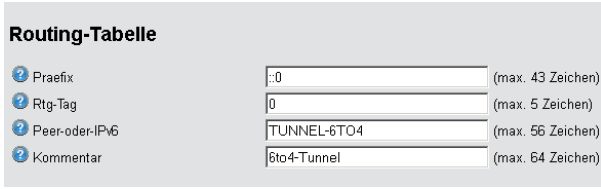


10. Vergeben Sie einen Namen für das Interface, das den 6to4-Tunnel verwendet, z. B. "INTRANET".

11. Bestimmen Sie als **Präfix** den Wert "::/64", um das vom Provider vergebene Präfix automatisch und in voller Länge zu übernehmen.
12. Übernehmen Sie den Default-Wert "1" für die **Subnetz-ID**.
13. Vergeben Sie als **PD-Quelle** den Namen der Gegenstelle, den Sie zuvor definiert haben, im Beispiel oben "TUNNEL-6TO4".
14. Speichern Sie die Eingaben mit **Setzen**.
15. Wechseln Sie in das Verzeichnis **HiLCOS-Menübaum** > **Setup** > **IPv6** > **Router-Advertisement**, öffnen Sie die Tabelle **Interface-Optionen** und klicken Sie auf **Hinzufügen**.

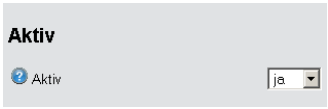


16. Übernehmen Sie alle weiteren Default-Werte unverändert.
17. Speichern Sie die Eingaben mit **Setzen**.
18. Wechseln Sie in das Verzeichnis **HiLCOS-Menübaum** > **Setup** > **IPv6**, öffnen Sie die Tabelle **Routing-Tabelle** und klicken Sie auf **Hinzufügen**.



19. Vergeben Sie als **Praefix** den Wert "::/0".
20. Übernehmen Sie für **Rtg-Tag** den Default-Wert "0".
21. Im Feld **Peer-oder-IPv6** tragen Sie den Namen des Interfaces ein, das den 6to4-Tunnel verwenden wird, im Beispiel oben "TUNNEL-6TO4".
22. Vergeben Sie einen aussagekräftigen **Kommentar** für diesen Eintrag.
23. Speichern Sie die Eingaben mit **Setzen**.

24. Aktivieren Sie den IPv6-Stack, indem Sie unter **HiLCOS-Menübaum** > **Setup** > **IPv6** die Option **Aktiv** auf "ja" einstellen und mit **Setzen** speichern.



8 Firewall

Für die meisten Firmen und viele Privatanwender ist eine Arbeit ohne das Internet nicht mehr denkbar. E-Mail und Web sind für die Kommunikation und Informationsrecherche unverzichtbar. Jede Verbindung der Rechner aus dem eigenen, lokalen Netzwerk mit dem Internet stellt aber eine potentielle Gefahr dar: Unbefugte können über diese Internet-Verbindung versuchen, Ihre Daten einzusehen, zu verändern oder Ihre Rechner zu manipulieren.

In diesem Kapitel widmen wir uns daher einem sehr wichtigen Thema: der Firewall als Abwehrmaßnahme vor diesen Zugriffen. Neben einer kurzen Einführung in das Thema Internetsicherheit zeigen wir Ihnen, welchen Schutz Ihnen ein Router bei richtiger Konfiguration bieten kann und wie Sie die entsprechenden Einstellungen konkret vornehmen.

8.1 Gefährdungsanalyse

Um die geeigneten Maßnahmen zur Gewährleistung der Sicherheit planen und umsetzen zu können, muss man sich zunächst einmal über die möglichen Gefahrenquellen im Klaren sein:

- Welche Gefahren bedrohen das eigene LAN bzw. die eigenen Daten?
- Über welche Wege verschaffen sich Eindringlinge den Zugang zu Ihrem Netzwerk?

Hinweis: Das Eindringen in geschützte Netzwerke bezeichnen wir im Weiteren dem allgemeinen Sprachgebrauch folgend als “Angriff”, den Eindringling daher auch als “Angreifer”.

8.1.1 Die Gefahren

Die Gefahren im Internet entspringen grundsätzlich ganz verschiedenen Motiven. Zum einen versuchen die Täter, sich persönlich zu bereichern oder die Opfer gezielt zu schädigen. Durch das immer stärker verbreitete Know-

How der Täter ist das “Hacken” aber auch schon zu einer Art Sport geworden, bei dem sich oft Jugendliche darin messen, wer die Hürden der Internetsicherheit am schnellsten überwindet.

Was auch immer im einzelnen Fall das Motiv ist, die Absichten der Täter laufen meistens auf die folgenden Muster hinaus:

- Einblick in vertrauliche Informationen wie Betriebsgeheimnisse, Zugangsinformationen, Passwörter für Bankkonten etc.
- Nutzung der Rechner im LAN für die Zwecke der Eindringlinge, z. B. für die Verbreitung von eigenen Inhalten, Angriffe auf dritte Rechner etc.
- Verändern der Daten auf den Rechnern im LAN, z. B. um sich auf diese Weise weitere Zugangsmöglichkeiten zu schaffen
- Zerstören von Daten auf den Rechnern im LAN
- Lahmlegen von Rechnern im LAN oder der Verbindung mit dem Internet

Hinweis: Wir beschränken uns hier auf die Angriffe auf lokale Netzwerke (LAN) bzw. auf Arbeitsplatzrechner und Server in solchen LANs.

8.1.2 Die Wege der Täter

Um ihrem Unwesen nachgehen zu können, brauchen die Täter natürlich zunächst einen Weg für den Zugriff auf Ihre Rechner und Daten. Im Prinzip stehen dazu folgende Wege offen, solange sie nicht gesperrt bzw. geschützt sind:

- Über die zentrale Internetverbindung, z. B. über einen Router
- Über dezentrale Verbindungen ins Internet, z. B. Modems an einzelnen PCs oder Mobiltelefone an Notebooks
- Über Funknetzwerke, die als Ergänzung zum drahtgebundenen Netzwerk eingesetzt werden

Hinweis: In diesem Kapitel betrachten wir ausschließlich die Wege über die zentrale Internetverbindung, über den Router.

Hinweis: Hinweise zum Schutz der Funknetzwerke entnehmen Sie bitte den entsprechenden Kapiteln dieses Referenz-Handbuchs bzw. der jeweiligen Gerätedokumentation.

8.1.3 Die Methoden

Normalerweise haben fremde Personen natürlich keinen Zugang zu Ihrem lokalen Netz oder den Rechnern darin. Ohne die entsprechenden Zugangsdaten oder Passwörter kann also niemand auf den geschützten Bereich zugreifen. Wenn das Ausspionieren dieser Zugangsdaten nicht möglich ist, versuchen die Angreifer auf einem anderen Weg zum Ziel zu kommen.

Ein grundlegender Ansatz dabei ist es, auf einem der zugelassenen Wege für den Datenaustausch Daten in das Netzwerk einzuschmuggeln, die dann von innen her den Zugang für den Angreifer öffnen. Durch Anhänge in E-Mails oder aktive Inhalte auf Webseiten kann so z. B. ein kleines Programm auf einen Rechner aufgespielt werden, der diesen anschließend zum Absturz bringt. Den Absturz nutzt das Programm dann, um einen neuen Administrator auf dem Rechner anzulegen, der anschließend aus der Ferne für weitere Aktionen im LAN genutzt werden kann.

Wenn der Zugang über E-Mail oder WWW nicht möglich ist, kann der Angreifer auch ausspähen, ob ein Server im LAN bestimmte Dienste anbietet, die er für seine Zwecke nutzen kann. Da die Dienste auf den Servern über bestimmte Ports im TCP/IP-Protokoll identifiziert werden, wird das Suchen nach offenen Ports auch als “Port-Scanning” bezeichnet. Der Angreifer startet dabei mit einem bestimmten Programm entweder allgemein im Internet oder nur auf bestimmten Netzwerken eine Anfrage nach den gewünschten Diensten und bekommt von ungeschützten Rechnern auch die entsprechende Antwort.

Eine dritte Möglichkeit besteht darin, sich in eine bestehende Datenverbindung einzuklinken und als Trittbrettfahrer zu nutzen. Dabei hört der Angreifer die Internetverbindung des Opfers ab und analysiert die Verbindungen. Eine aktive FTP-Verbindung nutzt er dann z. B., um auf dieser Verbindung seine eigenen Datenpakete mit in das zu schützende LAN zu schleusen.

Eine Variante dieser Methode ist der “man-in-the-middle”. Dabei hört der Angreifer zunächst die Kommunikation zwischen zwei Rechnern ab und klinkt sich dann dazwischen.

8.1.4 Die Opfer

Die Frage nach dem Gefährdungsgrad für einen Angriff beeinflusst in hohem Maße den Aufwand, den man für die Abwehr treffen will oder muss. Um einzuschätzen, ob Ihr Netzwerk als Opfer für einen Angreifer besonders interessant ist, können Sie folgende Kriterien heranziehen:

- Besonders gefährdet sind Netzwerke von allgemein bekannten Firmen oder Institutionen, in denen wertvolle Informationen vermutet werden. Dazu gehören z. B. die Ergebnisse einer Forschungsabteilung, die von Industriespionen gerne eingesehen werden, oder Bankserver, auf denen das große Geld verteilt wird.
- In zweiter Linie sind aber auch die Netzwerke von kleineren Organisationen gefährdet, die vielleicht nur für ganz bestimmte Gruppen interessant sind. Auf den Rechnern von Steuerberatern, Rechtsanwälten oder Ärzten schlummern sicherlich auch einige Informationen, die für Dritte durchaus interessant sein können.
- Nicht zuletzt sind aber auch die Rechner und Netzwerke Opfer von Angriffen, die augenscheinlich überhaupt keinen Nutzen für die Angreifer bieten. Gerade die “Script-Kiddies”, die aus jugendlichem Ehrgeiz ihre Möglichkeiten austesten, suchen manchmal einfach nur nach einem wehrlosen Opfer, um sich für höhere Aufgaben zu üben.

  Der Angriff auf einen eigentlich gar nicht interessanten, ungeschützten Rechner einer Privatperson kann auch dem Zweck dienen, eine Ausgangsbasis für Attacken auf die eigentlichen Ziele im zweiten Schritt vorzubereiten. Der “uninteressante” Rechner wird damit zur Quelle des Angriffs im zweiten Schritt, der Angreifer kann seine Identität verschleiern.

Unter dem Strich kann man also festhalten, dass die statistische Wahrscheinlichkeit für einen Angriff auf das Netzwerk der Global Player in der Industrie zwar größer ist als auf das Kleinst-Netzwerk im Home-Office. Aber auf der anderen Seite ist es bei einem schutzlos im Internet aufgestellten Rechner wahrscheinlich nur eine Frage der Zeit, bis er evtl. sogar zufällig einmal das Opfer von Angriffen wird.

8.2 Was ist eine Firewall?

Der Begriff der “Firewall” wird sehr unterschiedlich interpretiert. Wir möchten an dieser Stelle erläutern, was im Rahmen dieses Referenz-Handbuchs mit der “Firewall” gemeint ist:

Eine Firewall ist eine Zusammenstellung von Komponenten, die an einer zentralen Stelle den Datenaustausch zwischen zwei Netzwerken überwacht. Meistens überwacht die Firewall dabei den Datenaustausch zwischen einem

internen, lokalen Netzwerk (LAN) und einem externen Netzwerk wie dem Internet.

Die Firewall kann dabei aus Hard- und/oder Softwarekomponenten bestehen:

- In reinen Hardware-Systemen läuft oft die Firewall-Software auf einem proprietären Betriebssystem.
- Die Firewall-Software kann aber auch auf einem normalen Rechner mit Linux, Unix oder Windows laufen, der für diese Aufgabe abgestellt wurde.
- Als dritte und häufig anzutreffende Alternative läuft die Firewall-Software direkt in dem Router, der das LAN mit dem Internet verbindet.

Wir betrachten in den folgenden Abschnitten nur die Firewall in einem Router.

Hinweis: Die Funktionen “Intrusion Detection” und “DoS-Abwehr“ gehören in manchen Anwendungen mit zum Umfang einer Firewall. In diesem Router sind diese Funktionen natürlich auch enthalten, aber als separate Module neben der Firewall realisiert. Weitere Informationen dazu finden Sie in den Abschnitten *Abwehr von Einbruchsversuchen: Intrusion Detection* auf Seite 764 und *Schutz vor “Denial-of-Service”-Angriffen* auf Seite 766.

8.2.1 Die Aufgaben einer Firewall

Prüfung der Datenpakete

Wie überwacht die Firewall den Datenverkehr? Im Prinzip arbeitet die Firewall wie ein Türwächter für Datenpakete: Jedes Paket wird daraufhin geprüft, ob es die Türe des Netzwerks (die Firewall) in der gewünschten Richtung passieren darf oder nicht. Für diese Prüfung werden verschiedene Kriterien verwendet, die im Sprachgebrauch der Firewalls “Regeln” oder “Richtlinien” bezeichnet werden. Nach der Art der Informationen, die für die Erstellung der Regeln verwendet und im Betrieb der Firewall geprüft werden, unterscheidet man verschiedene Typen von Firewalls.

Wichtig ist vor allem der Aspekt der “zentralen” Positionierung: nur wenn wirklich der gesamte Datenverkehr zwischen “innen” und “außen” über die Firewall läuft, kann sie ihre Aufgabe sicher erfüllen. Jeder alternative Weg kann die Sicherheit der Firewall herabsetzen oder gar ausschalten. Diese zentrale Stellung der Firewall vereinfacht nebenbei auch die Wartung: eine Firewall als gemeinsamer Übergang zwischen zwei Netzwerken ist sicherlich

einfacher zu pflegen als eine “Personal Firewall” auf jedem der im LAN angeschlossenen Rechner.

Hinweis: Prinzipiell arbeiten Firewalls an der Schnittstelle zwischen zwei oder mehreren Netzwerken. Für die folgenden Ausführungen werden wir als Beispiel nur den Übergang zwischen einem lokalen Netzwerk in einem Unternehmen und dem Internet betrachten. Diese Erklärungen lassen sich aber sinngemäß auch auf anderen Netzwerk-Konstellationen übertragen, z. B. für den Schutz eines Subnetzes der Personalabteilung in einem Unternehmen gegen die restlichen Netzwerkbenutzer.

Protokollierung und Alarmierung

Eine wichtige Funktion einer Firewall ist neben dem Prüfen der Datenpakete und der richtigen Reaktion auf die Ergebnisse dieser Prüfung auch die Protokollierung aller Aktionen, die bei der Firewall ausgelöst wurden. Durch die Auswertung dieser Protokolle kann der Admin Rückschlüsse auf die erfolgten Angriffe ziehen und auf Grund dieser Informationen ggf. die Konfiguration der Firewall weiter verbessern.

Die Protokollierung alleine kommt aber manchmal zu spät. Oft kann durch ein sofortiges Eingreifen des Admins ein größerer Schaden verhindert werden. Aus diesem Grund verfügen Firewalls meistens über eine Alarmierungsfunktion, bei der die Meldungen der Firewall z. B. per E-Mail an den Administrator gemeldet werden.

8.2.2 Unterschiedliche Typen von Firewalls

Im Laufe der letzten Jahre hat sich die Arbeitsweise von Firewalls immer weiter entwickelt. Unter dem Oberbegriff “Firewall” werden eine ganze Reihe unterschiedlicher technischer Konzepte angeboten, mit denen das LAN geschützt werden soll. Hier stellen wir die wichtigsten Typen vor.

Paketfilter

Von einer paketfilterbasierten Firewall spricht man, wenn der Router nur die Angaben im Header der Datenpakete prüft und anhand dieser Informationen

entscheidet, ob das Paket durchgelassen werden soll oder nicht. Zu den geprüften Informationen der Datenpakete gehören:

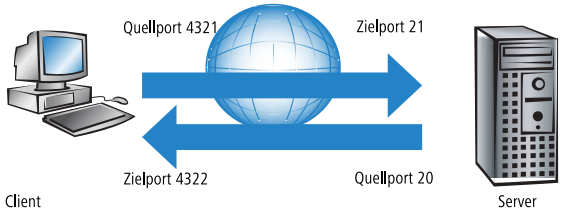
- IP-Adresse von Quelle und Ziel
- Übertragungsprotokoll (TCP, UDP oder ICMP)
- Portnummern von Quelle und Ziel
- MAC-Adresse

Die in einer paketfilterorientierten Firewall definierten Regeln legen z. B. fest, ob die Pakete von einem bestimmten IP-Adresskreis in das lokale Netzwerk weitergeleitet werden dürfen oder ob Pakete für bestimmte Dienste (d.h. mit speziellen Portnummern) gefiltert werden sollen. Durch diese Maßnahmen kann die Kommunkation mit bestimmten Rechnern, ganzen Netzwerken oder über bestimmte Dienste eingeschränkt oder verhindert werden. Die Regeln können dabei auch kombiniert werden, so kann z. B. der Zugang zum Internet über den TCP-Port 80 nur Rechnern mit bestimmten IP-Adressen erlaubt werden, während dieser Dienst für alle anderen Rechner gesperrt ist.

Die Konfiguration von paketfilternden Firewalls ist recht einfach, die Liste mit den zugelassenen oder verbotenen Paketen kann sehr schnell erweitert werden. Da auch die Anforderungen an die Performance eines Paketfilters mit recht geringen Mitteln erreicht werden kann, sind Paketfilter in der Regel direkt in Routern implementiert, die ohnehin als Schnittstelle zwischen den Netzwerken eingesetzt werden.

Nachteilig für die Paketfilter wirkt sich aus, dass die Liste der Regeln nach einiger Zeit nicht mehr so einfach zu überschauen ist. Außerdem werden bei einigen Diensten die Ports für die Verbindung dynamisch ausgehandelt. Um diese Kommunikation zu ermöglichen, muss der Administrator also alle dazu möglicherweise verwendeten Ports offen lassen, was der Grundausrichtung in den meisten Sicherheitskonzepten entgegenspricht.

Ein Beispiel für einen Vorgang, der für einfache Paketfilter recht problematisch ist, ist der Aufbau einer FTP-Verbindung von einem Rechner im eigenen LAN zu einem FTP-Server im Internet. Beim üblicherweise verwendeten aktiven FTP sendet der Client (aus dem geschützten LAN) eine Anfrage von einem Port im oberen Bereich (>1023) an den Port 21 des Servers. Dabei teilt der Client dem Server mit, auf welchem Port er die Verbindung erwartet. Der Server baut daraufhin von seinem Port 20 eine Verbindung zum gewünschten Port des Clients auf.



Um diesen Vorgang zu ermöglichen, muss der Administrator des Paketfilters alle Ports für eingehende Verbindungen öffnen, da er nicht vorher weiß, zu welchen Ports der Client die FTP-Verbindung anfordert. Eine Alternative ist über das passive FTP gegeben. Dabei baut der Client selbst die Verbindung zum Server auf über einen Port, den er vorher dem Server mitgeteilt hat. Dieses Verfahren wird jedoch nicht von allen Clients/Servern unterstützt.

Wenn man die Firewall weiterhin mit einem Pförtner vergleicht, prüft dieser Türsteher nur, ob er den Boten mit dem Paket an der Tür kennt oder nicht. Wenn der Kurier bekannt ist und schon einmal in das Gebäude hinein durfte, darf er auch bei allen folgenden Aufträgen ungehindert und unkontrolliert in das Gebäude bis zum Arbeitsplatz des Empfängers.

Stateful-Packet-Inspection

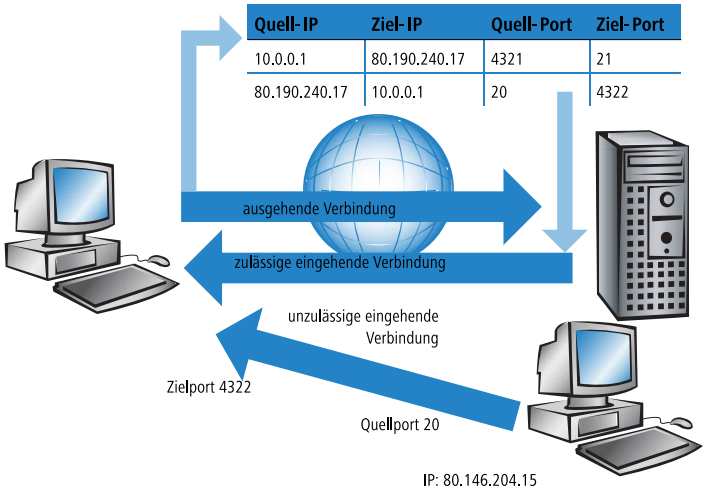
Die Stateful-Packet-Inspection (SPF) oder kurz Stateful Inspection erweitert den Ansatz der Paketfilter um eine Prüfung weiterer Verbindungsinformationen. Neben der eher statischen Tabelle mit den zugelassenen Ports und Adressbereichen wird bei dieser Variante eine dynamische Tabelle gepflegt, in die Informationen über den Zustand der einzelnen Verbindungen eingetragen werden. Diese dynamische Tabelle ermöglicht es, alle gefährdeten Ports zunächst zu sperren und nur bei Bedarf für eine zulässige Verbindung (festgelegt durch Quell- und Zieladresse) einen Port zu öffnen. Das Öffnen der Ports geschieht dabei immer nur vom geschützten Netzwerk zum ungeschützen hin, also meistens vom LAN zum WAN (Internet). Datenpakete, die nicht zu einer in der Zustandstabelle gespeicherten Verbindung gehören, werden automatisch verworfen.

Hinweis: Die Filter-Regeln einer Stateful-Inspection Firewall sind - anders als bei klassischen Portfilter-Firewalls - richtungsabhängig: Eine Verbindung kann immer von nur der Quelle zum Ziel aufgebaut werden; es sei denn, für

die Rückrichtung ist ein expliziter Eintrag vorhanden. Ist eine Verbindung aufgebaut, so werden nur die zu dieser Verbindung gehörenden Datenpakete - in beide Richtungen natürlich - übertragen. Damit lassen sich z. B. alle Zugriffe, die unaufgefordert und nicht aus dem lokalen Netz heraus erfolgen, zuverlässig abblocken.

Zusätzlich kann die Stateful Inspection aus dem Verbindungsaufbau ableiten, ob dabei zusätzliche Kanäle für den Datenaustausch ausgehandelt werden. Einige Protokolle wie z. B. FTP (für den Datentransfer), T.120, H.225, H.245 und H.323 (für Netmeeting oder IP-Telefonie), PPTP (für VPN-Tunnel) oder IRC (für den Chat) signalisieren beim Aufbau der Verbindung vom LAN zum Internet durch den verwendeten Quell-Port, dass sie weitere Ports mit der Gegenstelle vereinbaren. Die Stateful Inspection trägt dann auch diese zusätzlichen Ports in der Verbindungsliste mit ein, natürlich auch hier wieder beschränkt auf die jeweiligen Quell- und Ziel-Adressen.

Sehen wir uns dazu noch einmal das Beispiel FTP-Download an. Bei Starten der FTP-Sitzung baut der Client vom Quell-Port '4321' eine Verbindung zum Ziel-Port '21' beim Server auf. Die Stateful Inspection erlaubt diesen ersten Aufbau, sofern das FTP-Protokoll von den lokalen Rechnern nach außen freigegeben ist. In die dynamische Tabelle trägt die Firewall Quell- und Zieladresse sowie die jeweiligen Ports ein. Gleichzeitig kann die Stateful Inspection die Steuerinformationen einsehen, die an den Port 21 des Servers gesendet werden. Aus diesen Steuersignalen geht hervor, dass der Client damit eine Verbindung des Servers von dessen Port 20 auf den Port 4322 des Clients anfordert. Die Firewall trägt auch diese Werte in die dynamische Tabelle ein, weil die Verbindung in das LAN hinein vom Client angefordert wird. Der Server kann also anschließend wie gewünscht die Daten an den Client senden.



Versucht hingegen ein anderer Rechner im Internet, den gerade offenen Port 4322 im LAN zu nutzen, um selbst Daten von seinem Port 20 auf dem geschützten Client abzulegen, wird dieser Versuch von der Firewall unterbunden, denn die IP-Adresse des Angreifers passt nicht zur erlaubten Verbindung!

Hinweis: Nach der erfolgreichen Datenübertragung verschwinden die Einträge automatisch wieder aus der dynamischen Tabelle, die Ports werden also wieder geschlossen.

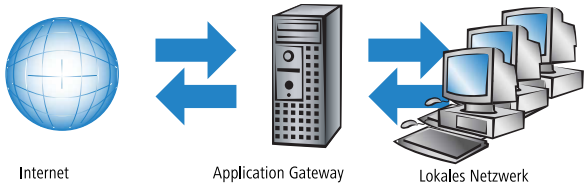
Eine Firewall mit Stateful-Inspection ist zudem meistens in der Lage, die empfangenen Datenpakete zu re-assemblieren, also einzelne Bestandteile zwischenzuspeichern und wieder zu einem gesamten Paket zusammenzubauen. Dadurch können bei fragmentierten Paketen nicht nur die einzelnen Teile von der Firewall geprüft werden, sondern auch das vollständige IP-Paket.

Dieser Pförtner macht seine Aufgabe also schon deutlich besser. Wenn in dieser Firma jemand einen Kurier bestellt, muss er parallel dazu auch den Pförtner anrufen und mitteilen, das er einen Kurier erwartet, um welche Uhrzeit der da sein wird und was auf dem Lieferschein des Paketes steht. Nur wenn diese Angaben beim Eintreffen des Kuriers mit dem Eintrag im Logbuch des Pförtners übereinstimmen, wird er den Kurier durchlassen. Bringt der Kurier nicht nur ein Paket, sondern gleich zwei, wird nur das mit dem richtigen Lie-

ferschein durchgelassen. Ebenso wird auch ein zweiter Kurier, der Durchlass zu dem Mitarbeiter verlangt, an der Pforte abgewiesen.

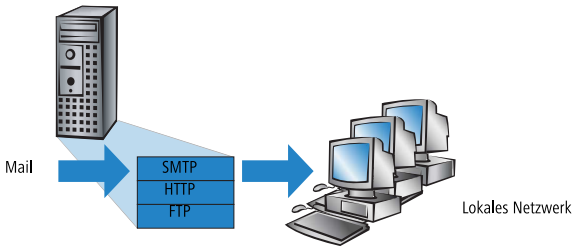
Application Gateway

Die Application Gateways erweitern die Adressprüfung der Paketfilter und die Verbindungsüberwachung der Stateful-Packet-Inspection um die Prüfung der Inhalte auf Anwendungsebene. Das Application Gateway läuft aufgrund der hohen Anforderungen an die Hardware-Performance in der Regel auf einem separaten Rechner. Dieser Rechner steht zwischen dem lokalen Netzwerk und dem Internet. Aus beiden Richtungen gesehen ist dieser Rechner die einzige Möglichkeit, mit dem jeweils anderen Netzwerk Daten auszutauschen. Es gibt keine direkte Verbindung zwischen den beiden Netzwerken, sondern immer nur bis zum Application Gateway.



Das Application Gateway steht damit als eine Art Vertreter (Proxy) für jedes der beiden Netzwerke da. Eine andere Bezeichnung für diese Konstellationen ist die des “dualhomed Gateway”, weil dieser Rechner sozusagen in zwei Netzwerken zu Hause ist.

Für jede Anwendung, die über dieses Gateway erlaubt werden soll, wird auf dem Gateway ein eigener Dienst eingerichtet, z. B. SMTP für Mail, HTTP zum Surfen im Internet oder FTP für den Datendownload.



Dieser Dienst nimmt die Daten an, die von einer der beiden Seiten empfangen werden, und bildet sie für die jeweils andere Seite wieder ab. Was auf den ersten Blick wie ein ziemlich unnötiges Spiegeln vorhandener Daten aussieht, stellt bei näherem Hinsehen aber das tiefgreifende Konzept der Application Gateways dar: Es gibt in dieser Konstellation niemals eine direkte Verbindung z. B. zwischen einem Client im lokalen Netzwerk und einem Server im Internet. Die Rechner im LAN “sehen” immer nur den Proxy, die Rechner aus dem Internet ebenfalls. Diese physikalische Trennung von LAN und WAN macht es einem Angreifer schon sehr viel schwerer, in das geschützte Netzwerk einzudringen.

In der Übersetzung in das Pförtner-Beispiel wird das Paket hier am Tor abgegeben, der Kurier darf gar nicht selbst auf das Firmengelände. Der Pförtner nimmt das Paket an, öffnet es nach Prüfung von Anschrift und Lieferschein und kontrolliert den Inhalt. Wenn das Paket alle diese Hürden erfolgreich genommen hat, bringt ein firmeninterner Bote das Paket selbst weiter zum Empfänger in der Firma. Er wird damit zum Vertreter des Kuriers auf dem Firmengelände. Umgekehrt müssen alle Mitarbeiter, die ein Paket verschicken wollen, den Pförtner anrufen, der das Paket am Arbeitsplatz abholen lässt und am Tor an einen bestellten Kurier übergibt.

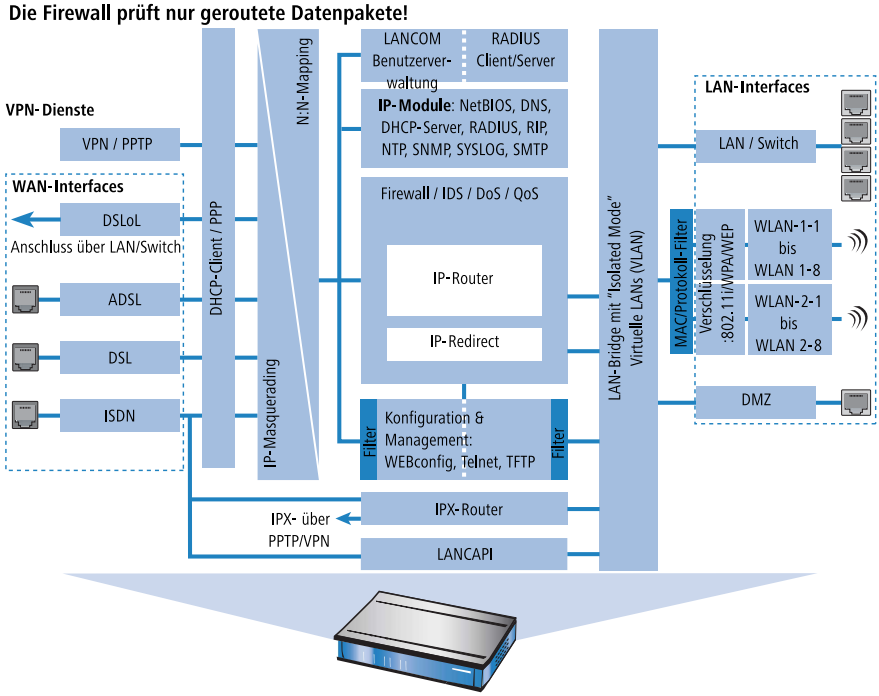
Hinweis: Die Funktion eines Application Gateways wird vom Gerät aufgrund der hohen Anforderungen an die Hardware nicht unterstützt.

8.3 Die Firewall im Gerät

Nach den allgemeinen Erläuterungen zu den Gefahren aus dem Internet sowie den Aufgaben und Typen von Firewalls finden sich in diesem Kapitel Beschreibungen zu den speziellen Funktionen der Firewall im Gerät und Hinweise auf die konkrete Konfiguration.

8.3.1 So prüft die Firewall im Gerät die Datenpakete

Die Firewall filtert aus dem gesamten Datenstrom, der über den IP-Router des Geräts läuft, diejenigen Datenpakete heraus, für die eine bestimmte Behandlung vorgesehen ist.



Die Firewall prüft nur die Datenpakete, die vom IP-Router im Gerät geroutet werden. In der Regel sind das die Datenpakete, die zwischen den internen Netzwerken (LAN, WLAN, DMZ) und der “Außenwelt” über eines der WAN-Interfaces ausgetauscht werden. Die Kommunikation z. B. zwischen LAN und WLAN untereinander wird normalerweise nicht über den Router abgewickelt, sofern die LAN-Bridge den direkten Austausch erlaubt. Hier wirken also auch nicht die Regeln der Firewall. Gleiches gilt für die so genannten “internen Dienste” wie Telnet, TFTP, SNMP und den Webserver für die Konfiguration über WEBconfig. Die Datenpakete dieser Dienste laufen nicht über den Router und werden daher auch nicht durch die Firewall beeinflusst.

Hinweis: Durch die Positionierung hinter dem Masquerading-Modul (aus Sicht des WANs) arbeitet die Firewall dabei mit den “echten” internen IP-Adressen der LAN-Stationen, nicht mit der nach außen bekannten Internetadresse des Geräts.

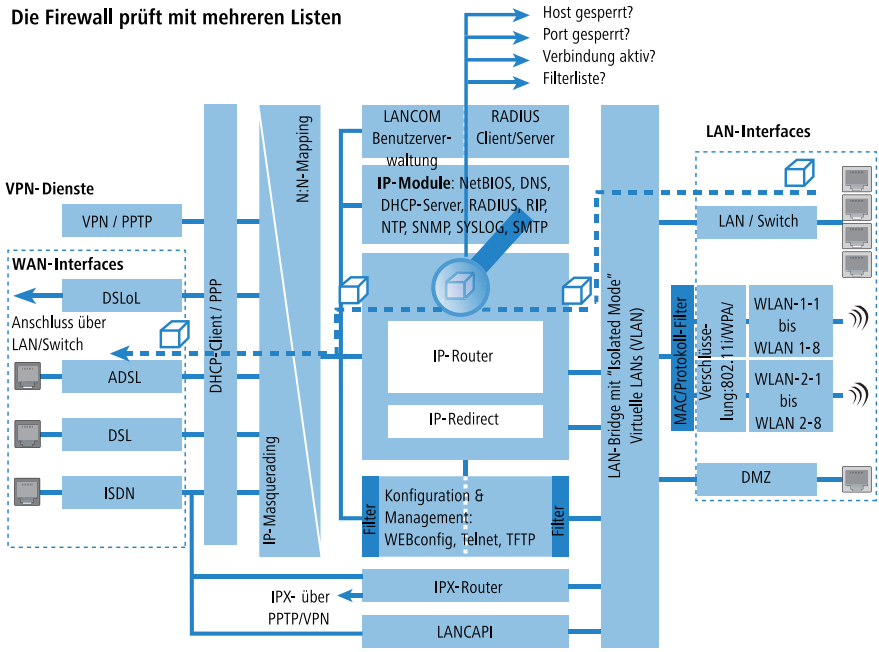
Die Firewall im Gerät verwendet für die Prüfung der Datenpakete mehrere Listen, die aus den Firewall-Regeln, den daraus ausgelösten Firewall-Aktionen oder den aktiven Datenverbindungen automatisch erzeugt werden:

- Hostsperrliste
- Portsperrliste
- Verbindungsliste
- Filterliste

Und so setzt die Firewall die Listen ein, wenn ein Datenpaket über den IP-Router geleitet werden soll:

1. Zuerst wird nachgeschaut, ob das Paket von einem Rechner kommt, der in der **Hostsperrliste** vermerkt ist. Ist der Absender gesperrt, wird das Paket verworfen.
2. Ist der Absender dort nicht gesperrt, wird in der **Portsperrliste** geprüft, ob die verwendete Port/Protokoll-Kombination auf dem Zielrechner geschlossen ist. In diesem Fall wird das Paket verworfen.
3. Sind Absender und Ziel in den beiden ersten Listen nicht gesperrt, wird geprüft, ob für dieses Paket ein Verbindungseintrag in der **Verbindungsliste** existiert. Existiert ein solcher Eintrag, dann wird mit dem Paket so verfahren, wie in der Liste vermerkt ist.
4. Wird für das Paket kein Eintrag gefunden, dann wird die **Filterliste** durchsucht, ob ein passender Eintrag vorhanden ist und die dort angege-

bene Aktion ausgeführt. Wenn die Aktion besagt, dass das Paket akzeptiert werden soll, so wird ein Eintrag in der Verbindungsliste vorgenommen und etwaige weitere Aktionen dort vermerkt.



Hinweis: Existiert für ein Datenpaket keine explizite Firewall-Regel, so wird das Paket akzeptiert (’Allow-All’). Damit ist eine Abwärtskompatibilität zu bestehenden Installationen gegeben. Für einen maximalen Schutz durch die Stateful-Inspection beachten Sie bitte den Abschnitt *Aufbau einer expliziten ”Deny-All”-Strategie* auf Seite 744.

Bleibt die Frage, woher die vier Listen ihre Informationen beziehen:

- In der Hostsperrliste werden die Stationen aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Die Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.

- In der Portsperrliste werden die Protokolle und Dienste aufgeführt, die aufgrund einer Firewall-Aktion für eine bestimmte Zeit gesperrt sind. Auch diese Liste ist dynamisch, neue Einträge können fortlaufend durch entsprechende Aktionen der Firewall hinzugefügt werden, nach Ablauf der Sperrzeit verschwinden die Einträge automatisch.
- In der Verbindungsliste wird für jede aufgebaute Verbindung ein Eintrag vorgenommen, wenn das geprüfte Paket von der Filterliste akzeptiert wird. In der Verbindungsliste wird festgehalten, von welcher Quelle zu welchem Ziel, über welches Protokoll und welchen Port eine Verbindung aktuell erlaubt ist. Darüber hinaus wird in dieser Liste festgehalten, wie lange der Eintrag noch in der Liste stehen bleibt und welche Firewall-Regel den Eintrag erzeugt hat. Diese Liste ist sehr dynamisch und permanent “in Bewegung”.
- Die Filterliste wird aus den Regeln der Firewall erzeugt. Die darin enthaltenen Filter sind statisch und ändern sich nur beim Hinzufügen, Bearbeiten oder Löschen von Firewall-Regeln.

Alle Listen, die von der Firewall zur Prüfung der Datenpakete herangezogen werden, basieren also letztendlich auf den Firewall-Regeln (*Die Parameter der Firewall-Regeln* auf Seite 728).

8.3.2 Besondere Protokolle

Ein wichtiger Punkt bei der Verbindungsüberwachung ist die Behandlung von Protokollen, die dynamisch Ports und / oder Adressen aushandeln, über die die weitere Kommunikation passiert. Beispiele für diese Protokolle sind FTP, H.323 oder auch viele UDP-basierte Protokolle. Hier ist es nötig, dass zusätzlich zu der ersten Verbindung ggf. weitere Verbindungen geöffnet werden. (siehe dazu auch *Unterschiedliche Typen von Firewalls* auf Seite 710).

UDP-Verbindungen

UDP ist eigentlich ein zustandsloses Protokoll, trotzdem kann man auch bei UDP-basierten Protokollen von einer nur kurzfristigen Verbindung sprechen, da es sich meistens um Request/Response-basierte Protokolle handelt, bei denen ein Client seinen Request an den Well-Known Port des Servers (z. B. 53 für DNS) richtet, und dieser darauf den Response wieder an den vom Client gewählten Quellport sendet:

Port Client	*Verbindung*	*Port Server*
12345	Request	53
		
12345	Response	53
		

Wenn der Server hingegen größere Datenmengen senden (z. B. TFTP) will und auf dem Well-Known Port nicht zwischen Requests und Acknowledges unterscheiden möchte oder kann, so schickt er zunächst das Response-Paket an den Quellport des Absenders. Dabei setzt er aber als eigenen Quellport einen freien Port ein, auf dem er nun mit dem Client Daten austauschen möchte:

Port Client	*Verbindung*	*Port Server*
12345	Request	69
		
12345	Response	54321
		
12345	AckData	54321
		
12345	Data/Ack	54321
		

Während sich die Datenübertragung nun über die Ports 12345 und 54321 abspielt, kann der Server auf dem Well-Known Port (69) weitere Requests annehmen. Wenn das Gerät eine “Deny-All-Strategie” verfolgt, wird durch die erste Anfrage des Clients ein Eintrag in der Verbindungsliste erzeugt, der nur die Datenpakete des Servers auf Port 69 zulässt. Die Antwort des Servers würde dabei also einfach verworfen. Um dies zu verhindern, wird beim Anlegen des Eintrags in der Verbindungsliste der Zielport der Verbindung zunächst freigehalten, und erst beim Eintreffen des ersten Antwortpakets gesetzt, wodurch beide möglichen Fälle einer UDP Verbindung abgedeckt werden.

TCP-Verbindungen

TCP-Verbindungen können nicht einfach nur durch die Prüfung der Ports nachgehalten werden. Bei einigen Protokollen wie z. B. FTP, PPTP oder H.323 sind Prüfungen der Nutzdaten nötig, um alle später ausgehandelten Verbindungen zu öffnen, und nur die wirklich zu den Verbindungen gehörenden Pakete zu akzeptieren. Dies entspricht einer vereinfachten Version dessen, was auch beim IP-Masquerading gemacht wird, nur ohne Adress- und Port-Mapping. Es reicht aus, die Verhandlung nachzuverfolgen, die entsprechenden Ports zu öffnen und mit der Hauptverbindung zu verknüpfen. Damit werden diese Ports einerseits mit dem Schließen der Hauptverbindung ebenfalls geschlossen, und andererseits hält der Datenverkehr auf den Nebenverbindungen auch die Hauptverbindung weiter offen.

ICMP-Verbindungen

Für ICMP werden zwei Fälle unterschieden: Das sind zum einen die ICMP-Request/Reply-Verbindungen, wie sie z. B. beim “ping” verwendet werden, zum anderen die ICMP-Fehlermeldungen, die als Antwort auf ein beliebiges IP-Paket empfangen werden können.

ICMP Request/Reply-Verbindungen können eindeutig durch den vom Initiator verwendeten Identifier zugeordnet werden, d.h. in der Zustandsdatenbank wird beim Senden eines ICMP-Requests ein Eintrag erstellt, der nur ICMP-Replies mit dem korrekten Identifier durchlässt. Alle anderen ICMP-Replies werden stillschweigend verworfen.

Bei ICMP-Fehlermeldungen steht der IP-Header und die ersten 8 Bytes des IP-Pakets (i.A. UDP- oder TCP-Header) innerhalb des ICMP-Pakets. Anhand dieser Information wird beim Empfang einer ICMP-Fehlermeldung der zugehörige Eintrag in der Zustandsdatenbank gesucht. Das Paket wird nur weitergeleitet, wenn ein solcher Eintrag existiert, ansonsten wird es stillschweigend verworfen. Zusätzlich dazu werden potentiell gefährliche ICMP-Fehlermeldungen (Redirect-Route) herausgefiltert.

Verbindungen sonstiger Protokolle

Bei allen anderen Protokollen können keine verwandten Verbindungen nachgehalten werden, d.h. bei ihnen kann nur eine Verbindung zwischen den

beteiligten Hosts in der Zustandsdatenbank aufgenommen werden. Diese können auch nur von einer Seite aus initiiert werden, es sei denn, in der Firewall ist ein dedizierter Eintrag für die “Gegenrichtung” vorhanden.

8.3.3 Allgemeine Einstellungen der Firewall

Neben den einzelnen Firewall-Regeln, die für die Einträge in den Filter- Verbindungs- und Sperrlisten sorgen, gelten einige Einstellungen für die Firewall allgemein:

- Firewall/QoS-Aktivierung
- Administrator-E-Mail *Administrator-E-Mail* auf Seite 723
- Fragmente *Fragmente* auf Seite 723
- Sitzungswiederherstellung *Sitzungswiederherstellung* auf Seite 724
- Ping-Block *Ping-Blocking* auf Seite 725
- Stealth-Modus *TCP-Stealth-Modus* auf Seite 726
- Authentifizierungs-Port tarnen *Authentifizierungs-Port tarnen* auf Seite 727

Firewall/QoS-Aktivierung

Mit dieser Option wird die gesamte Firewall inklusive der Quality-of-Service-Funktionen ein- bzw. ausgeschaltet.

Hinweis: Bitte beachten Sie, dass die Funktionen des N:N-Mapping nur wirksam sind, wenn die Firewall eingeschaltet ist!

Administrator-E-Mail

Zu den Aktionen, die die Firewall auslösen können, gehört auch die Alarmierung des Administrators per E-Mail. Die “Administrator-E-Mail” ist die Mail-Adresse, an die die entsprechenden Alarmierungs-Mails verschickt werden.

Fragmente

Manche Angriffe aus dem Internet versuchen, die Firewall durch fragmentierte Pakete (also in mehrere kleine Einheiten aufgeteilte Pakete) zu überlisten. Zu den Haupteigenschaften einer Stateful Inspection gehört auch die Fähigkeit,

fragmentierte Pakete zu Re-assemblieren (wieder zusammenzusetzen), um anschließend das gesamte IP-Paket prüfen zu können.

Das gewünschte Verhalten der Firewall kann zentral eingestellt werden. Dabei stehen folgende Möglichkeiten zur Auswahl:

- **Filtern**: Die fragmentierten Pakete werden von der Firewall direkt verworfen.
- **Weiterleiten**: Die fragmentierten Pakete werden ohne weitere Prüfung von der Firewall weitergeleitet, sofern die gültigen Filtereinstellungen das zulassen.
- **Re-assemblieren**: Die fragmentierten Pakete werden zwischengespeichert und wieder zu einem kompletten IP-Paket zusammengesetzt. Das re-assemblierte Paket wird dann nach den gültigen Filtereinstellungen geprüft und entsprechend behandelt.

Sitzungswiederherstellung

Die Firewall trägt in der Verbindungsliste alle aktuell erlaubten Verbindungen ein. Die Einträge verschwinden nach einer bestimmten Zeit (Timeout) automatisch wieder aus der Verbindungsliste, wenn keine Daten über die Verbindung übertragen werden und den Timeout erneuern.

Manchmal werden die Verbindungen gemäß den allgemeinen Aging-Einstellungen beendet, bevor die mit einer Anfrage angeforderten Datenpakete von der Gegenstelle empfangen wurden. In diesem Fall steht möglicherweise in der Verbindungsliste noch ein Eintrag für eine zulässige Verbindung, die Verbindung selbst ist aber nicht mehr vorhanden.

Der Parameter “Sitzungswiederherstellung” bestimmt das Verhalten der Firewall für Pakete, die auf eine ehemalige Verbindung schließen lassen:

- **Verbieten**: Die Firewall stellt die Sitzung auf keinen Fall wieder her und verwirft das Paket.
- **Verbieten für Default-Route**: Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über die Default-Route empfangen wurde.
- **Verbieten für WAN-Interfaces**: Die Firewall stellt die Sitzung nur wieder her, wenn das Paket nicht über eines der WAN-Interfaces empfangen wurde.
- **Erlauben**: Die Firewall stellt die Verbindung grundsätzlich wieder her, wenn das Paket zu einer “ehemaligen” Verbindung aus der Verbindungsliste gehört.

Hinweis: Da die Funktion der virtuellen Router auf der Auswertung der Schnittstellen-Tags basiert, müssen neben den ungetaggten Default-Routen auch weitere Routen als „Default-Routen“ einbezogen werden:

- Wenn ein Paket auf einem **WAN-Interface** empfangen wird, dann gilt diese WAN-Schnittstelle für die Firewall als Defaultroute, wenn entweder eine getaggte oder eine ungetaggte Defaultroute auf diese WAN-Schnittstelle verweist.
- Wenn ein Paket auf einem **LAN-Interface** empfangen wird und auf eine WAN-Schnittstelle geroutet werden soll, dann gilt diese WAN-Schnittstelle als Defaultroute, wenn entweder die ungetaggte Defaultroute oder eine mit dem Interface-Tag getaggte Defaultroute auf diese WAN-Schnittstelle verweist.

Ebenso greifen Defaultrouten-Filter auch, wenn sich die Defaultroute im LAN befindet. Hierbei gilt, dass der Filter dann greift, wenn

- ein Paket über ein getaggtes LAN-Interface empfangen wurde und über eine mit dem Interface getaggte Default-Route gesendet werden soll, oder
- ein Paket von einem weiteren Router in einem getaggten LAN-Interface empfangen wurde und eine mit dem Interface-Tag versehene Default-Route zur Quelladresse des Pakets existiert, oder
- ein Paket vom WAN empfangen wurde und auf eine beliebig getaggte Default-Route im LAN gesendet werden soll

Ping-Blocking

Eine - nicht unumstrittene - Methode die Sicherheit zu erhöhen, ist das Verstecken des Routers; frei nach der Methode: “Wer mich nicht sieht, wird auch nicht versuchen mich anzugreifen...”. Viele Angriffe beginnen mit der Suche nach Rechnern und/oder offenen Ports über eigentlich recht harmlose Anfragen, z. B. mit Hilfe des “ping”-Befehls oder mit einem Portscan. Jede Antwort auf diese Anfragen, auch die “Ich bin nicht hier”-Antwort, zeigt dem Angreifer, dass er ein potenzielles Ziel gefunden hat. Denn wer antwortet, der ist auch da. Um diese Rückschlüsse zu verhindern, kann das Gerät die Antworten auf diese Anfragen unterdrücken.

Um dies zu erreichen, kann das Gerät angewiesen werden, ICMP-Echo-Requests nicht mehr zu beantworten. Gleichzeitig werden auch die bei einem “traceroute” benutzten TTL-Exceeded Meldungen unterdrückt, so dass das Gerät weder durch ein “ping” noch ein “traceroute” gefunden werden kann.

Mögliche Einstellungen sind:

- **Aus**: ICMP-Antworten werden nicht blockiert
- **Immer**: ICMP-Antworten werden immer blockiert
- **WAN**: ICMP-Antworten werden auf allen WAN-Verbindungen blockiert
- **Default Route**: ICMP-Antworten werden auf der Default-Route (i.d.R. Internet) blockiert

Hinweis: Für die Auswahl der “Default-Routen” gelten hier die gleichen Hinweise wie bei *Sitzungswiederherstellung* auf Seite 724.

TCP-Stealth-Modus

Neben ICMP-Meldungen verrät auch das Verhalten bei TCP- und UDP-Verbindungen, ob sich an der angesprochenen Adresse ein Rechner befindet. Je nach umgebendem Netzwerk kann es sinnvoll sein, wenn TCP- und UDP-Pakete einfach verworfen werden, anstatt mit einem TCP-Reset bzw. einer ICMP-Meldung (port unreachable) zu antworten, wenn kein Listener für den jeweiligen Port existiert. Das jeweils gewünschte Verhalten kann im Gerät eingestellt werden.

Hinweis: Werden Ports ohne Listener versteckt, so ergibt sich auf maskierten Verbindungen das Problem, dass der “authenticate”- bzw. “ident”-Dienst nicht mehr funktioniert (bzw. nicht mehr korrekt abgelehnt wird). Der entsprechende Port kann daher gesondert behandelt werden (*Authentifizierungs-Port tarnen* auf Seite 727).

Mögliche Einstellungen sind:

- **aus**: Alle Ports sind geschlossen und TCP-Pakete werden mit einem TCP-Reset beantwortet
- **immer**: Alle Ports sind versteckt und TCP-Pakete werden stillschweigend verworfen.

- **WAN**: Auf der WAN-Seite sind alle Ports versteckt und auf der LAN-Seite geschlossen
- **Default-Route**: Die Ports sind auf der Default-Route (i.d.R. Internet) versteckt und auf allen anderen Routen geschlossen

Hinweis: Für die Auswahl der “Default-Routen” gelten hier die gleichen Hinweise wie bei *Sitzungswiederherstellung* auf Seite 724.

Authentifizierungs-Port tarnen

Wenn TCP- oder UDP-Ports versteckt werden, können z. B. die Anfragen von Mailservern zur Authentifizierung der Benutzer nicht mehr richtig beantwortet werden. Die Anfragen der Server laufen dann in einen Timeout, die Zustellung der Mails verzögern sich erheblich.

Auch bei aktiviertem TCP-Stealth-Modus erkennt die Firewall die Absicht einer Station im LAN, eine Verbindung zu einem Mailserver aufzubauen. Daraufhin wird der benötigte Port für die Authentifizierungsanfrage kurzzeitig (für 20 Sekunden) geöffnet.

Dieses Verhalten der Firewall im TCP-Stealth-Modus kann mit dem Parameter “Authentifizierungs-Port tarnen“ gezielt unterdrückt werden.

Hinweis: Das Aktivieren der Option “Authentifizierungs-Port tarnen“ kann zu erheblichen Verzögerungen beim Versand und Empfang z. B. von E-Mails oder News führen!

Ein Mail- oder News-Server, der mit Hilfe dieses Dienstes etwaige zusätzliche Informationen vom User anfordert, läuft dann zunächst in einen störenden Timeout, bevor er beginnt, die Mails auszuliefern. Dieser Dienst benötigt also einen eigenen Schalter um ihn zu verstecken bzw. “konform” zu halten.

Die Problematik dabei ist nun allerdings, dass eine Einstellung, die alle Ports versteckt, den ident-Port aber zurückweist, unsinnig ist - denn allein dadurch, dass der Ident-Port zurückgewiesen wird, wäre das Gerät zu sehen.

Das Gerät bietet zur Lösung dieses Problems an, Ident-Anfragen nur von den Mail und News-Servern abzulehnen, und bei Anfragen von allen anderen Rechnern diese einfach zu verwerfen. Hierzu werden bei der Abfrage eines

Mail- (SMTP, POP3, IMAP2) oder Newsservers (NNTP) für eine kurze Zeit (20 Sekunden) ident-Anfragen von den jeweiligen Servern abgelehnt.

Ist die Zeit abgelaufen, so wird der Port wieder versteckt.

8.3.4 Die Parameter der Firewall-Regeln

In diesem Abschnitt stellen wir vor, aus welchen Komponenten eine Firewall-Regel besteht und welche Optionen zur Einstellung der verschiedenen Parameter zur Verfügung stehen.

Die Komponenten einer Firewall-Regel

Eine Firewall-Regel wird zunächst bestimmt durch ihren Namen und einige weitere Optionen:

- **Ein-/Ausschalter**: Ist die Regel aktiv?
- VPN-Regel: Wird die Firewall-Regel auch zur Erzeugung von VPN-Regeln verwendet? *VPN-Regeln* auf Seite 730
- Verknüpfung: Sollen weitere Firewall-Regeln beachtet werden, wenn diese Regel für ein Datenpaket zutrifft? *Verknüpfung* auf Seite 729
- **Priorität**: Mit welcher Priorität wird die Regel bearbeitet? *Priorität* auf Seite 729
- **Quell-Tag**: Über ein Quell-Tag ergänzen Sie das Routing-Tag um die Angabe, auf welches Quell-Netzwerk das Gerät die Firewall-Regel anwendet. Geben Sie ein Quell-Tag an, um eine eindeutige Beziehung zwischen Quell- und Ziel-Hosts in ARF-Kontexten festzulegen: Das Gerät leitet nur dann Datenpakete an ein ARF-Netzwerk weiter, wenn diese von Hosts aus einem ARF-Netzwerk mit dem angegeben Quell-Tag stammen.
- **Routing-Tag**: Mit dem Einsatz des Routing-Tags können über die Ziel-IP-Adressen weitere Informationen wie z. B. der verwendete Dienst oder das verwendete Protokoll für die Auswahl der Zielroute genutzt werden. Durch das so realisierte Policy-based Routing ist eine deutlich feinere Steuerung des Routing-Verhaltens möglich.

  Hinweis: Das Routing-Tag 0 bedeutet hier 'nicht markieren'. Wenn das Gerät Datenpakete in ein mit 0 getaggtes Netz leiten soll, tragen Sie hier bitte 65535 ein.

Priorität

Das Gerät nimmt beim Aufbau der Filterliste aus den Firewall-Regeln eine automatische Sortierung der Einträge vor. Dabei wird der “Detallierungsgrad” berücksichtigt: Zunächst werden alle speziellen Regeln beachtet, danach die allgemeinen (z. B. Deny-All).

Wenn sich durch die automatische Sortierung nicht das gewünschte Verhalten der Firewall einstellt, kann die Priorität von Hand verändert werden. Je höher die Priorität der Firewall-Regel, desto eher wird der zugehörige Filter in der Filterliste platziert.

Hinweis: Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im Abschnitt *Firewall-Diagnose* auf Seite 756 beschrieben.

Verknüpfung

Es gibt Anforderungen an die Firewall, die mit einer einzelnen Regel nicht abgedeckt werden können. Wenn die Firewall dazu eingesetzt wird, den Internet-Traffic verschiedener Abteilungen (in eigenen IP-Subnetzen) zu begrenzen, können einzelne Regeln z. B. nicht gleichzeitig die gemeinsame Obergrenze abbilden. Soll jeder von z. B. drei Abteilungen eine Bandbreite von maximal 512 kBit/s zugestanden werden, die gesamte Datenrate der drei Abteilungen aber ein Limit von 1024 kBit/s nicht überschreiten, so muss eine mehrstufige Prüfung der Datenpakete eingerichtet werden:

- In der ersten Stufe wird geprüft, ob die aktuelle Datenrate der einzelnen Abteilung die Grenze von 512 kBit/s nicht übersteigt.
- In der zweiten Stufe wird geprüft, on die Datenrate aller Abteilungen zusammen die Grenze von 1024 kBit/s nicht übersteigt.

Normalerweise wird die Liste der Firewall-Regeln der Reihe nach auf ein empfangenes Datenpaket angewendet. Trifft eine Regel zu, wird die entsprechende Aktion ausgeführt. Die Prüfung durch die Firewall ist damit beendet, es werden keine weiteren Regeln auf das Paket angewendet.

Um eine zwei- oder mehrstufige Prüfung eines Datenpaketes zu erreichen, wird die “Verknüpfungsoption” für die Regeln aktiviert. Wenn eine Firewall-Regel mit aktivierter Verknüpfungsoption auf ein Datenpaket zutrifft, wird

zunächst die entsprechende Aktion ausgeführt, anschließend wird die Prüfung in der Firewall jedoch fortgesetzt. Trifft eine der weiteren Regeln auch auf dieses Paket zu, wird auch die in dieser Regel definierte Aktion ausgeführt. Ist auch bei dieser folgenden Regel die Verknüpfungsoption aktiviert, wird die Prüfung solange fortgesetzt, bis

- entweder eine Regel auf das Paket zutrifft, bei der die Verknüpfung nicht aktiviert ist
- oder die Liste der Firewall-Regeln ganz durchgearbeitet ist, ohne das eine weitere Regel auf das Paket zutrifft.

Zur Realisierung dieses Szenarios wird also für jedes Subnetz eine Firewall-Regel eingerichtet, die ab einer Datenrate von 512 kBit/s zusätzliche Pakete der Protokolle FTP und HTTP verwirft. Für diese Regeln wird die Verknüpfungsoption aktiviert. In einer weiteren Regel für alle Stationen im LAN werden alle Pakete verworfen, die über 1024 kBit/s hinausgehen.

VPN-Regeln

Eine VPN-Regel bezieht die Informationen über Quell- und Ziel-Netz u.a. aus den Firewall-Regeln.

Mit dem Aktivieren der Option “VPN-Regel” für eine Firewall-Regel wird festgelegt, dass aus dieser Firewall-Regel eine VPN-Regel abgeleitet wird.

Bei der Verwendung von mehreren lokalen Netzwerken, siehe auch ARF, muss die automatische Erzeugung der VPN-Regeln für jedes Netzwerk gezielt eingestellt werden. Zur Definition der Netzwerke mit automatischer VPN-Regel-Erzeugung wird das Schnittstellen-Tag verwendet, das für jedes Netzwerk angegeben ist. Über dieses Tag ist eine Zuordnung von lokalem Netz zur VPN-Route möglich: Jedes auf einem lokalen Interface empfangene Paket wird mit dem Schnittstellen-Tag markiert und auf eine Route mit dem selben Tag oder dem Default-Tag (0) weitergeleitet.

Für die automatische VPN-Regel-Erzeugung werden nun alle Netzwerke aufgenommen, die

- das Tag '0' haben oder
- die beiden folgenden Bedingungen erfüllen:

- Das Netzwerk hat das gleiche Schnittstellen-Tag wie der zur VPN-Verbindung gehörende Eintrag in der IP-Routing-Tabelle (nicht zu verwechseln mit dem Routing-Tag für das remote Gateway)
- Das Netzwerk ist vom Typ 'Intranet'

Hinweis: VPN-Regeln für eine DMZ müssen manuell ebenso erstellt werden wie für Netzwerke, deren Schnittstellen-Tag nicht zum Routing-Tag der VPN-Route passt.

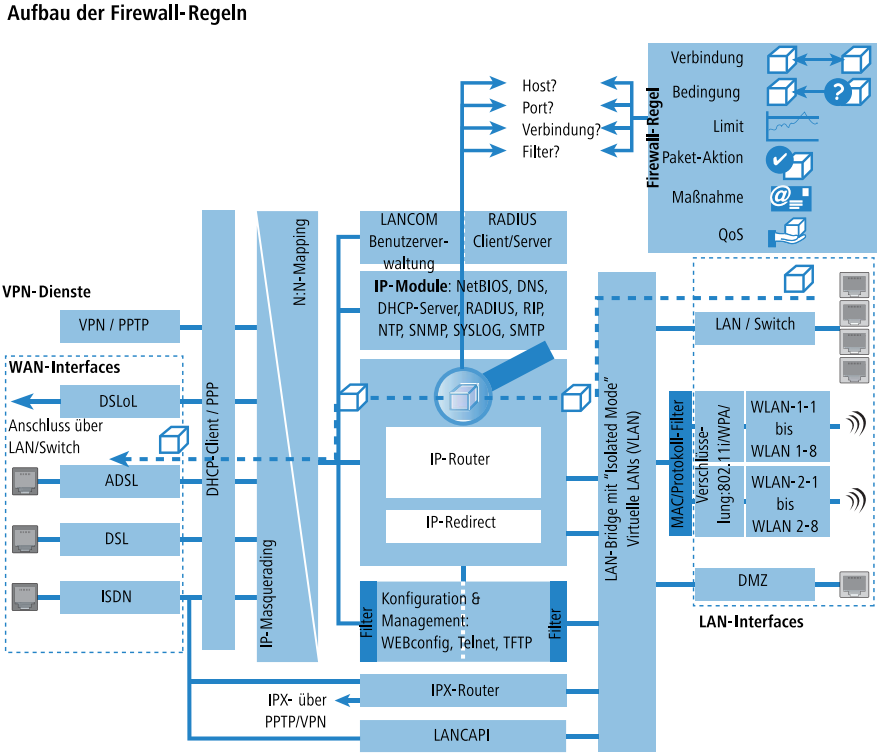
Anwendung der Firewall-Regel

Neben diesen Basisinformationen beantwortet eine Firewall-Regel die Fragen, wann bzw. worauf sie angewendet werden soll und welche Aktionen ggf. ausgeführt werden:

- Verbindung: Auf welche Stationen/Netzwerke und Dienste/Protokolle bezieht sich die Regel? *Verbindung* auf Seite 732
- Bedingung: Ist die Wirksamkeit der Regel durch Bedingungen eingeschränkt? *Bedingung* auf Seite 733
- Limit (Trigger): Beim Erreichen welcher Schwellwerte soll die Regel anspringen? *Limit (Trigger)* auf Seite 734
- Paket-Aktion: Was soll mit den Datenpaketen passieren, wenn die Bedingung erfüllt und das Limit erreicht sind? *Paket-Aktion* auf Seite 734
- Sonstige Maßnahmen: Sollen neben der Paket-Aktion noch weitere Maßnamen eingeleitet werden? *Sonstige Maßnahmen* auf Seite 735
- Quality of Service (QoS): Werden Datenpakete bestimmter Anwendungen oder mit entsprechenden Markierungen durch die Zusicherung von speziellen Dienstgütern besonders bevorzugt? *Quality of Service (QoS)* auf Seite 735

Hinweis: Bedingung, Limit, Paket-Aktion und sonstige Maßnahmen bilden zusammen ein so genanntes “Aktionen-Set”. Jede Firewall-Regel kann mehrere Aktionen-Sets beinhalten. Wenn für mehrere Aktionen-Sets das gleiche Limit verwendet wird, kann die Reihenfolge der Aktionen-Sets eingestellt werden.

Im Abschnitt *So prüft die Firewall im Gerät die Datenpakete* auf Seite 717 wurde bereits dargestellt, dass die Listen zur Prüfung der Datenpakete letztlich aus den Firewall-Regeln gebildet werden. Die Erweiterung der Grafik stellt sich damit wie folgt dar:



Verbindung

Mit der Verbindung in der Firewall-Regel legen Sie fest, auf welche Datenpakete sich die Vorschrift bezieht. Eine Verbindung wird definiert durch die Quelle, das Ziel und den verwendeten Dienst. Zur Bezeichnung von Quelle oder Ziel können die folgenden Angaben verwendet werden:

- Alle Stationen

- Das gesamte lokale Netz (LAN)
- Bestimmte Gegenstellen (bezeichnet durch den Namen aus der Gegenstellenliste)
- Bestimmte Stationen im LAN (bezeichnet durch den Hostnamen)
- Bestimmte MAC-Adressen

  Hinweis: MAC steht für Media Access Control und ist Dreh- und Angelpunkt für die Kommunikation innerhalb eines LAN. In jedem Netzwerkadapter ist eine MAC-Adresse fest eingespeichert. MAC-Adressen sind weltweit eindeutig und unverwechselbar, ähnlich zu Seriennummern von Geräten. Über die MAC-Adressen lassen sich die PCs im LAN zuverlässig auswählen, um ihnen gezielt Rechte auf IP-Paketebene zu gewähren oder zu versagen. MAC-Adressen werden häufig außen auf den Netzwerkgeräten in hexadezimaler Darstellung (z. B. 00:A0:57:01:02:03) angebracht.

- Bereiche von IP-Adressen
- Komplette IP-Netzwerke

Hostnamen können nur dann verwendet werden, wenn das Gerät die Namen in IP-Adressen auflösen kann. Dafür muss das Gerät die Namen über DHCP oder NetBIOS gelernt haben, oder die Zuordnung muss statisch in der DNS- oder IP-Routing-Tabelle eingetragen sein. Ein Eintrag in der IP-Routing-Tabelle kann dabei einem Hostnamen ein ganzes Netz zuordnen.

Hinweis: Werden die Quelle oder Ziel für eine Firewall-Regel nicht näher bestimmt, gilt die Regel generell für Datenpakete “von allen Stationen” bzw. “an alle Stationen”.

Der Dienst wird bestimmt durch die Kombination eines IP-Protokolls mit entsprechenden Quell- und/oder Zielports. Für häufig verwendete Dienste (WWW, Mail etc.) sind die entsprechenden Verknüpfungen im Gerät schon vordefiniert, andere können je nach Bedarf zusätzlich angelegt werden.

Bedingung

Mit den zusätzlichen Bedingungen schränkt man die Wirksamkeit einer Firewall-Regel weiter ein. Folgende Bedingungen stehen zur Auswahl:

- Nur für Pakete mit bestimmten ToS- bzw. DiffServ-Markierungen

- Nur wenn Verbindung noch nicht besteht
- Nur für Defaultroute (Internet)
- Nur für VPN-Routen

Limit (Trigger)

Das Limit (oder auch Trigger) bezeichnet einen quantifizierten Schwellwert, der auf der definierten Verbindung überschritten werden muss, bevor der Filter ein Datenpaket erfasst. Ein Limit setzt sich zusammen aus folgenden Eckwerten:

- Einheit (kBit, kByte oder Pakete)
- Betrag, also Datenrate oder Anzahl
- Bezugsgröße (pro Sekunde, pro Minute, pro Stunde oder absolut)

Zusätzlich kann für das Limit vereinbart werden, ob es sich auf eine logische Verbindung bezieht oder auf alle Verbindungen gemeinsam, die zwischen den festgelegten Ziel- und Quell-Stationen über die zugehörigen Dienste bestehen. So wird gesteuert, ob der Filter greift, wenn z. B. alle HTTP-Verbindungen der User im LAN in Summe das Limit überschreiten oder ob es ausreicht, wenn eine einzige der parallel aufgebauten HTTP-Verbindungen den Schwellwert durchbricht.

Bei absoluten Werten kann außerdem definiert werden, dass der zugehörige Zähler beim Überschreiten des Limits zurückgesetzt wird.

Hinweis: Die Daten werden bis zum Erreichen des Limits auf jeden Fall übertragen! Mit einem Betrag von “0” wird die Regel sofort aktiv, wenn auf der definierten Verbindung Datenpakete zur Übertragung anstehen.

Paket-Aktion

Die Firewall hat drei Möglichkeiten, ein gefiltertes Paket zu behandeln:

- **Übertragen**: Das Paket wird normal übertragen.
- **Verwerfen**: Das Paket wird stillschweigend verworfen.
- **Zurückweisen**: Das Paket wird zurückgewiesen, der Empfänger erhält eine entsprechenden Nachricht über ICMP.

Sonstige Maßnahmen

Die Firewall dient nicht nur dazu, die gefilterten Datenpakete zu verwerfen oder durchzulassen, sie kann auch zusätzliche Maßnahmen ergreifen, wenn ein Datenpaket durch den Filter erfasst wurde. Die Maßnahmen gliedern sich dabei in die beiden Bereiche “Protokollierung/Benachrichtigung” und “Verhindern weiterer Angriffe”:

- Syslog-Nachricht senden: Sendet eine Nachricht über das SYSLOG-Modul an einen SYSLOG-Client, wie im Konfigurationsbereich “Meldungen” festgelegt.
- E-Mail-Nachricht senden: Sendet eine E-Mail-Nachricht an den Administrator, der im Konfigurationsbereich “Meldungen” festgelegt ist.
- SNMP senden: Sendet einen SNMP-Trap, der z. B. vom LANmonitor ausgewertet wird.

  Hinweis: Jede dieser drei Benachrichtigungsmaßnahmen führt automatisch zu einem Eintrag in der Firewall-Ereignisstabelle.

- Verbindung trennen: Trennt die Verbindung, über die das gefilterte Paket empfangen wurde.

  Hinweis: Dabei wird die physikalische Verbindung getrennt (also z. B. die Internetverbindung), nicht nur die logische Verbindung zwischen den beiden beteiligten Rechnern!

- Absender-Adresse sperren: Sperrt die IP-Adresse, von der das gefilterte Paket empfangen wurde, für eine einstellbare Zeit.
- Ziel-Port sperren: Sperrt den Ziel-Port, an den das gefilterte Paket gesendet wurde, für eine einstellbare Zeit.

Quality of Service (QoS)

Neben den Beschränkungen für die Übertragung von Datenpaketen kann die Firewall auch für bestimmte Anwendungen eine “Sonderbehandlung” einräumen. Die QoS-Einstellungen nutzen dabei die Möglichkeiten der Firewall, Datenpakete gezielt Verbindungen oder Diensten zuordnen zu können.

8.3.5 Die Alarmierungsfunktionen der Firewall

In diesem Abschnitt werden die Meldungen, die von der Firewall bei sicherheitsrelevanten Ereignissen verschickt werden, im Detail beschrieben. Es stehen die folgenden Meldungstypen zur Verfügung:

- E-Mail-Benachrichtigung
- SYSLOG-Meldung
- SNMP-Trap

Benachrichtigungen können dabei jeweils getrennt entweder durch die Intrusion Detection, die Denial-of-Service Protection oder durch frei einstellbare Maßnahmen in der Firewall ausgelöst werden. Die spezifischen Parameter für die verschiedenen Benachrichtigungsarten (wie z. B. das zu benutzende E-Mail-Konto) können Sie an folgenden Stellen angeben:

LANconfig: Meldungen / SMTP-Konto bzw. Meldungen E SYSLOG

WEBconfig: HiLCOS-Menübaum / Setup / Mail bzw. HiLCOS-Menübaum / Setup / SYSLOG

Ein Beispiel:

Es sei ein Filter namens ’BLOCKHTTP’ definiert, der den Zugriff auf einen HTTP-Server (192.168.200.10) abblockt, und für den Fall, dass doch jemand auf den Server zugreifen wollte, jeden Traffic von und zu diesem Rechner unterbindet und den Administrator über SYSLOG informiert.

Benachrichtigung per SYSLOG

Wenn die Portfilter-Firewall ein entsprechendes Paket verwirft, wird über Syslog eine Meldung ausgegeben, z. B.:

```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port
 filter
```

Die Ports werden dabei nur bei portbehafteten Protokollen ausgegeben. Zusätzlich werden Rechnernamen dann ausgegeben, wenn das Gerät diese direkt (d.h. ohne weitere DNS-Anfrage) auflösen kann.

Werden für einen Filter die Syslog-Meldungen aktiviert (%s-Aktion), so wird diese Meldung ausführlicher. Dann werden Name des Filters, überschrittenes

Limit, sowie ausgeführte Aktionen zusätzlich mit ausgegeben. Für das obige Beispiel könnte die Meldung dann so aussehen:

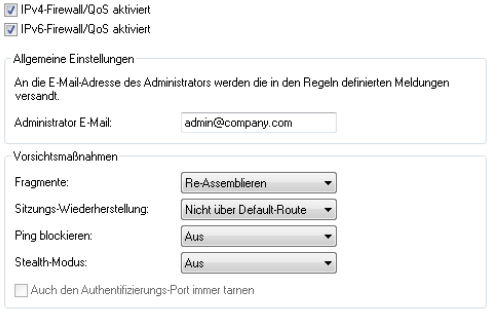
```
PACKET_ALERT: Dst: 192.168.200.10:80 {}, Src: 10.0.0.37:4353 {} (TCP): port
 filter
PACKET_INFO:
matched filter: BLOCKHTTP
exceeded limit: more than 0 packets transmitted or received on a connection
actions: drop; block source address for 1 minutes; send syslog message;
```

Benachrichtigung per E-Mail

Ist das E-Mail-System des Gerätes aktiviert, so können Sie die bequeme Benachrichtigung per E-Mail nutzen. Das Gerät sendet dann eine E-Mail in der folgenden Form an den Administrator, sobald die entsprechende Aktion der Firewall ausgeführt wurde:

```
FROM: device@company.com
TO: admin@company.com
SUBJECT: packet filtered
Date: 9/24/2002 15:06:46
The packet below
Src: 10.0.0.37:4353 {cs2} Dst: 192.168.200.10:80 {ntserver} (TCP)
45 00 00 2c ed 50 40 00 80 06 7a a3 0a 00 00 25 | E..,.P@. ..z....%
c0 a8 c8 0a 11 01 00 50 00 77 5e d4 00 00 00 00 | .......P .w^.....
60 02 20 00 74 b2 00 00 02 04 05 b4 | `. .t... ....
matched this filter rule: BLOCKHTTP
and exceeded this limit: more than 0 packets transmitted or received on a
connection
because of this the actions below were performed:
drop
block source address for 1 minutes
send syslog message
send SNMP trap
send email to administrator
```

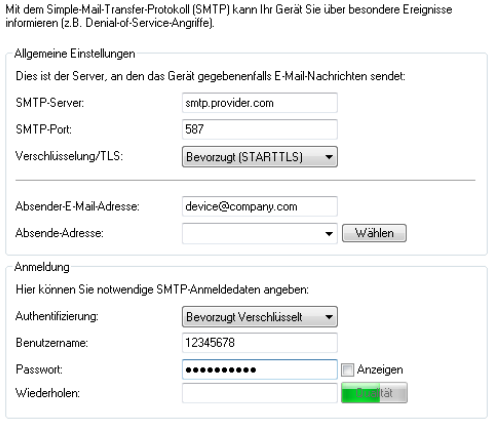
Damit der Mailversand an den Administrator funktioniert, muss die E-Mailadresse des Empfängers richtig eingetragen sein.



LANconfig: Firewall/QoS / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Firewall

Außerdem muss ein Mail-Postfach eingerichtet sein, über das die E-Mail verschickt werden kann.



LANconfig: Meldungen / SMTP-Konto

WEBconfig: HiLCOS-Menübaum / Setup / SMTP / Firewall

Benachrichtigung per SNMP-Trap

Wenn als Benachrichtigungsmethode das Versenden von SNMP-Traps aktiviert wurde, so wird die erste Zeile der Logging-Tabelle als Enterprise-Specific

Trap 26 verschickt. Dieser Trap enthält zusätzlich noch den System-Descriptor und den System-Namen aus der MIB-2.

Für das Beispiel wird ein SNMP-Trap erzeugt, aus dem man u.a. folgende Informationen ablesen kann:

```
SNMP: SNMPv1; community = public; SNMPv1 Trap; Length = 443 (0x1BB)
SNMP: Message type = SNMPv1
SNMP: Version = 1 (0x0)
SNMP: Community = public
SNMP: PDU type = SNMPv1 Trap
SNMP: Enterprise = 1.3.6.1.4.1.2356.400.1.6021
SNMP: Agent IP address = 10.0.0.43
SNMP: Generic trap = enterpriseSpecific (6)
SNMP: Specific trap = 26 (0x1A)
SNMP: Time stamp = 1442 (0x5A2)
```

- System-Descriptor:

```
SNMP: OID = 1.3.6.1.2.1.1.1.0 1.

SNMP: String Value = Hirschmann BAT-R 2.80.0001 / 23.09.2002 8699.000.036
```

- Device-String:

```
SNMP: OID = 1.3.6.1.2.1.1.5.0 2. System-Name

SNMP: String Value = Hirschmann BAT-R
```

- Time-Stamp:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.2.1 3.
SNMP: String Value = 9/23/2002 17:56:57
```

- Quell-Adresse:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.3.1 3.
SNMP: IP Address = 10.0.0.37
```

- Ziel-Adresse:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.4.1 4.
SNMP: IP Address = 192.168.200.10
```

- Protokoll (6 = TCP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.5.1 5.
SNMP: Integer Value = 6 (0x6) TCP
```

- Quell-Port:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.6.1 6.
SNMP: Integer Value = 4353 (0x1101)
```

- Ziel-Port (80 = HTTP):

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.7.1 7.
SNMP: Integer Value = 80 (0x50)
```

- Name der Filterregel:

```
SNMP: OID = 1.3.6.1.4.1.2356.400.1.6021.1.10.26.1.8.1 8.
SNMP: String Value = BLOCKHTTP
```

Hinweis: Dieser Trap und alle anderen im Gerät generierten Traps werden sowohl an alle manuell konfigurierten Trap-Empfänger gesendet, ebenso wie auch an jeden angemeldeten LANmonitor, welcher diesen und u.U. auch alle anderen Traps auswerten kann

8.3.6 Strategien für die Einstellung der Firewall

Firewalls bilden die Schnittstelle zwischen Netzwerken und schränken dort den ungehinderten Datenaustausch mehr oder weniger deutlich ein. Damit stehen die Firewalls den Zielsetzungen der Netzwerke, zu denen sie selbst gehören, entschieden entgegen: Netzwerke sollen Rechner verbinden, Firewalls sollen die Verbindung verhindern.

Aus diesem Widerspruch lässt sich das Dilemma der verantwortlichen Administratoren erkennen, die in der Folge verschiedene Strategien zur Lösung entwickelt haben.

Allow-All

Die Allow-All-Strategie stellt die ungehinderte Kommunikation der Mitarbeiter in den Netzwerken über die Sicherheit. Dabei wird zunächst jede Kommunikation erlaubt, das LAN steht für Angreifer weiter offen. Erst durch die Konfiguration des Admins wird das LAN sukzessive sicherer, in dem nach und nach neue Regeln aufgebaut werden, die Teile der Kommunikation einschränken oder verhindern.

Deny-All

Bei der Deny-All-Strategie wird zunächst nach der Methode “Alles sperren!” verfahren, die Firewall blockt die Kommunikation zwischen dem zu schützenden Netzwerk und dem Rest der Welt vollständig ab. Im zweiten Schritt öffnet der Administrator dann die Adressbereiche oder Ports, die für die tägliche Kommunikation mit dem Internet etc. erforderlich sind.

Dieser Ansatz ist für die Sicherheit des LANs besser als die Allow-All-Strategie, führt aber in der Anfangsphase oft zu Schwierigkeiten mit den Benutzern. Einige Dinge laufen eben nach Einschalten der Deny-All-Firewall vielleicht nicht mehr so wie vorher, bestimmte Rechner können ggf. nicht mehr erreicht werden etc.

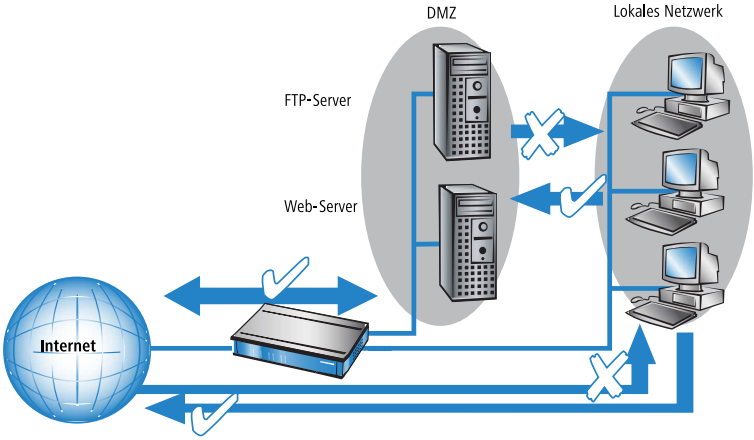
Firewall mit DMZ

Die demilitarisierte Zone (DMZ) stellt einen speziellen Bereich des lokalen Netzes dar, der durch eine Firewall sowohl gegen das Internet als auch gegen das eigentliche LAN abgeschirmt ist. In diesem Netzabschnitt werden alle Rechner positioniert, auf die aus dem unsicheren Netz (Internet) direkt zugegriffen werden soll. Dazu gehören z. B. die eigenen FTP- und Web-Server.

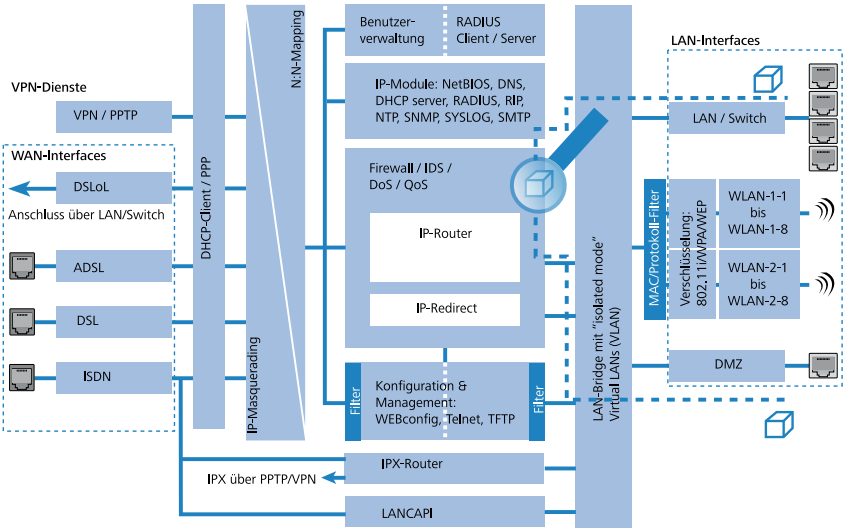
Die Firewall schützt dabei zunächst die DMZ gegen Angriffe aus dem Internet. Zusätzlich schützt die Firewall aber auch das LAN gegen die DMZ. Die Firewall wird dazu so konfiguriert, dass nur folgende Zugriffe möglich sind:

- Stationen aus dem Internet können auf die Server in der DMZ zugreifen, der Zugriff aus dem Internet auf das LAN ist jedoch nicht möglich.
- Die Stationen aus dem LAN können auf das Internet und auf die Server in der DMZ zugreifen.

- Die Server aus der DMZ können nicht auf die Stationen im LAN zugreifen. damit ist sichergestellt, dass auch ein “gehackter” Server aus der DMZ nicht zu einem Sicherheitsrisiko für das LAN wird.



Einige Router-Modelle unterstützen diesen Aufbau durch eine separate LAN-Schnittstelle, die nur für die DMZ verwendet wird. Betrachtet man den Weg der Daten durch das Gerät, dann wird die Funktion der Firewall für die Abschirmung des LANs gegenüber der DMZ deutlich.



Der direkte Datenaustausch zwischen LAN und DMZ ist über die LAN-Bridge nicht möglich, wenn ein DMZ-Port verwendet wird. Der Weg vom LAN in die DMZ und umgekehrt geht also nur über den Router, und damit auch über die Firewall! Die wiederum schirmt das LAN gegen Anfragen aus der DMZ genau so ab wie gegenüber dem Internet.

Hinweis: Das Abschirmen der DMZ gegenüber dem Internet auf der einen und dem LAN auf der anderen Seite wird in vielen Netzstrukturen mit zwei separaten Firewalls gelöst. Beim Einsatz eines Geräts mit DMZ-Port benötigt man für diesen Aufbau nur ein Gerät, was u.a. den Vorteil einer deutlich vereinfachten Konfiguration mit sich bringt.

8.3.7 Tipps zur Einstellung der Firewall

Mit der Geräte-Firewall steht ein extrem flexibles und leistungsfähiges Werkzeug zur Verfügung. Um Ihnen bei der Erstellung individuell angepasster Firewall-Regeln behilflich zu sein, finden Sie im folgenden Hinweise zur optimalen Einstellung für Ihre spezifische Anwendung.

Die Default-Einstellung der Firewall

Im Auslieferungszustand befindet sich mit der “WINS-Regel” genau ein Eintrag in der Firewall-Regeltabelle. Diese Regel verhindert unerwünschte Verbindungsaufbauten auf der Default-Route (i.d.R. zum Internet) durch das NetBIOS-Protokoll. Windows Netzwerke senden in regelmäßigen Intervallen Anfragen in das Netzwerk um herauszufinden, ob die bekannten Stationen noch verfügbar sind. Dies führt bei zeitbasierter Abrechnung einer Netzwerkkopplung zu unerwünschten Verbindungsaufbauten.

Hinweis: Das Gerät kann durch den integrierten NetBIOS-Proxy auch für Netzwerkkopplungen diese unerwünschten Verbindungsaufbauten verhindern, indem es selbst solange eine Antwort für die betreffende Ressource vortäuscht, bis ein tatsächlicher Zugriff erfolgt.

Sicherheit durch NAT und Stateful-Inspection

Sofern keine weitere Firewall-Regel eingetragen wird, wird das lokale Netz durch das Zusammenspiel von Network Address Translation und Stateful-Inspection geschützt: Nur Verbindungen aus dem lokalen Netz heraus erzeugen einen Eintrag in der NAT-Tabelle, woraufhin das Gerät einen Kommunikationsport öffnet. Die Kommunikation über diesen Port wird durch die Stateful-Inspection überwacht: Nur Pakete, die genau zu dieser Verbindung gehören, dürfen über diesen Port kommunizieren. Für Zugriff von außen auf das lokale Netzwerk ergibt sich somit eine implizite “Deny-All”-Strategie.

Wichtig: Sofern Sie in Ihrem LAN einen Server betreiben, der über Einträge in der Servicetabelle für Zugriffe aus dem Internet freigegeben ist, können Stationen aus dem Internet von außen Verbindungen zu diesem Server aufbauen. Das inverse Masquerading hat in diesem Fall Vorrang vor der Firewall, solange keine explizite “Deny-All”-Regel eingerichtet wurde.

Aufbau einer expliziten ”Deny-All”-Strategie

Für einen maximalen Schutz und bestmögliche Kontrolle über den Datenverkehr wird empfohlen, zunächst einmal jeglichen Datentransfer durch die Firewall zu unterbinden. Danach werden dann selektiv nur genau die benötigten Funktionen und Kommunikationspfade freigeschaltet. Dies bietet z. B. Schutz vor sog. ’Trojanern’ bzw. E-Mail-Viren, die aktiv eine abgehende Verbindung auf bestimmten Ports aufbauen.

Die **Deny-All**-Regel ist mit Abstand die wichtigste Regel zum Schutz des lokalen Netzwerks. Mit dieser Regel verfährt die Firewall nach dem Prinzip: “Alles, was nicht ausdrücklich erlaubt ist, bleibt verboten!” Nur mit dieser Strategie kann der Administrator sicher sein, dass er nicht irgendwo eine Zugangsmöglichkeit “vergessen” hat, denn es gibt nur die Zugänge, die er selbst geöffnet hat.

Wir empfehlen die Einrichtung der Deny-All-Regel, bevor das LAN über ein Gerät mit dem Internet verbunden wird. Anschließend kann man in der Logging-Tabelle (z. B. über LANmonitor zu starten) sehr komfortabel nachvollziehen, welche Verbindungsaufbauten von der Firewall verhindert werden. Mit

diesen Informationen wird dann sukzessive die Firewall und “Allow-Regeln” erweitert.

Einige typische Anwendungsfälle sind im Folgenden aufgezeigt.

Hinweis: Alle hier beschriebenen Filter können sehr komfortabel mit dem Firewall-Assistenten eingerichtet werden, um danach bei Bedarf mit z. B. LANconfig weiter verfeinert zu werden.

- Beispielkonfiguration “Basic Internet”

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst (Zielport)*
ALLOW_HTTP	Lokales Netzwerk	Alle Stationen	Übertragen	HTTP, HTTPS
ALLOW_FTP	Lokales Netzwerk	Alle Stationen	Übertragen	FTP
ALLOW_EMAIL	Lokales Netzwerk	Alle Stationen	Übertragen	MAIL, NEWS
ALLOW_DNS_FORWARDING	Lokales Netzwerk	IP-Adresse des LANOM (alternativ: Lokales Netzwerk)	Übertragen	DNS
DENY_ALL	Alle Stationen	Alle Stationen	Zurückweisen	ANY

- Sofern Sie VPN-Einwahl auf ein Gerät als VPN-Gateway gestatten wollen, benötigen Sie eine Firewall-Regel, die die Kommunikation des Clients mit dem lokalen Netz erlaubt:

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst*
ALLOW_VPN_DIAL_IN	Gegenstellenname	Lokales Netzwerk	Übertragen	ANY

- Für den Fall, dass ein VPN nicht vom Gerät selbst terminiert wird (z. B. VPN-Client im lokalen Netz, oder das Gerät als Firewall vor einem zusätzlichen VPN-Gateway), so müssen Sie zusätzlich IPSec bzw. PPTP (für das ’IPSec over PPTP’ des VPN Clients) freischalten:

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst (Zielport)*
ALLOW_VPN	VPN-Client	VPN-Server	Übertragen	IPSEC, PPTP

- Sofern Sie ISDN-Einwahl oder V.110-Einwahl (z. B. per HSCSD-Handy) gestatten, müssen Sie die betreffende Gegenstelle freischalten:

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst*
ALLOW_DIAL_IN	Gegenstellenname	Lokales Netzwerk	Übertragen	ANY

- Für eine Netzwerkkopplung gestatten Sie zusätzlich die Kommunikation zwischen den beteiligten Netzwerken:

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst*
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	Übertragen	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	Übertragen	ANY

- Wenn Sie einen z. B. einen eigenen Webserver betreiben, so schalten Sie selektiv den Server frei:

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst (Zielport)*
ALLOW_WEBSERVER	ANY	Webserver	Übertragen	HTTP, HTTPS

- Für Diagnosezwecke empfiehlt sich ferner die Freischaltung des ICMP-Protokolls (z. B. ping):

Regel	*Quelle*	*Ziel*	*Aktion*	*Dienst*
ALLOW_PING	Lokales Netzwerk	Alle Stationen	Übertragen	ICMP

Diese Regeln können jetzt beliebig verfeinert werden - z. B. durch die Angabe von Mindest- und Maximalbandbreiten für den Serverzugriff, oder aber durch die feinere Einschränkung auf bestimmte Dienste, Stationen oder Gegenstellen.

Hinweis: Das Gerät nimmt beim Aufbau der Filterliste eine automatische Sortierung der Firewall-Regeln vor. Dies geschieht dadurch, dass die Regeln anhand ihres Detaillierungsgrades sortiert in die Filterliste eingetragen werden. Zunächst werden alle spezifischen Regeln beachtet, danach die allgemein (z. B. Deny-All). Prüfen Sie bei komplexen Regelwerken die Filterliste, wie im nachfolgenden Abschnitt beschrieben.

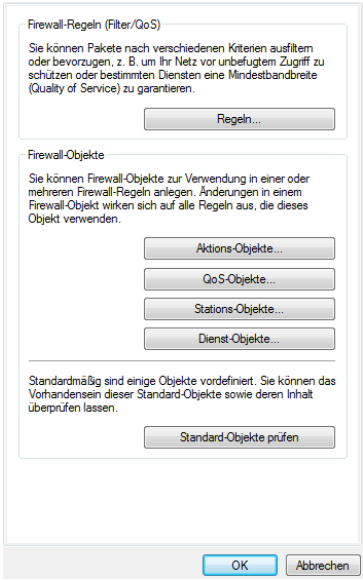
8.4 Konfiguration der Firewall mit LANconfig

8.4.1 Definition der Firewall-Objekte

Bei der Konfiguration der Firewall mit LANconfig können verschiedene Objekte definiert werden, die in den Firewall-Regeln verwendet werden. Auf diese Weise müssen häufig benutzte Definitionen (z. B. eine bestimmte Aktion) nicht bei jeder Regel neu eingegeben werden, sondern können einmal an einem zentralen Ort abgelegt werden.

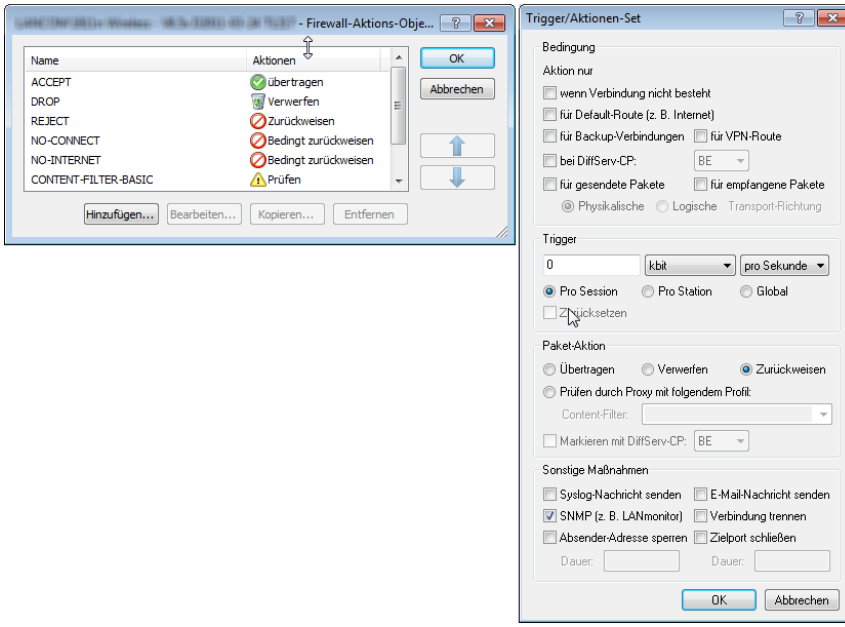
Hinweis: Bitte beachten Sie, dass sich eine Änderung der Firewall-Objekte auf alle Firewall-Regeln auswirkt, die dieses Objekt verwenden. Daher werden beim Ändern von Firewall-Objekten alle Firewall-Regeln angezeigt, die ebenfalls diese Objekte verwenden.

Hinweis: Existierende Firewalls (in der %-Schreibweise) werden beim Öffnen der Konfiguration mit LANconfig nicht automatisch auf die objektorientierte Form umgestellt.



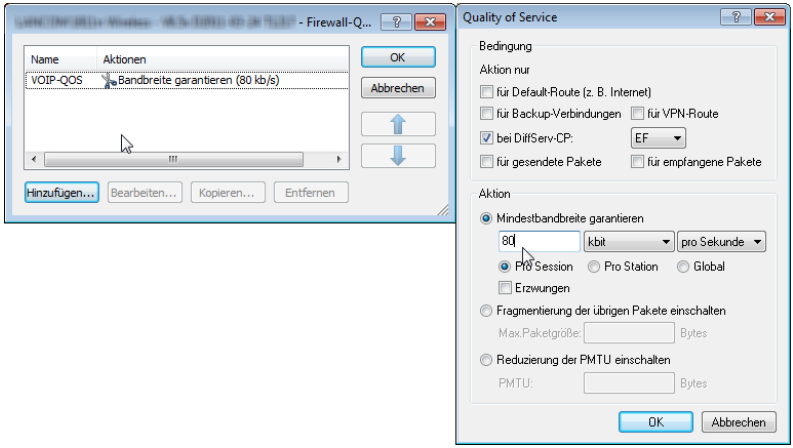
Aktions-Objekte

Hier legen Sie die Firewall-Aktion fest, bestehend aus Bedingung, Limit, Paket-Aktion und sonstigen Maßnahmen, die durch die Firewall-Regeln verwendet werden sollen.



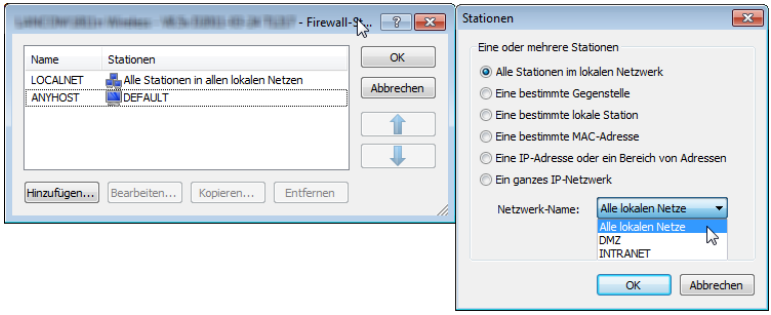
QoS-Objekte

Hier können Sie die Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die Firewall-Regeln verwendet werden sollen.



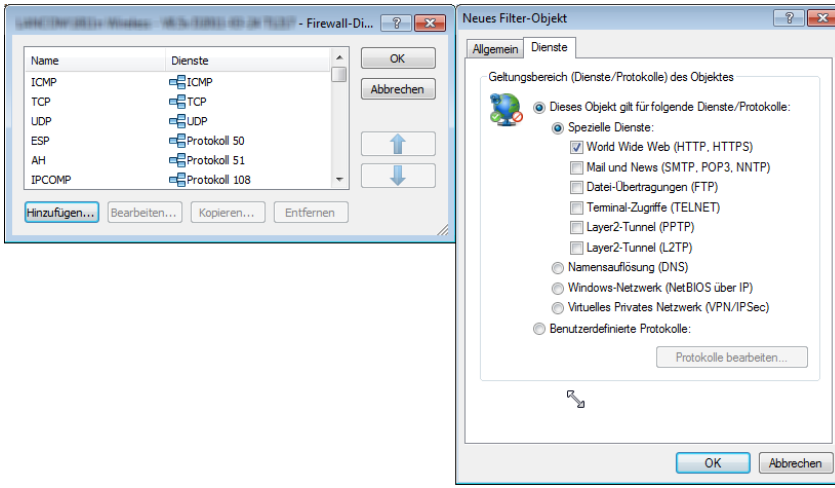
Stations-Objekte

Hier werden die Stationen festgelegt, die als Absender oder Adressat der Pakete durch die Firewall-Regeln verwendet werden sollen. Die Stations-Objekte sind dabei nicht auf Quelle oder Ziel festgelegt, sondern können in den Firewall-Regeln je nach Bedarf verwendet werden. Im Zusammenhang mit ARF ist es z. B. möglich, eine bestimtmes IP-Netzwerk als Stations-Objekt zu definieren.



Dienst-Objekte

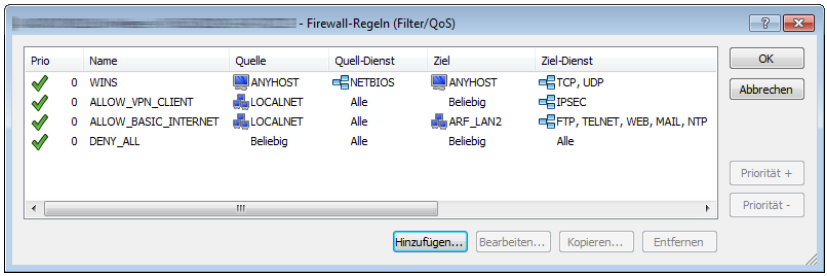
Hier werden die IP-Protokolle, Quell- und Zielports definiert, die durch die Firewall-Regeln verwendet werden sollen.



8.4.2 Definition der Firewall-Regeln

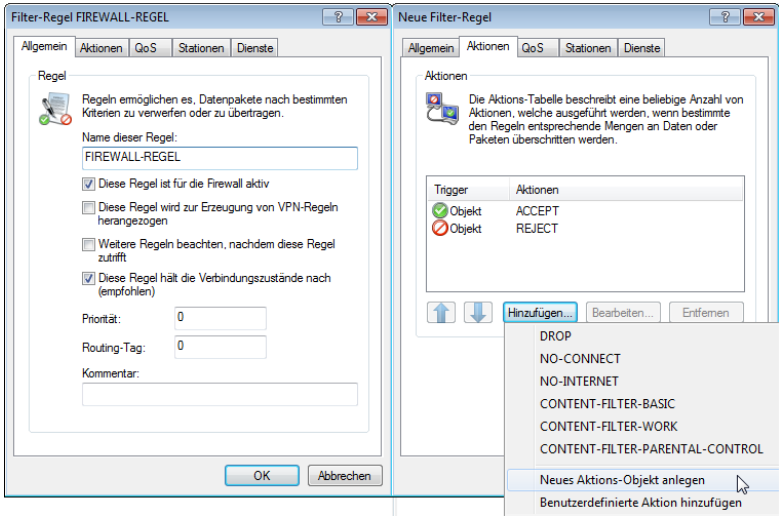
Die Firewall-Regeln werden in einer übersichtlichen Tabelle mit folgenden Informationen dargestellt:

- In der Spalte äußerst links zeigen Symbole den Zustand der Firewall-Regel an:
  - Grünes Häkchen: Firewall-Regel ist aktiv.
  - Rotes Kreuzchen: Firewall-Regel ist nicht aktiv.
  - Schloss: Firewall-Regel wird zur manuellen Erzeugung von VPN-Regeln verwendet.
  - Zwei verkettete Pfeile: Wenn diese Firewall-Regel zutrifft, bitte weitere Regeln beachten.
- Name der Firewall-Regel
- Quelle
- Ziel
- Quell- und Ziel-Dienst
- Aktion/QoS
- Kommentar



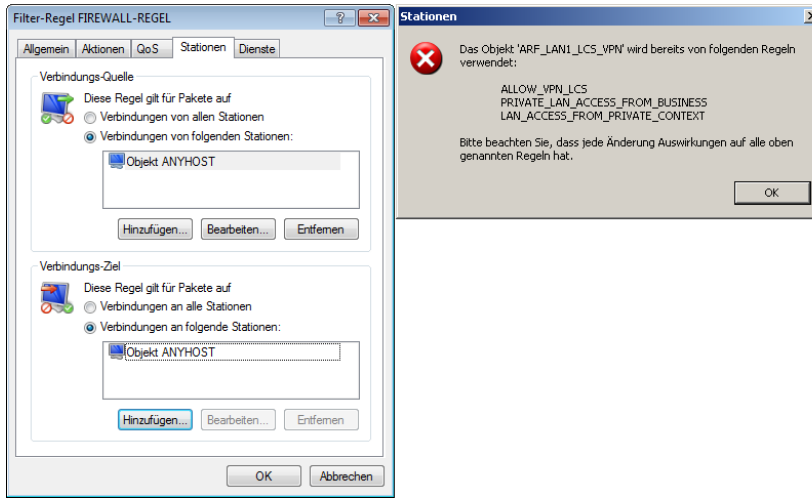
Neue Firewall-Regel hinzufügen

Beim Anlegen einer neuen Firewall-Regel werden zunächst die allgemeinen Daten erfasst. Auf den folgenden Registerkarten für Aktionen, QoS, Stationen oder Dienste werden die schon definierten Objekte zur direkten Verwendung angeboten. Alternativ können von dieser Stelle aus neue Objekte angelegt werden, die auch in anderen Regeln verwendet werden können oder benutzerdefinierte Einträge, die nur in der aktiven Firewall-Regel zum Einsatz kommen.



Firewall-Regel bearbeiten

Beim Bearbeiten einer bestehenden Firewall-Regel wird angezeigt, ob Aktionen, QoS, Stationen oder Dienste als vordefiniertes Objekt eingefügt wurden. Wenn ein referenziertes Objekt bearbeitet werden soll, das schon in anderen Firewall-Regeln verwendet wird, wird ein entsprechender Hinweis ausgegeben.



8.4.3 Getrennte Ansicht für IPv4- und IPv6-Firewall

Ab Firmware-Version 8.80 können Sie die Regeln für die IPv4- und IPv6-Firewalls mit LANconfig jeweils in getrennten Ansichten konfigurieren.

Sie finden die jeweilige Konfigurationen nun unter **Firewall/QoS** > **IPv4-Regeln** bzw. **Firewall/QoS** > **IPv6-Regeln**.

8.5 Konfiguration der Firewall-Regeln mit WEBconfig oder Telnet

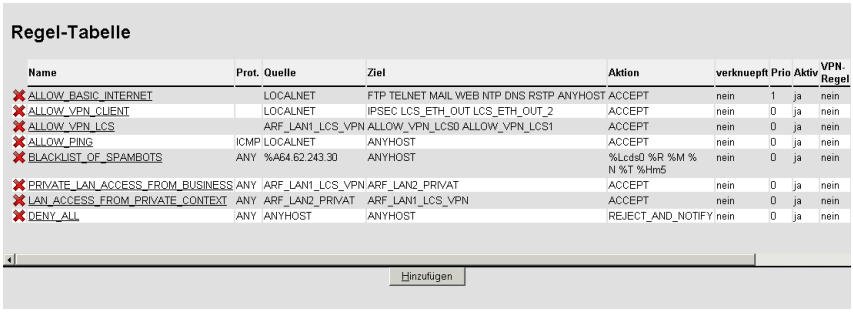
8.5.1 Regel-Tabelle

WEBconfig: Setup / IP-Router / Firewall / Regel-Tabelle

In der Regel-Tabelle werden verschiedene Informationen zu einer Firewall-Regel verknüpft. Die Regel enthält das zu filternde Protokoll, die Quelle, das Ziel sowie die auszuführende Firewall-Aktion. Zusätzlich gibt es für jede Firewall-Regel einen Ein-/Ausschalter, eine Priorität, die Option für eine Verknüpfung mit anderen Regeln und eine Aktivierung der Regel für VPN-Verbindungen.

Hinweis: Das Routing-Tag 0 bedeutet hier 'nicht markieren'. Wenn das Gerät Datenpakete in ein mit 0 getaggtes Netz leiten soll, tragen Sie hier bitte 65535 ein.

Wie in LANconfig kann auch in WEBconfig die Konfiguration der Firewall mit Hilfe von Objekten vorgenommen werden. Die im folgenden beschriebene %-Schreibweise ist nur bei der Definition von Objekten oder Aktionen erforderlich.



Hinweis: Existierende Firewalls in der %-Schreibweise werden nicht automatisch auf die objektorientierte Form umgestellt.

Hinweis: Bei Geräten mit einer Firmware-Version 7.6 oder neuer sind automatisch die wichtigsten Objekte in der Firewall vordefiniert. Bei der Bearbeitung von älteren Konfiguration mit LANconfig werden die Standard-Objekte der Firewall automatisch ergänzt.

Zur Beschreibung der Firewall-Regeln gibt es in der Firmware eine spezielle Syntax. Diese Syntax erlaubt es, auch komplexe Zusammenhänge für die Prüfung und Behandlung von Datenpaketen in der Firewall mit wenigen Zeichen darzustellen. Die Regeln werden in der Regel-Tabelle definiert. Damit häufig verwendete Objekte nicht jedesmal wieder neu in der Firmware-Syntax eingetragen werden müssen, können in zwei weiteren Tabellen vordefinierte Objekte gespeichert werden:

- In der Aktionstabelle sind die Firewall-Aktionen enthalten
- In der Objekttabelle sind die Stationen und Dienste enthalten

Hinweis: Die Objekte aus diesen Tabellen können bei der Regeldefinition verwendet werden, müssen es aber nicht! Sie erleichtern lediglich die Verwendung von häufiger verwendeten Objekten.

Die Definition der Firewall-Regeln kann sowohl aus Einträgen der Objekttabelle für Protokolle, Dienste, Stationen und der Aktionstabelle für die Firewall-Aktionen bestehen, als auch direkte Beschreibungen in der entsprechenden Firmware-Syntax enthalten (z. B. %P6 für TCP).

Hinweis: Bei der direkten Eingabe der Pegel-Parameter in der Firmware-Syntax gelten die gleichen Regeln, wie sie für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

8.5.2 Objekttabelle

WEBconfig: Setup / IP-Router / Firewall / Objekt-Tabelle

In der Objekttabelle werden diejenigen Elemente bzw. Objekte definiert, die in der Regeltabelle der Firewall verwendet werden sollen. Objekte können sein:

- einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- ganze Netze

- Protokolle
- Dienste (Ports oder Port-Bereiche, z. B. HTTP, Mail&News, FTP, ...)

Diese Elemente lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z. B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man darauf aufbauend Objekte z. B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

8.5.3 Aktionstabelle

WEBconfig: Setup / IP-Router / Firewall / Aktions-Tabelle

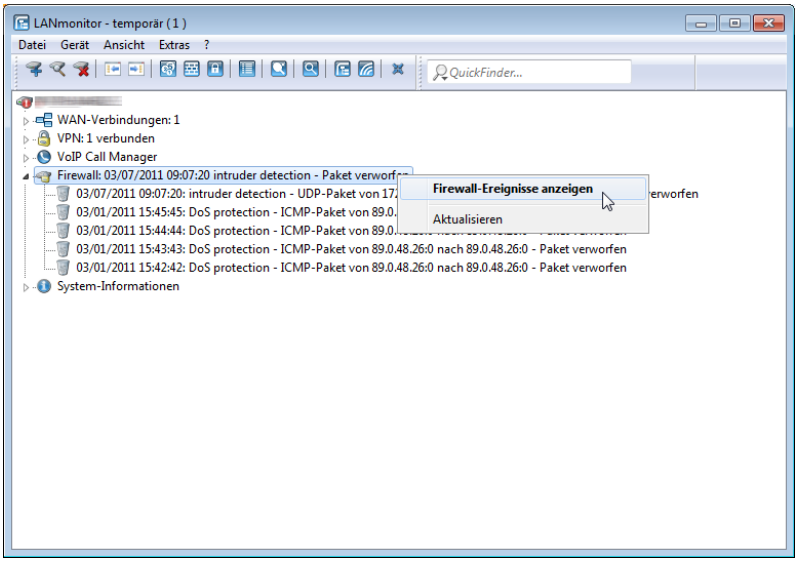
Eine Firewall-Aktion besteht aus einer Bedingung, einem Limit, einer Paket-Aktion und sonstigen Maßnahmen.

Die Firewall-Aktionen können wie bereits die Elemente der Objekt-Tabelle mit einem Namen versehen und beliebig rekursiv miteinander kombiniert werden, wobei die maximale Rekursionstiefe auf 16 beschränkt ist. Sie können aber auch direkt in das Aktionsfeld der Regeltabelle eingetragen werden.

8.6 Firewall-Diagnose

Alle Ereignisse, Zustände und Verbindungen der Firewall können detailliert protokolliert und überwacht werden.

Die komfortabelste Überwachung ergibt sich mit der Anzeige der Logging-Tabelle (s. u.) durch den LANmonitor. Im LANmonitor werden im Bereich ’Firewall’ die letzten fünf Ereignisse angezeigt, die durch eine Firewall-Regel, das DoS- oder IDS-System mit aktivierter ’SNMP’-Option ausgelöst wurden.



Mit einem Klick der rechten Maustaste auf diese Rubrik öffnet sich im Kontextmenü unter dem Eintrag Firewall-Ereignisanzeige ein neues Fenster mit der vollständigen Logging-Tabelle *Die Firewall-Tabelle* auf Seite 757.

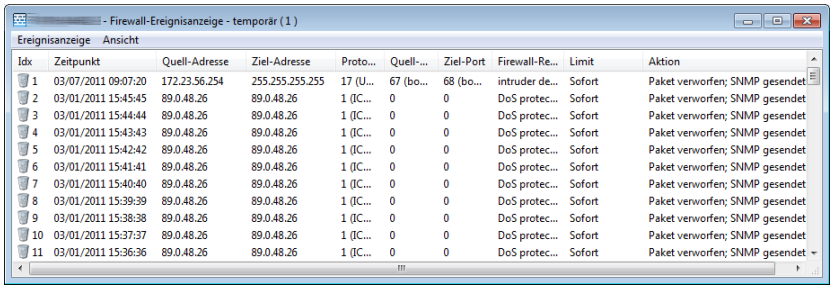
Alle in diesem Abschnitt beschriebenen Listen und Tabellen finden Sie unter folgenden Menüpunkten:

WEBconfig: HiLCOS-Menübaum / Status / IP-Router-Statistik

8.6.1 Die Firewall-Tabelle

Wenn ein zu loggendes Ereignis eingetreten ist, d.h. als auszuführende Aktion beim Empfang eines Paketes ist eine Mitteilung per E-Mail, Syslog oder SNMP gefordert, so wird dieses Ereignis in einer Logging-Tabelle festgehalten.

Wird die Logging-Tabelle über den LANmonitor aufgerufen, präsentiert sie sich in folgender Darstellung:



Wird die Logging-Tabelle über WEBconfig aufgerufen, präsentiert sie sich in folgender Darstellung:

Experten-Konfiguration
Status
IP-Router-Statistik

Log-Tabelle

Idx.	System-Zeit	Quell-Adresse	Ziel-Adresse	Prot.	Quell-Port	Ziel-Port	Filterregel	Limit	Schwelle	Aktion
0001	9.12.2003 10:58:48	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0002	9.12.2003 10:58:48	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0003	9.12.2003 10:58:20	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0004	9.12.2003 10:13:49	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0005	9.12.2003 10:13:49	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0006	9.12.2003 9:24:27	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0007	9.12.2003 5:05:21	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0008	8.12.2003 21:59:24	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
0009	8.12.2003 20:19:38	192.168.2.60	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108
000a	8.12.2003 20:19:38	0.0.0.0	224.0.0.22	2	0	0	DENY_ALL	00000022	0	40000108

Diese Tabelle enthält die folgenden Werte:

Element	***Bedeutung***
Idx.	laufender Index (damit die Tabelle auch über SNMP abgefragt werden kann)
System-Zeit	System-Zeit in UTC Kodierung (wird bei der Ausgabe der Tabelle in Klartext umgewandelt)
Quell-Adresse	Quell-Adresse des gefilterten Pakets
Ziel-Adresse	Zieladresse des gefilterten Pakets
Prot.	Protokoll (TCP, UDP etc.) des gefilterten Pakets
Quell-Port	Quell-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)
Ziel-Port	Ziel-Port des gefilterten Pakets (nur bei portbehafteten Protokollen)
Filterregel	Name der Regel, die den Eintrag erzeugt hat.
Limit	Bitfeld, dass das überschrittene Limit beschreibt, durch welches das Paket gefiltert wurde. Folgende Werte sind zur Zeit definiert: ▶ 0x01 Absolute Anzahl

Element	*Bedeutung*
	▶ 0x02 Anzahl pro Sekunde ▶ 0x04 Anzahl pro Minute ▶ 0x08 Anzahl pro Stunde ▶ 0x10 globales Limit ▶ 0x20 Bytelimit (wenn nicht gesetzt, handelt es sich um ein Paket-Limit) ▶ 0x40 Limit gilt nur in Empfangsrichtung ▶ 0x80 Limit gilt nur in Senderichtung
Schwelle	überschrittener Grenzwert des auslösenden Limits
Aktion	Bitfeld, das alle ausgeführten Aktionen aufführt. Folgende Werte sind zur Zeit definiert: ▶ 0x00000001 Accept ▶ 0x00000100 Reject ▶ 0x00000200 Aufbaufilter ▶ 0x00000400 Internet- (Defaultrouten-) Filter ▶ 0x00000800 Drop ▶ 0x00001000 Disconnect ▶ 0x00004000 Quell-Adresse sperren ▶ 0x00020000 Zieladresse und -port sperren ▶ 0x20000000 Sende Syslog-Benachrichtigung ▶ 0x40000000 Sende SNMP-Trap ▶ 0x80000000 Sende E-Mail

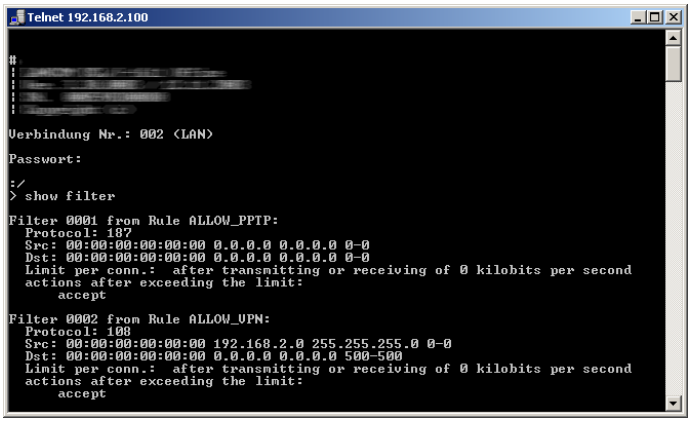
Hinweis: Alle Firewall-Aktionen werden ebenfalls im IP-Router-Trace angezeigt. Einige Modelle verfügen ferner über eine Firewall-LED, welche jedes gefilterte Paket signalisiert.

Die Filterliste

Über die Filterliste können die aus den in der Aktions-, Objekt- und Regeltabelle definierten Regeln erzeugten Filter ermittelt werden.

Hinweis: Bei einer manuellen Filter-Definition über Telnet oder WEBconfig wird kein Eintrag in der Filterliste angelegt, wenn die Definition Fehler in der Syntax enthält. In diesem Fall wird auch keine Fehlermeldungen ausgegeben! Wenn Sie die Filter manuell konfigurieren, sollten Sie in jedem Fall anhand der Filterliste überprüfen, ob die gewünschten Filter erzeugt wurden.

Auf Telnet-Ebene kann der Inhalt der Filterliste auch mit dem Kommando `show filter` anzeigt werden:



Unter WEBconfig hat die Filterliste den folgenden Aufbau:

Experten-Konfiguration
Status
IP-Router-Statistik

Filter-Liste

Idx.	Prot.	Quell-MAC	Quell-Adresse	Quell-Netz-Maske	Q-von	Q-bis	Ziel-MAC	Ziel-Adresse	Ziel-Netz-Maske	Z-von	Z-bis	Aktion	verknuepft	Prio
0001	187	000000000000	0.0.0.0	0.0.0.0	0	0	000000000000	0.0.0.0	0.0.0.0	0	0	limit: accept	nein	0
0002	108	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept	nein	0
0003	51	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept	nein	0
0004	50	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept	nein	0
0005	17	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0	0	0	limit: inet reject	nein	0
0006	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	0.0.0.0	0.0.0.0	500	500	limit: accept	nein	0
0007	17	000000000000	192.168.2.0	255.255.255.0	0	0	000000000000	192.168.2.100	255.255.255.255	53	53	limit: accept	nein	0
0008	17	000000000000	0.0.0.0	0.0.0.0	0	0	000000000000	0.0.0.0	0.0.0.0	0	0	limit: accept	nein	0
0009	6	000000000000	0.0.0.0	0.0.0.0	137	139	000000000000	0.0.0.0	0.0.0.0	0	0	limit: inet reject	nein	0

Die einzelnen Felder in der Filterliste haben folgende Bedeutung:

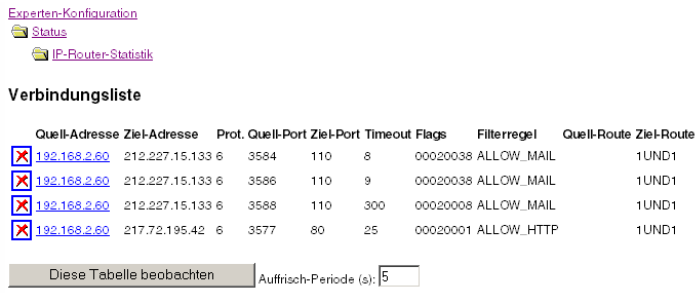
Eintrag	*Beschreibung*
Idx.	laufender Index
Prot	zu filterndes Protokoll, also z. B. 6 für TCP oder 17 für UDP
Quell-MAC	Ethernet-Quell-Adresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Quell-Adresse	Quell-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Quell-Netzmaske	Quell-Netzmaske, die zusammen mit der Quell-IP-Adresse das Quell-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete aus allen Netzen gelten soll
Q-von	Start-Quell-Port der zu filternden Pakete.
Q-bis	End-Quell-Port der zu filternden Pakete. Spannt zusammen mit dem Start-Quell-Port einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Quell-Ports

Eintrag	*Beschreibung*
Ziel-MAC	Ethernet-Zieladresse des zu filternden Pakets oder 000000000000, wenn der Filter für alle Pakete gelten soll
Ziel-Adresse	Ziel-IP-Adresse oder 0.0.0.0, wenn der Filter für alle Pakete gelten soll
Ziel-Netzmaske	Ziel-Netzmaske, die zusammen mit der Ziel-IP-Adresse das Ziel-Netz bestimmt, oder 0.0.0.0, wenn der Filter für Pakete zu allen Netzen gelten soll
Z-von	Start-Zielport der zu filternden Pakete.
Z-bis	End-Zielport der zu filternden Pakete. Spannt zusammen mit dem Start-Zielport einen Portbereich auf, in dem der Filter wirksam ist. Sind Start und Endport 0, so gilt der Filter für alle Zielports
Aktion	In dieser Spalte wird die “Hauptaktion”, also die Aktion textuell ausgegeben, die bei überschreiten des ersten Limits ausgeführt wird. Das erste Limit kann auch ein implizites Limit sein, so z. B. wenn nur ein Limit zur Beschränkung des Durchsatzes konfiguriert wurde, so wird ein implizites Limit, das mit einer “accept” Aktion verknüpft ist eingefügt. Als Hauptaktion wird in diesem Fall “accept” ausgegeben. Die vollständigen Aktionen lassen sich über das Kommando `show filter` anzeigen.
verknüpft	Gibt an, ob es sich bei dieser Regel um eine “First Match”-Regel handelt (verknüpft = Nein). Nur bei verknüpften Regeln werden im Falle des Zutreffens dieser Regel auch weitere Regeln ausgewertet.
Prio	Priorität der Regel, durch die der Eintrag erzeugt wurde.

Die Verbindungsliste

In der Verbindungstabelle werden Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port, Ziel-Port, etc. einer Verbindung nachgehalten sowie mögliche Aktionen gespeichert. Diese Tabelle ist sortiert nach Quell-Adresse, Ziel-Adresse, Protokoll, Quell-Port und Ziel-Port des Pakets, das den Eintrag in der Tabelle hervorgerufen hat.

Unter WEBconfig hat die Filterliste den folgenden Aufbau:



Die Tabelle enthält die folgenden Elemente:

Element	*Bedeutung*
Quell-Adresse	Quell-Adresse der Verbindung
Ziel-Adresse	Ziel-Adresse der Verbindung
Prot.	verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben
Quell-Port	Quell-Port der Verbindung. Der Port wird nur bei portbehafteten Protokollen (TCP/UDP) oder Protokollen, die ein vergleichbares Feld besitzen (ICMP/GRE) angegeben
Ziel-Port	Ziel-Port der Verbindung (bei UDP-Verbindungen wird dieser erst mit der ersten Antwort besetzt)
Timeout	Jeder Eintrag altert mit der Zeit aus dieser Tabelle heraus, damit die Tabelle bei “gestorbenen” Verbindungen nicht überläuft
Flags	In den Flags wird der Zustand der Verbindung und weitere (interne) Informationen in einem Bitfeld gespeichert. Als Zustände sind folgende Werte möglich: new, establish, open, closing, closed, rejected (entsprechend der TCP-Flags: SYN, SYN ACK, ACK, FIN, FIN ACK und RST) UDP-Verbindungen kennen nun die Zustände new, open und closing (letzteren nur, wenn die UDP-Verbindung mit einem zustandsbehafteten Steuerkanal verknüpft ist. Dies ist z. B. beim Protokoll H.323 der Fall)
Quell-Route	Name der Gegenstelle, über die das erste Paket empfangen wurde.
Ziel-Route	Name der Gegenstelle, auf die das erste Paket gesendet wird.
Filterregel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Bedeutung der Flags in der Verbindungsliste

Flag	*Bedeutung*
00000001	TCP: SYN gesendet
00000002	TCP: SYN/ACK empfangen
00000004	TCP: warte auf ACK des Servers
00000008	alle: Verbindung offen
00000010	TCP: FIN empfangen
00000020	TCP: FIN gesendet
00000040	TCP: RST gesendet oder empfangen
00000080	TCP: Sitzung wird wiederhergestellt
00000100	FTP: passive FTP-Verbindung wird aufgebaut
00000400	H.323: zugehörige T.120-Verbindung
00000800	Verbindung über Loopback-Interface

Flag	*Bedeutung*
00001000	prüfe verkettete Regeln
00002000	Regel ist verkettet
00010000	Ziel ist auf "lokaler Route"
00020000	Ziel ist auf Default-Route
00040000	Ziel ist auf VPN-Route
00080000	physikalische Verbindung ist nicht aufgebaut
00100000	Quelle ist auf Default-Route
00200000	Quelle ist auf VPN-Route
00800000	keine Route zum Ziel
01000000	enthält globale Aktion mit Bedingung

Portsperrliste

Wenn als Aktion die Sperrung des Zielports auf dem Zielrechner ausgewählt wurde, so werden Adresse, Protokoll und Port des Zielrechners in der Portsperrtabelle abgelegt. Diese Tabelle ist ebenfalls eine sortierte halbdynamische Tabelle. Die Sortierung erfolgt nach Adresse, Protokoll und Port. Die Tabelle enthält die folgenden Elemente:

Element	*Bedeutung*
Address	Adresse des Rechners, für den die Sperre gelten soll.
Protocol	Verwendetes Protokoll (TCP/UDP etc.) Das Protokoll wird dezimal angegeben.
Port	Zu sperrender Port auf dem Rechner. Wenn das jeweilige Protokoll nicht portbehaftet ist, dann wird das gesamte Protokoll für diesen Rechner gesperrt.
Timeout	Dauer der Sperre in Minuten.
Filterregel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

Hostsperrliste

Wenn als Aktion eines Filters die Sperrung des Absenders ausgewählt wurde, so werden Adresse des Rechners in der Hostsperrtabelle abgelegt. Diese Tabelle ist eine nach der Absenderadresse sortierte halbdynamische Tabelle und enthält die folgenden Elemente:

Element	*Bedeutung*
Address	Adresse des Rechners, der gesperrt werden soll
Timeout	Dauer der Sperre in Minuten
Filter-Regel	Name der Regel, die den Eintrag erzeugt hat (diese bestimmt auch die auszuführenden Aktionen), wenn ein passendes Paket empfangen wird.

8.7 Grenzen der Firewall

Neben dem Verständnis der Funktionsweise der Firewall ist es auch sehr wichtig, ihre Grenzen zu erkennen und sie ggf. weiter zu ergänzen. So schützt die Firewall grundsätzlich nicht vor bösartigen Inhalten, die auf den zugelassenen Wegen in das lokale Netzwerk gelangen. Die Auswirkungen einiger Viren und Würmer werden zwar unterbunden, weil die Kommunikation über die benötigten Ports gesperrt ist, aber einen echten Schutz vor Viren bietet die Firewall allein nicht.

Auch das Abhören von sensiblen Daten im Internet wird durch die Firewall nicht verhindert. Sind die Daten erst einmal über die Firewall hinaus in das unsichere Netz gelangt, stehen sie dort weiterhin den bekannten Gefahren gegenüber. Vertrauliche Informationen wie Verträge, Passwörter, Entwicklungsinformationen etc. sollten daher auch bei Einsatz einer Firewall nur geschützt übertragen werden, z. B. durch den Einsatz geeigneter Verschlüsselungsverfahren oder über VPN-Verbindungen.

8.8 Abwehr von Einbruchsversuchen: Intrusion Detection

Die Firewall hat die Aufgabe, den Datenverkehr über die Grenzen zwischen den Netzwerken hinweg zu prüfen und diejenigen Datenpakete, die keine Erlaubnis für die Übertragung mitbringen, zurückzuweisen bzw. zu verwerfen. Neben dem Ansatz, direkt auf einen Rechner im geschützten Netzwerk zuzugreifen, gibt es aber auch Angriffe auf die Firewall selbst oder Versuche, die Firewall mit gefälschten Datenpaketen zu überlisten.

Solche Versuche werden über ein Intrusion-Detection-System (IDS) erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYSLOG-Alarmen gewählt werden. Das IDS prüft den Datenverkehr auf bestimmte Eigenschaften hin und erkennt so auch neue Angriffe, die nach auffälligen Mustern ablaufen.

8.8.1 Beispiele für Einbruchsversuche

Als typische Einbruchsversuche kann man gefälschte Absender-Adressen (“IP-Spoofing”) und Portscans ansehen, sowie den Missbrauch spezieller Protokolle wie z. B. FTP, um einen Port im angegriffenen Rechner und der davor hängenden Firewall zu öffnen.

IP-Spoofing

Beim IP-Spoofing gibt sich der Absender eines Pakets als ein anderer Rechner aus. Dies geschieht entweder, um Firewalls zu überlisten, die Paketen aus dem eigenen Netz mehr Vertrauen schenken als Paketen aus fremden Netzen, oder um den Urheber eines Angriffs (z. B. Smurf) zu verschleiern.

Die Geräte-Firewall schützt sich davor durch Routenprüfung, d.h. sie überprüft, ob das Paket überhaupt über das Interface empfangen werden durfte, von dem es empfangen wurde.

Portscan-Erkennung

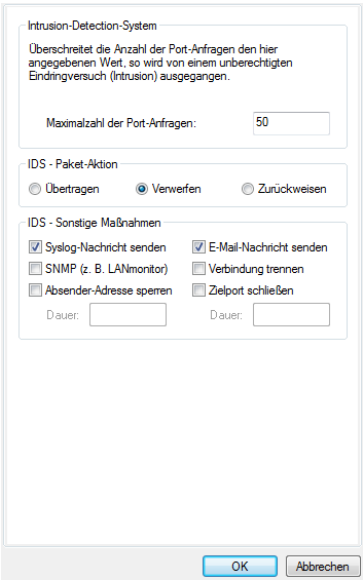
Das Intrusion-Detection System versucht Portscans zu erkennen, zu melden und geeignet auf den Angriff zu reagieren. Dies geschieht ähnlich der Erkennung eines ’SYN Flooding’-Angriffs (siehe *SYN Flooding* auf Seite 769): Es werden auch hier die “halboffenen” Verbindungen gezählt, wobei ein TCP-Reset, das vom gescannten Rechner gesendet wird, die “halboffene” Verbindung weiterhin offen lässt.

Wenn eine bestimmte Anzahl von halboffenen Verbindungen zwischen dem gescannten und dem scannenden Rechner existiert, so wird dies als Portscan gemeldet.

Ebenso wird der Empfang von leeren UDP-Paketen als versuchter Portscan interpretiert

8.8.2 Konfiguration des IDS

Hier finden Sie die Einstellungen des IDS.



LANconfig: Firewall/QoS / IDS

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Firewall

Neben der Maximalzahl der Portanfragen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- Die Verbindung wird getrennt
- Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

8.9 Schutz vor “Denial-of-Service”-Angriffen

Angriffe aus dem Internet können neben Einbruchsversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Diese Angriffe nennt man auch “Denial-Of-Service”.

Die Geräte sind mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit erhalten.

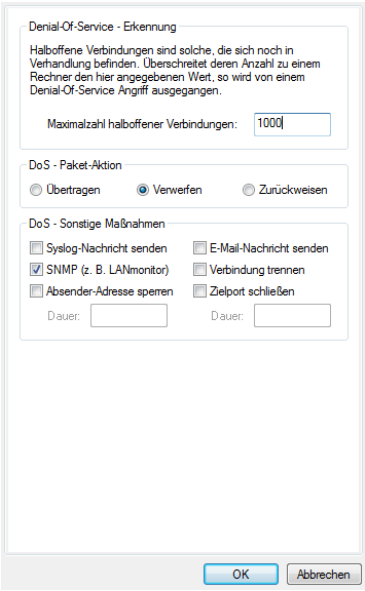
8.9.1 Erhöhter DoS-Schwellwert für Zentralgeräte

Denial-Of-Service Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen aus.

- Zu den Angriffen, die prinzipielle Schwächen ausnutzen, gehören z. B. SYN-Flood und Smurf.
- Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop) oder mit gefälschten Absenderadressen arbeiten (z. B. Land).

Ihr Gerät erkennt die meisten dieser Angriffe und kann mit gezielten Gegenmaßnahmen reagieren. Für diese Erkennung wird die Anzahl der Verbindungen ermittelt, die sich noch in Verhandlung befinden (halboffene Verbindungen). Überschreitet die Anzahl der halboffenen Verbindungen einen Schwellwert, geht das Gerät von einem DoS-Angriff aus. Die dann resultierenden Aktionen und Maßnahmen können wie bei Firewall-Regeln definiert werden.

Hinweis: Für Zentralgeräte befinden sich aufgrund der zumeist höheren Anzahl der angeschlossenen Benutzer auch ohne DoS-Angriff eine große Zahl von Verbindungen im halboffenen Zustand. Aus diesem Grund verwenden diese Geräte einen höheren Standard-Schwellwert für die Erkennung der DoS-Angriffe.



LANconfig: Firewall/QoS / DoS

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Firewall

- **Maximalzahl halboffene Verbindungen**

  Legen Sie hier fest, ab welcher Anzahl von halboffenen Verbindungen die Aktionen zur Abwehr von DoS-Angriffen ausgelöst werden sollen.

  Mögliche Werte:

  – 0 bis 9999

  Default:

  – 100
  – 1000 für Zentralgeräte wie 7100, 7111, 8011, 9100, 4025(+), 4100.

8.9.2 Beispiele für Denial-of-Service-Angriffe

Denial-Of-Service-Angriffe nutzen prinzipielle Schwächen der TCP/IP-Protokolle sowie fehlerhafte Implementationen von TCP/IP-Protokollstacks aus. Zu den Angriffen, die prinzipiellen Schwächen ausnutzen, gehören z. B. SYN-

Flood und Smurf. Zu den Angriffen, die fehlerhafte Implementationen zum Ziel haben, gehören alle Angriffe, die mit fehlerhaft fragmentierten Paketen operieren (z. B. Teardrop), oder die mit gefälschten Absenderadressen arbeiten (z. B. Land). Im folgenden werden einige dieser Attacken, deren Auswirkungen und mögliche Gegenmaßnahmen beschrieben.

SYN Flooding

Beim SYN-Flooding schickt der Angreifer in kurzen zeitlichen Abständen TCP-Pakete, mit gesetztem SYN-Flag und sich ständig ändernden Quell-Ports auf offene Ports seines Opfers. Der angegriffene Rechner richtet darauf hin eine TCP-Verbindung ein, sendet dem Angreifer ein Paket mit gesetzten SYN- und ACK-Flags und wartet nun vergeblich auf die Bestätigung des Verbindungsaufbaus. Dadurch bleiben dann hunderte “halboffener” TCP-Verbindungen zurück, und verbrauchen Ressourcen (z. B. Speicher) des angegriffenen Rechners. Das ganze kann letztendlich so weit gehen, dass das Opfer keine TCP-Verbindung mehr annehmen kann oder gar aufgrund von Speichermangel abstürzt.

Als Gegenmaßnahme in einer Firewall hilft nur, die Anzahl “halboffener” TCP-Verbindungen, die zwischen zwei Rechnern bestehen zu überwachen und zu beschränken, d.h. falls weitere TCP-Verbindungen zwischen diesen Rechnern aufgebaut werden, dann müssen diese von der Firewall abgeblockt werden.

Smurf

Der Smurf-Angriff arbeitet zweistufig und legt gleich zwei Netze lahm. Im ersten Schritt wird mit gefälschter Absenderadresse ein Ping (ICMP Echo-Request) an die Broadcastadresse des ersten Netzes gesendet, worauf alle Rechner in diesem Netz mit einem ICMP-Echo-Reply und die gefälschte Absenderadresse (die im zweiten Netz liegt) antworten. Wenn die Rate der einkommenden Echo-Requests sowie die Anzahl der antwortenden Rechner hoch genug ist, dann wird zum einen der gesamte einkommende Traffic des zweiten Netzes für die Dauer der Attacke blockiert, zum anderen kann der Besitzer der gefälschten Adresse für die Dauer der Attacke keine normalen Daten mehr annehmen. Ist die gefälschte Absenderadresse die Broadcastadresse des zweiten Netzes, so sind sogar alle Rechner in diesem Netz blockiert.

In diesem Fall blockiert die DoS-Erkennung des Gerätes das Weiterleiten von Paketen, die an die lokale Broadcastadresse gerichtet sind.

LAND

Beim LAND-Angriff handelt es sich um ein TCP-Paket, dass mit gesetztem SYN-Flag und gefälschter Absender-Adresse an den Opferrechner geschickt wird. Das Pikante dabei ist, dass die gefälschte Absenderadresse gleich der Adresse des Opfers ist. Bei einer unglücklichen Implementierung des TCP wird das auf dieses Paket gesendete SYN-ACK vom Opfer wieder als “SYN” interpretiert und ein neues SYN-ACK gesendet. Dies führt zu einer Endlosschleife, die den Rechner einfrieren lässt.

Bei einer neueren Variante wird als Absenderadresse des Pakets nicht die Adresse des angegriffenen Rechners eingesetzt, sondern die Loopback-Adresse “127.0.0.1”. Sinn dieser Täuschung ist es, Personal Firewalls zu überlisten, die zwar auf die klassische Variante (Absenderadresse = Zieladresse) reagieren, die neue Form aber ungehindert durchlassen. Diese Form wird vom Gerät ebenfalls erkannt und geblockt.

Ping of Death

Der Ping of Death gehört zu den Angriffen, die Fehler bei der Reassemblierung von fragmentierten Paketen ausnutzen. Dies funktioniert wie folgt:

Im IP-Header befindet sich das Feld “Fragment-Offset” das angibt, an welcher Stelle das empfangene Fragment in das IP-Paket eingebaut werden soll. Dieses Feld hat eine Länge von 13 Bit und gibt die Einfügeposition in jeweils 8 Byte grossen Schritten an. Die Einfügeposition kann daher zwischen 0 und 65528 Bytes liegen. Bei einer MTU auf dem Ethernet von 1500 Bytes kann somit ein bis zu 65528 + 1500 - 20 = 67008 Byte großes IP-Paket erzeugt werden, was zu Überläufen von internen Zählern führen oder gar Pufferüberläufe provozieren kann und es somit dem Angreifer gar die Möglichkeit eröffnet, eigenen Code auf dem Opferrechner auszuführen.

Hier bieten sich der Firewall zwei Möglichkeiten: Entweder, die Firewall reassembliert das gesamte einkommende Paket und prüft dessen Integrität, oder aber es wird nur das Fragment, das über die maximale Paketgröße hinaus geht, verworfen. Im ersten Fall kann die Firewall bei einer fehlerhaften Implementation selbst zum Opfer werden, im zweiten Fall sammeln sich beim

Opfer “halb” reassemblierte Pakete an, die erst nach einer gewissen Zeit verworfen werden, wodurch sich ein neuer Denial-Of-Service Angriff ergeben kann, wenn dem Opfer dadurch der Speicher ausgeht.

Teardrop

Der Teardrop-Angriff arbeitet mit überlappenden Fragmenten. Dabei wird nach dem ersten Fragment ein weiteres geschickt, das komplett innerhalb des ersten liegt, d.h. das Ende des zweiten Fragments liegt vor dem Ende des ersten. Wird nun aus Bequemlichkeit des Programmierers des IP-Stack bei der Ermittlung der Länge der zur Reassemblierung zu kopierenden Bytes einfach “neues Ende” - “altes Ende” gerechnet, so ergibt sich ein negativer Wert, bzw. ein sehr großer positiver Wert, durch den bei der Kopieroperation Teile des Speichers des Opfers überschrieben werden und der Rechner daraufhin abstürzt.

Auch hier hat die Firewall wieder zwei Möglichkeiten: Entweder sie reassembliert selbst und verwirft ggf. das gesamte Paket, oder sie hält nur minimalen Offset und maximales Ende des Pakets nach und verwirft alle Fragmente, deren Offset oder Ende in diesen Bereich fallen. Im ersten Fall muss die Implementation innerhalb der Firewall korrekt sein, damit diese nicht selbst Opfer wird, im anderen Fall sammeln sich wieder “halb” reassemblierte Pakete beim Opfer.

Bonk/Fragrouter

Bonk ist eine Variante des Teardrop-Angriffs, die jedoch nicht zum Ziel hat den angegriffenen Rechner zum Absturz zu bringen, sondern einfache Portfilter Firewalls, die auch fragmentierte Pakete akzeptieren auszutricksen und somit in das zu schützende Netz einzudringen. Bei diesem Angriff wird nämlich durch geschickte Wahl des Fragment-Offsets der UDP- oder TCP-Header des ersten Fragments überschrieben. Hierdurch akzeptieren einfache Portfilter-Firewalls das erste Paket und die dazugehörenden Fragmente. Durch das Überschreiben des Headers im zweiten Fragment, wird so ganz plötzlich aus einem erlaubten Paket ein Paket, das eigentlich in der Firewall geblockt werden sollte.

Auch hier gilt, die Firewall kann entweder selbst Re-assemblieren, oder nur das falsche Fragment (und alle nachfolgenden) filtern, mit den bereits oben angedeuteten Problemen der einen oder anderen Lösung.

Hinweis: In der Default-Einstellung sind alle Einstellungen auf “sicher” konfiguriert, d.h. maximal 100 zulässige halboffene Verbindungen von verschiedenen Rechnern (vgl. SYN-Flooding), maximal 50 halboffene Verbindungen von einem Rechner (vgl. Portscan) fragmentierte Pakete werden re-assembliert.

8.9.3 Konfiguration der DoS-Abwehr

LANconfig: Firewall/QoS / DoS

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Firewall

Hinweis: Um die Anfälligkeit des Netzes vor DoS-Attacken schon im Vorfeld drastisch zu reduzieren, dürfen Pakete aus entfernten Netzen nur dann angenommen werden, wenn entweder eine Verbindung vom internen Netz aus initiiert wurde, oder die einkommenden Pakete durch einen expliziten Filtereintrag (Quelle: entferntes Netz, Ziel: lokales Netz) zugelassen werden. Diese Maßnahme blockiert bereits eine Vielzahl von Angriffen.

Für alle erlaubten Zugriffe werden im Gerät explizit Verbindungszustand, Quell-Adressen und Korrektheit von Fragmenten überprüft. Dies geschieht sowohl für einkommende als auch für ausgehende Pakete, da ein Angriff auch aus dem lokalen Netz heraus gestartet werden kann.

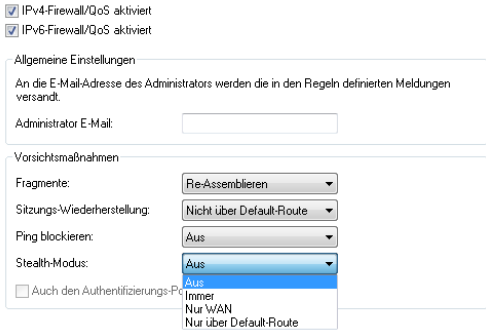
Um nicht durch fehlerhafte Konfiguration der Firewall ein Tor für DoS-Angriffe zu öffnen, wird dieser Teil zentral konfiguriert. Neben der Maximalzahl der halboffenen Verbindungen, der Paket-Aktion und den möglichen Meldemechanismen gibt es hier noch weitergehende Reaktionsmöglichkeiten:

- Die Verbindung wird getrennt
- Die Adresse des Absenders wird für eine einstellbare Zeit gesperrt
- Der Zielport des Scans wird für eine einstellbare Zeit gesperrt

Immer aktiv hingegen sind folgende Schutzmechanismen:

- Adressüberprüfung (gegen IP-Spoofing)
- Abblocken von Broadcasts in lokale Netz (gegen Smurf und Co).

8.9.4 Konfiguration von ping-Blocking und Stealth-Modus



LANconfig: Firewall/QoS / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Firewall

9 Quality-of-Service

Dieses Kapitel widmet sich dem Thema Quality-of-Service (kurz: QoS). Unter diesem Oberbegriff sind die Funktionen des HiLCOS zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstgüten befassen.

9.1 Wozu QoS?

Generell möchte man mit dem Quality-of-Service erreichen, dass bestimmte Datenpakete entweder besonders sicher oder möglichst sofort übertragen werden.

9.2 Welche Datenpakete bevorzugen?

Die Notwendigkeit für das QoS-Konzept entsteht erst durch die Tatsache, dass die verfügbare Bandbreite nicht immer ausreicht, um alle anstehenden Datenpakete zuverlässig und rechtzeitig zu übertragen. Werden über die Datenleitung gleichzeitig große FTP-Downloads gefahren, E-Mails ausgetauscht und IP-Telefone verwendet, kommt es sehr schnell zu Belastungsspitzen. Um auch in diesen Situationen die Anforderungen an die gewünschte Datenübertragung sicher zu stellen, müssen bestimmte Datenpakete bevorzugt behandelt werden. Dazu muss ein Gerät zunächst einmal erkennen, welche Datenpakete denn überhaupt bevorzugt werden sollen.

Es gibt zwei Möglichkeiten, den Bedarf für eine bevorzugte Behandlung von Datenpaketen im Gerät zu signalisieren:

- Die Applikation, wie z. B. die Software von einigen IP-Telefonen, kann die Datenpakete selbst entsprechend kennzeichnen. Diese Kennzeichnung, das “Tag”, wird in den Header der IP-Pakete eingefügt. Die beiden verschiedenen Varianten dieser Kennzeichnung “ToS” und “DiffServ” können vereinfacht dargestellt folgende Zustände annehmen:

- ToS “Low Delay“
- ToS “High Reliability“
- DiffServ “Expedited Forwarding“
- DiffServ “Assured Forwarding“

Hinweis: Die IP-Header-Bits des ToS- bzw. DiffServ-Feldes werden im Falle einer VPN-Strecke auch in den umgebenden IP-Header des IPSec-VPN-Paketes kopiert. Somit steht QoS auch für VPN-Strecken über das Internet zur Verfügung, sofern der Provider entsprechende Pakete auch im WAN bevorzugt behandelt.

- Wenn die Applikation selbst nicht die Möglichkeit hat, die Datenpakete entsprechend zu kennzeichnen, kann das Gerät für die richtige Behandlung sorgen. Dazu werden die vorhandenen Funktionen der Firewall genutzt, die Datenpakete z. B. nach Subnetzen oder Diensten (Anwendungen) klassifizieren kann. Mit diesen Funktionen ist es z. B. möglich, die Datenpakete einer FTP-Verbindung oder die einer bestimmten Abteilung (in einem separaten Subnetz) gesondert zu behandeln.

  Für die Behandlung von Datenpaketen, die über die Firewall klassifiziert werden, stehen die beiden folgenden Möglichkeiten zur Auswahl:

  - Garantierte Mindestbandbreite
  - Limitierte Maximalbandbreite

9.2.1 Was ist DiffServ?

DiffServ steht für “Differentiated Services” und stellt ein relativ neues Modell dar, die Priorität der Datenpakete zu signalisieren. DiffServ basiert auf dem bekannten Type-of-Service(ToS)-Feld und nutzt das gleiche Byte im IP-Header.

ToS verwendet die ersten drei Bits zur Kennzeichnung der Prioritäten (Precedence) 0 bis 7 und vier weitere Bits (die ToS-Bits) zur Optimierung des Datenflusses (u.a. “Low Delay” und “High Reliability”). Dieses Modell ist recht unflexibel und wurde daher in der Vergangenheit eher selten verwendet.

Das DiffServ-Modell nutzt die ersten 6 Bits zur Unterscheidung verschiedener Klassen. Damit sind bis zu 64 Abstufungen (Differentiated Services Code Point, DSCP) möglich, die eine feinere Priorisierung des Datenflusses ermöglichen:

- Um die Abwärtskompatibilität zur ToS-Implementation sicherzustellen, können mit den “Class Selectors” (CS0 bis CS7) die bisherigen Precedence-Stufen abgebildet werden. Die Stufe “CS0” wird dabei auch als “Best Effort” (BE) bezeichnet und steht für die normale Übertragung der Datenpakete ohne besondere Behandlung.
- Die “Assured Forwarding”-Klassen werden für die gesicherte Übertragung von Datenpaketen eingesetzt. Die erste Ziffer der AF-Klasse steht jeweils für die Priorität der Übertragung (1 bis 4), die zweite Ziffer für “Drop-Wahrscheinlichkeit” (1 bis 3). Pakete mit AFxx-Kennzeichnung werden “gesichert” übertragen, also nicht verworfen.

Mit der Klasse “Expedited Forwarding” schließlich werden die Pakete markiert, die vor allen anderen Paketen (bevorzugt) übertragen werden sollen.

Codepoint	*DSCP Bits*	*Dez.*	*Codepoint*	*DSCP Bits*	*Dez.*	*Codepoint*	*DSCP Bits*	*Dez.*
CS0 (BE)	000000	0	AF11	001010	10	AF33	011110	30
CS1	001000	8	AF12	001100	12	AF41	100010	34
CS2	010000	16	AF13	001110	14	AF42	100100	36
CS3	011000	24	AF21	010010	18	AF43	100110	38
CS4	100000	32	AF22	010100	20	EF	101110	46
CS5	101000	40	AF23	010110	22			
CS6	110000	48	AF31	011010	26			
CS7	111000	56	AF32	011100	28			

9.2.2 Garantierte Mindestbandbreiten

Hiermit geben Sie Vorfahrt für sehr wichtige Applikationenoder bestimmte Benutzergruppen.

Volldynamisches Bandbreitenmanagement beim Senden

Das Bandbreitenmanagement erfolgt in Senderichtung dynamisch. Dies bedeutet, dass z. B. eine garantierte Mindestbandbreite nur solange zur Verfügung gestellt wird, wie auch tatsächlich entsprechender Datentransfer anliegt.

Hinweis: Für das korrekte Funktionieren dieses Mechanismus darf die Summe der konfigurierten Mindestbandbreiten die effektiv zur Verfügung stehende Sendebandbreite nicht übersteigen.

Dynamisches Bandbreitenmanagement auch beim Empfang

Zur empfangsseitigen Bandbreitensteuerung können Pakete zwischengespeichert und erst verzögert bestätigt werden. Dadurch regeln sich TCP/IP-Verbindungen selbständig auf eine geringere Bandbreite ein.

Jedem WAN-Interface ist eine maximale Empfangsbandbreite zugeordnet. Diese Bandbreite wird durch jede QoS-Regel, die eine minimale Empfangsbandbreite auf diesem Interface garantiert, entsprechend reduziert.

- Ist die QoS-Regel verbindungsbezogen definiert, wird die reservierte Bandbreite direkt nach dem Beenden der Verbindung wieder freigegeben, und die maximal auf dem WAN-Interface verfügbare Bandbreite steigt entsprechend an.
- Ist die QoS-Regel global definiert, wird die reservierte Bandbreite erst nach dem Beenden der letzten Verbindung wieder freigegeben.

9.2.3 Limitierte Maximalbandbreiten

Hiermit schränken Sie z. B. die gesamte oder verbindungsbezogene Maximalbandbreite für Serverzugriffe ein.

Ein Beispiel:

Sie betreiben einen Webserver und ein lokales Netzwerk an einem gemeinsamen Internetzugang.

Um zu verhindern, dass Ihr Produktivnetz (LAN) von vielen Internetzugriffen auf Ihren Webserver lahmgelegt wird, limitieren Sie alle Serverzugriffe auf die Hälfte der Ihnen zur Verfügung stehenden Bandbreite. Um ferner sicherzustellen, dass Ihre Serverdienste vielen Usern gleichzeitig und gleichberechtigt zugute kommen, setzen Sie pro Verbindung zum Server eine bestimmte Maximalbandbreite.

Kombination möglich

Minimal- und Maximalbandbreiten können kombiniert zusammen verwendet werden. Somit kann die zur Verfügung stehende Bandbreite speziell nach Ihren Erfordernissen z. B. auf bestimmte Benutzergruppen oder Anwendungen verteilt werden.

9.3 Das Warteschlangenkonzept

9.3.1 Sendeseitige Warteschlangen

Die Anforderungen an die Dienstgüte werden im HiLCOS durch den Einsatz mehrerer Warteschlangen (Queues) für die Datenpakete realisiert. Auf der Sendeseite kommen folgende Queues zum Einsatz:

- Urgent-Queue I

  Diese Queue wird immer vor allen anderen abgearbeitet. Hier landen folgende Datenpakete:

  - Pakete mit ToS “Low Delay“
  - Pakete mit DiffServ “Expedited Forwarding“
  - Alle Pakete, denen eine bestimme Mindestbandbreite zugewiesen wurde, solange die garantierte Minimalbandbreite nicht überschritten wird
  - TCP-Steuerungspakete können ebenfalls durch diese Queue bevorzugt versendet werden

- Urgent Queue II

  Hier landen alle Pakete, die eine garantierte Mindestbandbreite zugewiesen bekommen haben, deren Verbindung diese aber überschritten hat.

  Solange das Intervall für die Mindestbandbreite läuft (z. B. bis zum Ende der laufenden Sekunde) werden alle Pakete in dieser Queue ohne weitere besondere Priorität behandelt. Alle Pakete in dieser Queue, der “gesicherten Queue” und der “Standard-Queue” teilen sich von nun an die vorhandene Bandbreite. Die Pakete werden beim Senden in der Reihenfolge aus den Queues geholt, in der sie auch in die Queues gestellt wurden. Läuft

das Intervall ab, werden alle Blöcke, die sich zu diesem Zeitpunkt noch in der “Urgent-Queue II” befinden, bis zum Überschreiten der jeweils zugeteilten Mindestbandbreite wieder in die “Urgent-Queue I” gestellt, der Rest verbleibt in der “Urgent-Queue II”.

Mit diesem Verfahren wird sichergestellt, dass priorisierte Verbindungen den restlichen Datenverkehr nicht erdrücken.

- gesicherte Queue

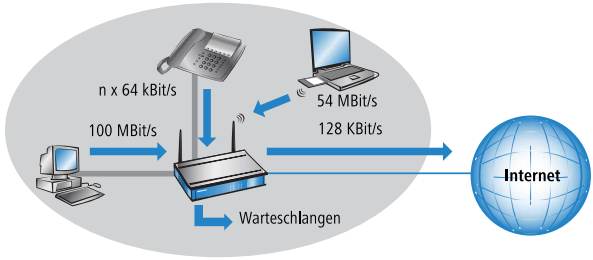
  Diese Warteschlange hat keine gesonderte Priorität. Jedoch werden Pakete in dieser Queue niemals verworfen (garantierte Übertragung). Hier landen folgende Datenpakete:

  - Pakete mit ToS “High Reliability“
  - Pakete mit DiffServ “Assured Forwarding

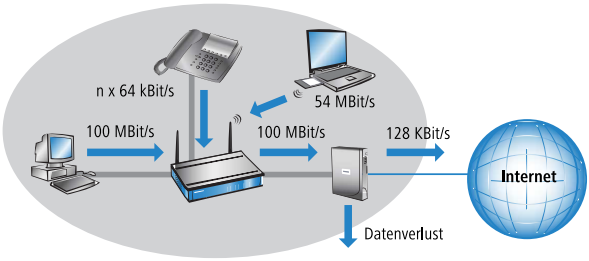
- Standard-Queue

  Die Standard-Warteschlange enthält alle nicht klassifizierten Datenpakete. Pakete in dieser Queue werden zuerst verworfen, sofern die Datenpakete nicht schnell genug abgeliefert werden können.

  Das Konzept der Warteschlangen funktioniert natürlich nur, wenn sich an der Schnittstelle vom LAN zum WAN ein Stau von Datenpaketen bildet. Dieser Stau bildet sich dann, wenn das Interface im Gerät weniger Daten an das WAN abgeben kann, als aus dem LAN in den Spitzenzeiten angeliefert werden. Das ist z. B. dann der Fall, wenn die Schnittstelle zum WAN ein integriertes ADSL Interface mit vergleichsweiser geringer Sendegeschwindigkeit (Upstream) ist. Das integrierte ADSL-Modem meldet selbständig an das Gerät zurück, wie viele Datenpakete es noch aufnehmen kann und bremst so den Datenfluss schon im Router. Dabei werden dann automatisch die Warteschlangen gefüllt.



Anders sieht das aus, wenn ein Ethernet-Interface die Verbindung ins WAN darstellt. Aus Sicht des Geräts sieht die Verbindung ins Internet über das ein externes DSL-Modem wie ein Ethernet-Abschnitt aus. Auf der Strecke vom Gerät zum DSL-Modem werden die Daten auch mit der vollen LAN-Geschwindigkeit von 10 oder 100 MBit/s übertragen. Hier bildet sich also kein natürlicher Stau, da die Ein- und Ausgangsgeschwindigkeiten gleich sind. Außerdem meldet das Ethernet zwischen Gerät und DSL-Modem nichts über die Kapazität der Verbindung zurück. Die Folge: erst im DSL-Modem kommt es zum Stau. Da hier keine Warteschlangen mehr vorhanden sind, gehen die überschüssigen Daten verloren. Eine Priorisierung der “bevorzugten” Daten ist also nicht möglich



Um dieses Problem zu lösen, wird die Übertragungsrate des WAN-Interfaces im Gerät künstlich gedrosselt. Die Schnittstelle wird dabei auf die Übertragungsrate eingestellt, die für den Transport der Daten ins WAN zur Verfügung stehen. Bei einem Standard-DSL-Anschluss wird also das DSL-Interface im Gerät auf die entsprechende Upstreamrate (128 KBit/s) eingestellt.

Tipp: Bei der von den Providern angegebenen Datenraten handelt es sich meistens um die Nettodatenrate. Die für das Interface nutzbare Bruttodatenrate liegt etwas höher als die vom Provider garantierte Nettodatenrate. Wenn Sie die Bruttodatenrate Ihres Providers kennen, können Sie diesen Wert für das Interface eintragen und damit den Datendurchsatz leicht steigern. Mit der Angabe der Nettodatenrate sind Sie aber auf jeden Fall auf der sicheren Seite!

9.3.2 Empfangsseitige Warteschlangen

Neben der Übertragungsrate in Senderichtung gilt die gleiche Überlegung auch für die Empfangsrichtung. Hier bekommt das WAN-Interface des Geräts vom DSL-Modem deutlich weniger Daten angeliefert, als eigentlich aufgrund des 10 oder 100 MBit Ethernet-Interfaces möglich wäre. Alle auf dem WAN-Interface empfangenen Datenpakete werden gleichberechtigt in das LAN übertragen.

Um die eingehenden Daten priorisieren zu können, muss also auch in dieser Richtung eine künstliche “Bremse” eingeschaltet werden. Wie schon bei der Senderichtung wird daher die Übertragungsrate der Schnittstelle in Empfangsrichtung an das Angebot des Providers angepasst, für einen Standard-DSL-Anschluss also z. B. auf eine Downstreamrate von 768 KBit/s. Auch hier kann wie bei der Upstreamrate die Bruttodatenrate eingetragen werden, wenn bekannt.

Das Reduzieren der Empfangsbandbreite macht es nun möglich, die empfangenen Datenpakete angemessen zu behandeln. Die bevorzugten Datenpakete werden bis zur garantierten Mindestbandbreite direkt in das LAN weitergegeben, die restlichen Datenpakete laufen in einen Stau. Dieser Stau führt in der Regel zu einer verzögerten Bestätigung der Pakete. Bei einer TCP-Verbindung wird der sendende Server auf diese Verzögerungen reagieren, seine Sendefrequenz herabsetzen und sich so der verfügbaren Bandbreite anpassen.

Auf der Empfangsseite kommen folgende Queues zum Einsatz:

- Deferred Acknowledge Queue

  Jedes WAN-Interface erhält zusätzlich eine QoS-Empfangsqueue, welche die Pakete aufnimmt, die “ausgebremst” werden sollen. Die Verweildauer jedes einzelnen Pakets richtet sich nach der Länge des Pakets und der aktuell zulässigen Empfangsbandbreite. Pakete, für die über eine QoS-Regel eine empfangsseitige Mindestbandbreite definiert ist, werden ungebremst durchgelassen, solange die Mindestbandbreite nicht überschritten wurde.

- normale Empfangsqueue

  Hier landen alle Pakete, die nicht aufgrund einer empfangsseitig aktiven QoS-Regel gesondert behandelt werden müssen. Pakete in dieser Queue werden direkt weitergeleitet bzw. bestätigt, ohne Maximalbandbreiten zu berücksichtigen.

9.4 QoS in Sende- oder Empfangsrichtung

Bei der Steuerung der Datenübertragung mit Hilfe der QoS kann man auswählen, ob die entsprechende Regel für die Sende- oder Empfangsrichtung gilt. Welche Richtung bei einer konkreten Datenübertragung jetzt aber Sende- und welche Empfangsrichtung ist, hängt vom Blickwinkel der Betrachtung ab. Es gibt dabei die beiden folgenden Varianten:

- Die Richtung entspricht dem logischen Verbindungsaufbau
- Die Richtung entspricht der physikalischen Datenübertragung über das jeweilige Interface

Die Betrachtung eines FTP-Transfers macht die Unterschiede deutlich. Ein Client im LAN ist über ein Gerät mit dem Internet verbunden.

- Bei einer aktiven FTP-Session sendet der Client dem Server über den PORT-Befehl die Informationen, auf welchem Port er die DATA-Verbindung erwartet. Der Server baut daraufhin die Verbindung zum Client auf und sendet in der gleichen Richtung die Daten. Hier gehen also sowohl die logische Verbindung als auch der tatsächliche Datenstrom über das Interface vom Server zum Client, das Gerät wertet beides als Empfangsrichtung.
- Anders sieht es aus bei einer passiven FTP-Session. Dabei baut der Client selbst die Verbindung zum Server auf. Der logische Verbindungsaufbau geht hierbei also vom Client in Richtung Server, die Datenübertragung über das physikalische Interface jedoch in umgekehrter Richtung vom Server zum Client.

In der Standardeinstellung bewertet ein Gerät die Sende- oder Empfangsrichtung anhand des logischen Verbindungsaufbaus. Weil diese Sichtweise in manchen Anwendungsszenarien nicht einfach zu durchschauen ist, kann der Blickwinkel alternativ auf die Betrachtung des physikalischen Datenstroms umgestellt werden.

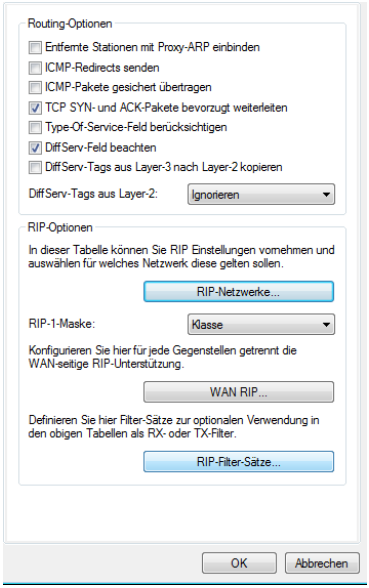
Hinweis: Die Unterscheidung von Sende- und Empfangsrichtung gilt nur für die Einrichtung von Maximalbandbreiten. Bei einer garantierten Mindestbandbreite sowie bei Fragmentierung und PMTU-Reduzierung gilt immer die physikalische Datenübertragung über das jeweilige Interface als Richtung!

9.5 QoS-Konfiguration

9.5.1 ToS- und DiffServ-Felder auswerten

ToS- oder DiffServ?

Wählen Sie bei der Konfiguration mit LANconfig den Konfigurationsbereich 'IP-Router'. Auf der Registerkarte 'Allgemein' wird eingestellt, ob das 'Type-of-Service-Feld' oder alternativ das 'DiffServ-Feld' bei der Priorisierung der Datenpakete berücksichtigt wird. Werden beide Optionen ausgeschaltet, wird das ToS/DiffServ-Feld ignoriert.



Bei der Konfiguration mit WEBconfig oder Telnet wird die Entscheidung für die Auswertung der ToS- oder DiffServ-Felder an folgenden Stellen eingetragen:

Konfigurationstool	*Aufruf*
WEBconfig	Setup/IP-Router/Routing-Methode

Konfigurationstool	*Aufruf*
Telnet	Setup/IP-Router/Routing-Methode

Die Einstellmöglichkeiten des Wertes Routing-Methode sind folgende:

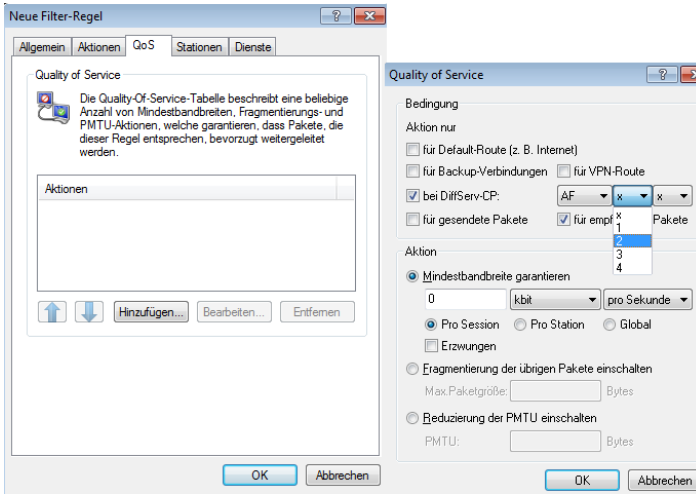
- **Normal**: Das ToS/DiffServ-Feld wird ignoriert.
- **TOS**: Das ToS/DiffServ-Feld wird als ToS-Feld betrachtet, es werden die Bits “Low-Delay” und “High-Reliability” ausgewertet.
- **DiffServ**: Das ToS/DiffServ-Feld wird als DiffServ-Feld betrachtet und wie folgt ausgewertet:

DSCP Codepoints	*Übertragungsweise*
CSx (inklusive CS0 = BE)	normal übertragen
AFxx	gesichert übertragen
EF	bevorzugt übertragen

DiffServ in den Firewall-Regeln

In den Firewallregeln können die Code Points aus dem DiffServ-Feld ausgewertet werden, um weitere QoS-Parameter wie Mindestbandbreiten oder PMTU-Reduzierung zu steuern.

Die Parameter für die Auswertung der DiffServ-Felder werden im LANconfig beim Definieren der QoS-Regel festgelegt:



Je nach Auswahl des DSCP-Typs (BE, CS, AF, EF) können in zusätzlichen Drop-Down-Listen die gültigen Werte eingestellt werden. Alternativ kann auch der DSCP-Dezimalwert direkt eingetragen werden. Eine Tabelle mit den gültigen Werten findet sich unter *Was ist DiffServ?* auf Seite 775.

Bei der Konfiguration mit WEBconfig oder Telnet werden diese Parameter an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	***Aufruf***
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Die Regel in der Firewall wird dabei um die Bedingung “@d” und den DSCP (Differentiated Services Code Point) erweitert. Der Code Point kann entweder über seinen Namen (CS0 - CS7, AF11 bis AF 43, EF oder BE) oder seine dezimale bzw. hexadezimale Darstellung angegeben werden. “Expedited Forwarding” kann somit als “@dEF”, “@d46” oder “@d0x2e” angegeben werden. Desweiteren sind Sammelnamen (CSx bzw. AFxx) möglich.

Beispiele:

- **%Lcds0 @dAFxx %A**: Akzeptieren (gesichert Übertragen) bei DiffServ “AF”, Limit “0”
- **%Qcds32 @dEF**: Mindestbandbreite für DiffServ “EF” von 32 kBit/s

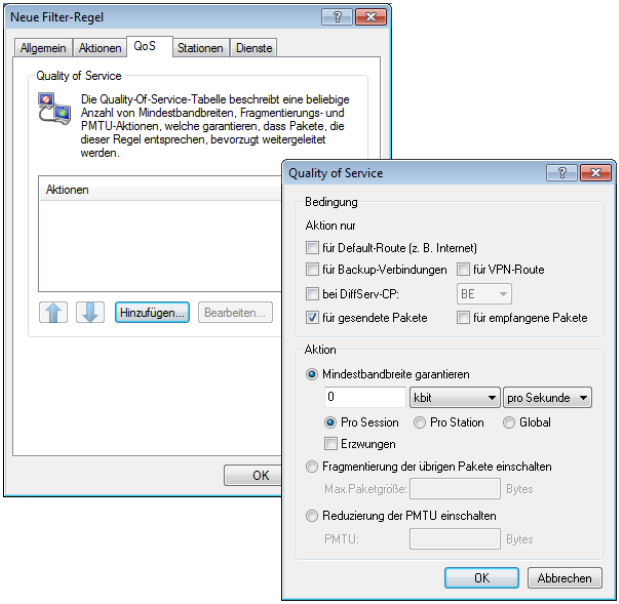
- **%Fprw256 @dEF**: PMTU-Reduzierung beim Empfang für DiffServ “EF” auf 256 Bytes)

Mit den hier aufgeführten Beispielen kann man für Voice-over-IP-Telefonate die gewünschte Bandbreite freihalten. Der erste Baustein “%Lcds0 @dAFxx %A“ akzeptiert die mit dem DSCP “AFxx” markierten Pakete zur Signalisierung eines Anrufs. Die mit “EF” gekennzeichneten Sprachdaten werden durch den Eintrag “%Qcds32 @dEF“ priorisiert übertragen, dabei wird eine Bandbreite von 32 KBit/s garantiert. Parallel dazu wird mit “%Fprw256 @dEF“ die PMTU auf 256 Byte festgelegt, was eine Sicherung der erforderlichen Bandbreite in Empfangsrichtung erst möglich macht.

9.5.2 Minimal- und Maximalbandbreiten definieren

Eine Mindestbandbreite für eine bestimmte Anwendung wird im LANconfig über eine Firewallregel nach den folgenden Randbedingungen definiert:

- Die Regel benötigt keine Aktion, da für die QoS-Regeln immer implizit das “Übertragen” als Aktion vorausgesetzt wird.
- Auf der Registerkarte 'QoS' wird die garantierte Bandbreite festgelegt.



- Mit der Option 'Aktion nur für Default-Route' beschränkt man die Regel auf Pakete, die über die Defaultroute gesendet oder empfangen werden.
  - Mit der Option 'Aktion nur für VPN-Route' beschränkt man die Regel auf Pakete, die über einen VPN-Tunnel gesendet oder empfangen werden.
  - Mit der Option 'Erzwungen' wird eine statische Bandbreitenreservierung definiert. Die so reservierte Bandbreite bleibt für alle anderen Verbindungen auch dann gesperrt, wenn die bevorzugte Verbindung die Bandbreite zur Zeit nicht in Anspruch nimmt.
  - Mit der Option 'Pro Verbindung' bzw. 'Global' wird festgelegt, ob die hier eingestellte Mindestbandbreite für jede einzelne Verbindung gilt, die dieser Regel entspricht (Pro Verbindung), oder ob es sich dabei um die Obergrenze für die Summe aller Verbindungen gemeinsam handelt (Global).
- Auf den Registerkarten 'Stationen' und 'Dienste' wird wie bei anderen Firewallregeln vereinbart, für welche Stationen im LAN / WAN und für welche Protokolle diese Regel gilt.

Bei der Konfiguration mit WEBconfig oder Telnet werden die Minimal- bzw. Maximalbandbreiten an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	*Aufruf*
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Eine geforderte Mindestbandbreite wird in den Regeln mit dem Bezeichner “%Q” eingeleitet. Dabei wird implizit angenommen, dass es sich bei der entsprechenden Regel um eine “Accept”-Aktion handelt, die Pakete also übertragen werden.

Für eine Maximalbandbreite wird eine einfache Limit-Regel definiert, die mit einer “Drop”-Aktion alle Pakete verwirft, die über die eingestellte Bandbreite hinausgehen.

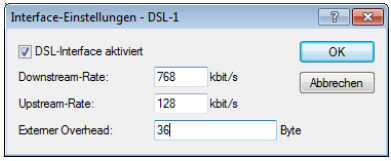
Beispiele:

- **%Qcds32**: Mindestbandbreite von 32 kBit/s für jede Verbindung
- **%Lgds256 %d**: Maximalbandbreite von 256 kBit/s für alle Verbindungen (global)

9.5.3 Übertragungsraten für Interfaces festlegen

Hinweis: Geräte mit eingebautem ADSL/SDSL-Modem bzw. mit ISDN-Adapter nehmen diese Einstellungen für das jeweilige Interface selbständig vor. Bei einem Modell mit DSL- **und** ISDN-Interface wird diese Einstellung also nur für das Ethernet-Interface vorgenommen.

Die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL-Interfaces werden im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' bei den Einstellungen für die verschiedenen WAN-Interfaces festgelegt:



- Ein DSL-Interface kann in diesem Dialog vollständig ausgeschaltet werden.
- Als Upstream- und Downstream-Rate werden hier die Bruttodatenraten angegeben, die üblicherweise etwas über den Nettodatenraten liegen, die der Provider als garantierte Datenrate angibt (siehe auch *Das Warteschlangenkonzept* auf Seite 778).
- Der “externe Overhead” berücksichtigt Informationen, die bei der Datenübertragung den Paketen zusätzlich angehängt werden. Bei Anwendungen mit eher kleinen Datenpaketen (z. B. Voice-over-IP) macht sich diese Extra-Overhead durchaus bemerkbar. Beispiele für den externen Overhead:

Übertragung	*externer Overhead*	*Bemerkung*
T-DSL	36 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
PPTP	24 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (LLC)	22 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
IPoA (VC-MUX)	18 Bytes	zusätzliche Header, Verluste durch nicht vollständig genutzte ATM-Zellen
Kabelmodem	0	direkte Übertragung von Ethernet-Paketen

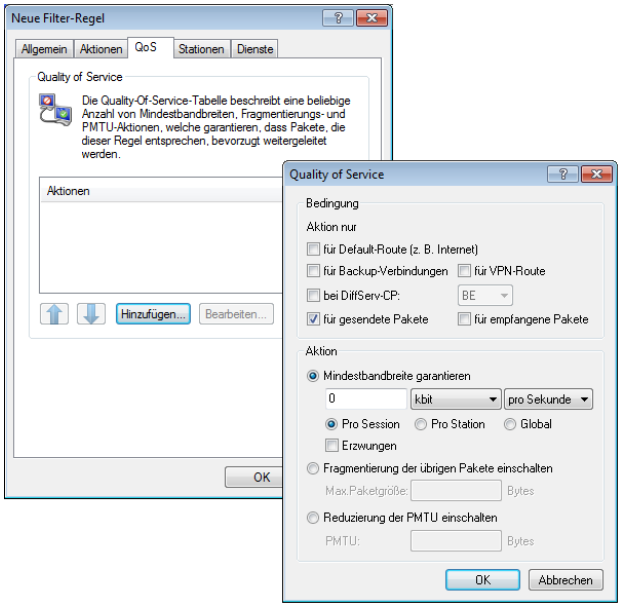
Unter WEBconfig oder Telnet können die Beschränkungen der Datenübertragungsrate für Ethernet-, DSL und DSLoL-Interfaces an folgender Stelle eingetragen werden:

Konfigurationstool	*Aufruf*
WEBconfig	Setup/Schnittstellen/DSL-Schnittstellen
Telnet	Setup/Schnittstellen/DSL-Schnittstellen

Hinweis: Die Werte für die Upstream-Rate und die Downstream-Rate werden in KBit/s angegeben, die Werte für den externen Overhead in Bytes/Paket.

9.5.4 Sende- und Empfangsrichtung

Die Bedeutung der Datenübertragungsrichtung wird im LANconfig beim Definieren der QoS-Regel festgelegt:



Bei der Konfiguration mit WEBconfig oder Telnet wird die Bedeutung der Datenübertragungsrichtung über die Parameter “R” für receive (Empfangen),

“T” für transmit (Senden) und “W” für den Bezug zum WAN-Interface an folgenden Stellen in eine neue Regel der Firewall eingetragen:

Konfigurationstool	*Aufruf*
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Die Beschränkung der Datenübertragung auf 16 KBit/s in Senderichtung bezogen auf das physikalische WAN-Interface wird also z. B. durch die folgende Regel in der Firewall erreicht:

- %Lcdstw16%d

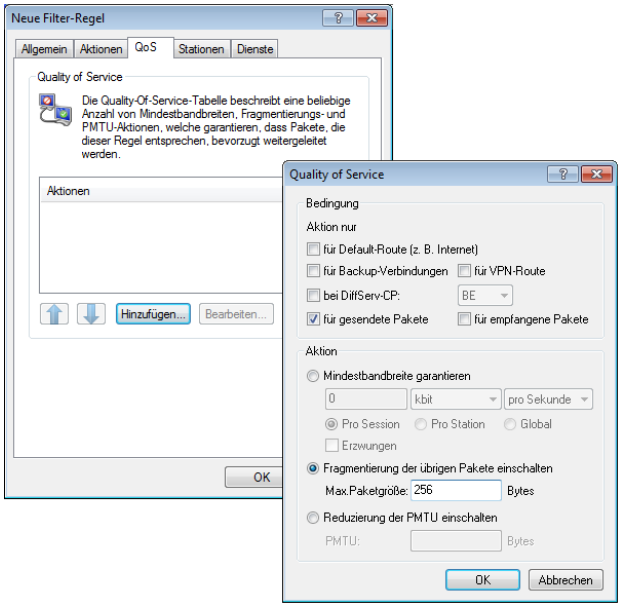
9.5.5 Reduzierung der Paketlänge

Die Längenreduzierung der Datenpakete wird definiert über eine Regel in der Firewall nach den folgenden Randbedingungen:

- Die Reduzierung bezieht sich auf **alle** Pakete, die auf das Interface gesendet werden und **nicht** der Regel entsprechen.
- Es werden nicht bestimmte Protokolle reduziert, sondern global alle Pakete auf dem Interface.

Bei Geräten mit integrierter oder nachträglich über Software-Option freigeschalteter VoIP-Funktion können Fragmentierung und PMTU-Reduzierung separat für SIP-Gespräche eingestellt werden!

Die Längenreduzierung der Datenpakete wird im LANconfig beim Definieren der QoS-Regel festgelegt:



Bei der Konfiguration mit WEBconfig oder Telnet wird die Reduzierung über die Parameter “P” für die Reduzierung der PMTU (Path MTU, MTU = Maximum Transmission Unit) und “F” für die Größe der Fragmente an folgenden Stellen in eine neue Firewallregel eingetragen:

Konfigurationstool	***Aufruf***
WEBconfig	Setup/IP-Router/Firewall/Regelliste
Telnet	Setup/IP-Router/Firewall/Regel-Liste

Hinweis: PMTU-Reduzierung und Fragmentierung beziehen sich immer auf die physikalische Verbindung. Die Angabe des Parameters “W” für die WAN-Senderichtung ist also hier nicht erforderlich und wird ignoriert, falls vorhanden.

Das folgende Beispiel zeigt eine Einstellung für Voice-over-IP-Telefonie:

Regel	***Quelle***	***Ziel***	***Aktion***	***Protokoll***
VOIP	IP-Adressen der IP-Telefone im LAN, alle Ports	IP-Adressen der IP-Telefone im LAN, alle Ports	%Qcds32 %Prt256	UDP

Diese Regel setzt die Mindestbandbreite für Senden und Empfang auf 32 KBit/s, erzwingt und verringert die PMTU beim Senden und Empfang auf 256 Byte große Pakete. Für die TCP-Verbindungen wird die Maximum Segment Size des lokalen Rechners auf 216 gesetzt, damit der Server maximal 256 Bytes große Pakete sendet (Verringerung der PMTU in Sende- und Empfangsrichtung).

9.6 QoS für WLANs nach IEEE 802.11e (WMM/WME)

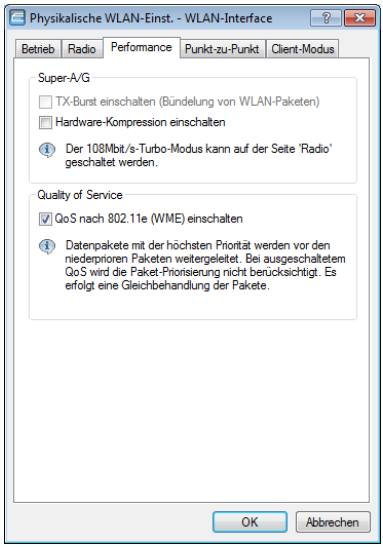
Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienstgüten angeboten werden (Quality of Service). 802.11e unterstützt u.a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voice over WLAN – VoWLAN).

Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM (Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier Kategorien (Sprache, Video, Best Effort und Hintergrund), die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden.

Der 802.11e-Standard nutzt zur Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

Hinweis: Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der Access Point den 802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechenden Prioritäten kennzeichnen.

Die Verwendung von 802.11e kann in einem Access Point für jedes physikalische WLAN-Netzwerk getrennt aktiviert werden.



Konfigurationstool	***Aufruf***
LANconfig	Wireless LAN / Physikalische WLAN-Einstellungen / Performance
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Schnittstellen > WLAN > Leistung

10 Virtual Private Networks - VPN

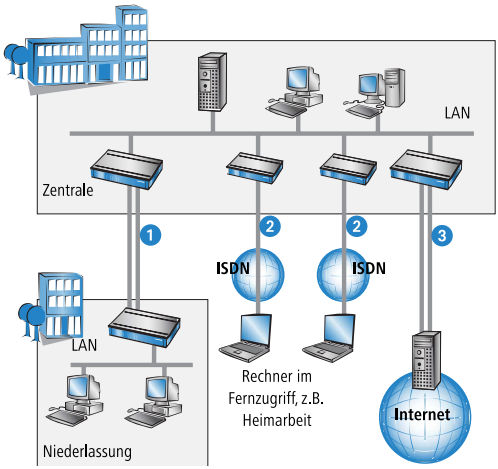
10.1 Welchen Nutzen bietet VPN?

Mit einem VPN (**V**irtual **P**rivate **N**etwork) können sichere Datenverkehrsverbindungen über kostengünstige, öffentliche IP-Netze aufgebaut werden, beispielsweise über das Internet.

Was sich zunächst unspektakulär anhört, hat in der Praxis enorme Auswirkungen. Zur Verdeutlichung schauen wir uns zunächst ein typisches Unternehmensnetzwerk ohne VPN-Technik an. Im zweiten Schritt werden wir dann sehen, wie sich dieses Netzwerk durch den Einsatz von VPN optimieren lässt.

10.1.1 Herkömmliche Netzwerkstruktur

Blicken wir zunächst auf eine typische Netzwerkstruktur, die in dieser oder ähnlicher Form in vielen Unternehmen anzutreffen ist:



Das Unternehmensnetz basiert auf einem internen Netzwerk (LAN) in der Zentrale. Dieses LAN ist über folgende Wege mit der Außenwelt verbunden:

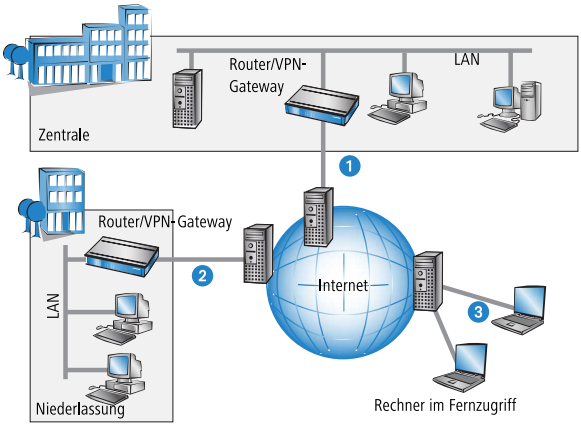
1. Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
2. Rechner wählen sich über ISDN oder Modem ins zentrale Netzwerk ein (Remote Access Service – RAS).
3. Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit zum Versand und Empfang von E-Mails zu geben.

Alle Verbindungen zur Außenwelt basieren auf dedizierten Leitungen, d. h. Wähl- oder Standleitungen. Dedizierte Leitungen gelten einerseits als zuverlässig und sicher, andererseits aber auch als teuer. Ihre Kosten sind in aller Regel von der Verbindungsdistanz abhängig. So hat es gerade bei Verbindungen über weite Strecken Sinn, nach preisgünstigeren Alternativen Ausschau zu halten.

In der Zentrale muss für jeden verwendeten Zugangs- und Verbindungsweg (analoge Wählverbindung, ISDN, Standleitungen) entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

10.1.2 Vernetzung über Internet

Bei Nutzung des Internets anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teueren dedizierten Leitungen zwischen den Teilnehmern mehr.

1. Nur noch die Internet-Verbindung des LANs der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.
2. Die Niederlassung ist ebenfalls mit einer eigenen Verbindung ans Internet angeschlossen.
3. Die RAS-Rechner wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber herkömmlichen Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selber nur einen Zugang ins Internet. Die Zugangstechnologie spielt dabei keine Rolle: Idealerweise kommen Breitbandtechnologien wie DSL (Digital Subscriber Line) in Verbindung mit Flatrates zum Einsatz. Aber auch herkömmliche ISDN-Verbindungen können verwendet werden.

Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

Niedrige Verbindungskosten und hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Übertragungsmedium für ein Unternehmensnetzwerk.

Zwei technische Eigenschaften des IP-Standards stehen allerdings der Nutzung des Internets als Teil von Unternehmensnetzwerken entgegen:

- Die Notwendigkeit öffentlicher IP-Adressen für alle Teilnehmer
- Fehlende Datensicherheit durch ungeschützte Datenübertragung

10.1.3 Private IP-Adressen im Internet?

Der IP-Standard definiert zwei Arten von IP-Adressen: öffentliche und private. Eine öffentliche IP-Adresse hat weltweite Gültigkeit, während eine private IP-Adresse nur in einem abgeschotteten LAN gilt.

Öffentliche IP-Adressen müssen weltweit eindeutig und daher einmalig sein. Private IP-Adressen dürfen weltweit beliebig häufig vorkommen, innerhalb eines abgeschotteten Netzwerkes jedoch nur einmal.

Normalerweise haben Rechner im LAN nur private IP-Adressen, lediglich der Router mit Anschluss ans Internet verfügt auch über eine öffentliche IP-Adresse. Die Rechner hinter diesem Router greifen über dessen öffentliche IP-Adresse auf das Internet zu (IP-Masquerading). In einem solchen Fall ist nur der Router selber über das Internet ansprechbar. Rechner hinter dem Router sind aus dem Internet heraus ohne Vermittlung durch den Router nicht ansprechbar.

Routing auf IP-Ebene mit VPN

Soll das Internet zur Kopplung von Netzwerken eingesetzt werden, müssen deshalb IP-Strecken zwischen Routern mit jeweils öffentlicher IP-Adresse eingerichtet werden. Diese Router stellen die Verbindung zwischen mehreren Teilnetzen her. Schickt ein Rechner ein Paket an eine private IP-Adresse in einem entfernten Netzwerksegment, dann setzt der eigene Router dieses Paket über das Internet an den Router des entfernten Netzwerksegments ab.

Das „Einpacken“ der Datenpakete mit privaten IP-Adressen in Pakete mit öffentlichen IP-Adressen übernimmt das VPN-Gateway. Ohne VPN können Rechner ohne eigene öffentliche IP-Adresse nicht über das Internet miteinander kommunizieren.

10.1.4 Sicherheit des Datenverkehrs im Internet?

Es existiert Skepsis gegenüber der Idee, Teile der Unternehmenskommunikation über das Internet abzuwickeln. Der Grund für die Skepsis ist die Tatsache, dass sich das Internet dem direkten Einflussbereich des Unternehmens entzieht. Anders als bei dedizierten Verbindungen laufen die Daten durch fremde Netzstrukturen, deren Eigentümer dem Unternehmen häufig unbekannt sind.

Das Internet basiert außerdem nur auf einer simplen Form der Datenübertragung in Form unverschlüsselter Datenpakete. Dritte, durch deren Netze diese Pakete laufen, können sie mitlesen und möglicherweise sogar manipulieren. Der Zugang zum Internet ist für jedermann möglich. Dadurch ergibt sich die Gefahr, dass sich auch Dritte unbefugt Zugang zu den übertragenen Daten verschaffen.

VPN – Sicherheit durch Verschlüsselung

Zur Lösung dieses Sicherheitsproblems wird der Datenverkehr zwischen zwei Teilnehmern im VPN verschlüsselt. Während der Übermittlung sind die Daten für Dritte unlesbar.

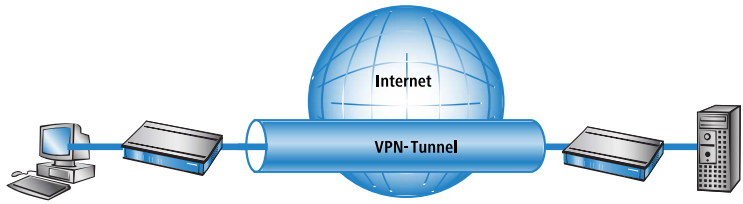
Für die Verschlüsselung kommen die modernsten und sichersten Kryptografieverfahren zum Einsatz. Aus diesem Grund übertrifft die Übertragungssicherheit im VPN das Sicherheitsniveau dedizierter Leitungen bei weitem.

Für die Datenverschlüsselung werden Codes zwischen den Teilnehmern vereinbart, die man üblicherweise als „Schlüssel“ bezeichnet. Diese Schlüssel kennen nur die Beteiligten im VPN. Ohne gültigen Schlüssel können Datenpakete nicht entschlüsselt werden. Die Daten bleiben Dritten unzugänglich, sie bleiben „privat“.

Schicken Sie Ihre Daten in den Tunnel – zur Sicherheit

Jetzt wird auch klar, warum VPN ein virtuelles privates Netz aufbaut: Es wird zu keinem Zeitpunkt eine feste, physikalische Verbindung zwischen den Geräten aufgebaut. Die Daten fließen vielmehr über geeignete Routen durchs Internet. Dennoch ist es unbedenklich, wenn Dritte die übertragenen Daten während der Übertragung abfangen und aufzeichnen. Da die Daten durch VPN verschlüsselt sind, bleibt ihr eigentlicher Inhalt unzugänglich. Experten

vergleichen diesen Zustand mit einem Tunnel: Offen nur am Anfang und am Ende, dazwischen perfekt abgeschirmt. Die sicheren Verbindungen innerhalb eines öffentlichen IP-Netzes werden deshalb auch „Tunnel“ genannt.

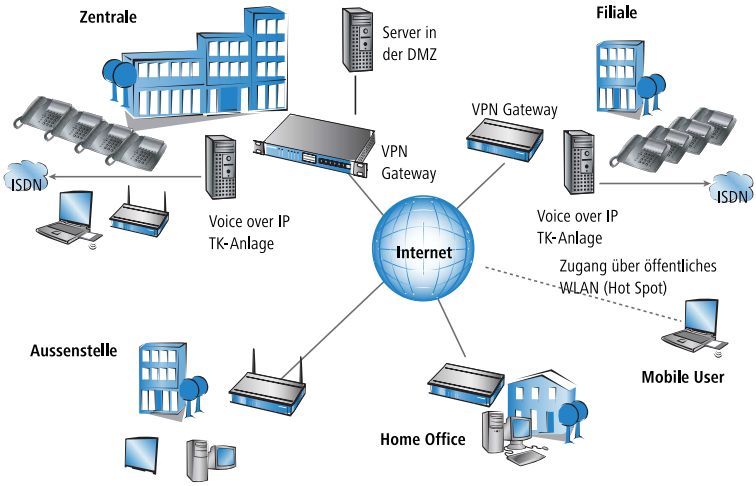


Damit ist das Ziel moderner Netzwerkstrukturen erreicht: Sichere Verbindungen über das größte und kostengünstigste aller öffentlichen IP-Netze: das Internet.

10.2 Das VPN-Modul im Überblick

10.2.1 VPN Anwendungsbeispiel

VPN-Verbindungen werden in sehr unterschiedlichen Anwendungsgebieten eingesetzt. Meistens kommen dabei verschiedene Übertragungstechniken für Daten und auch Sprache zum Einsatz, die über VPN zu einem integrierten Netzwerk zusammenwachsen. Das folgende Beispiel zeigt eine typische Anwendung, die so oder ähnlich in der Praxis oft anzutreffen ist.



Die wesentlichen Komponenten und Merkmale dieser Anwendungen:

- Kopplung von Netzwerken z. B. zwischen Zentrale und Filiale
- Anbindung von Aussenstellen ohne feste IP-Adressen über VPN-Router
- Anbindung von Home Offices ohne feste IP, ggf. über ISDN oder analoge Modems
- Anbindung an Voice-over-IP-Telefonanlagen
- Anbindung von mobilen Usern, z. B. über öffentliche WLAN-Zugänge

10.2.2 Funktionen des VPN-Moduls

In diesem Abschnitt sind alle Funktionen und Eigenschaften des HiLCOS-VPN-Moduls aufgelistet. Experten im Bereich VPN bietet er eine stark komprimierte Zusammenfassung über die Leistungsfähigkeit der Funktion. Das Verständnis der verwendeten Fachtermini setzt allerdings solide Kenntnisse über die technischen Grundlagen von VPN voraus. Für die Inbetriebnahme und den Normalbetrieb von VPN sind diese Informationen jedoch nicht erforderlich.

- VPN-Tunnel über Festverbindung, Wählverbindung und IP-Netzwerk
- Dynamic VPN: Öffentliche IP-Adressen können statisch oder dynamisch sein (für den Aufbau zu Gegenstellen mit dynamischer IP-Adresse ist eine ISDN-Verbindung erforderlich)
- VPN nach dem IPSec-Standard

- IPSec-Protokolle ESP, AH und IPCOMP im Tunnelmodus
- Hash-Algorithmen:
  - HMAC-MD5-96, Hashlänge 128 Bits
  - HMAC-SHA-1-96, Hashlänge 160 Bits
  - HMAC-SHA-256, Hashlänge 256 Bits
  - HMAC-SHA-384, Hashlänge 384 Bits
  - HMAC-SHA-512, Hashlänge 512 Bits
- Kompression mit “Deflate” (ZLIB)
- Schlüsselmanagement nach ISAKMP (IKEv1, IKEv2)
- Symmetrische Verschlüsselungsverfahren
  - AES, Schlüssellänge 128, 192 und 256 Bits
  - Triple-DES (3DES), Schlüssellänge 168 Bits
  - Blowfish, Schlüssellänge 128-448 Bits
  - CAST, Schlüssellänge 128 Bits
  - DES, Schlüssellänge 56 Bits
- IKEv1 Main- und Aggressive-Modus
- IKEv1/IKEv2 Config Mode
- IKEv1 mit Preshared Keys und IKEv2
- IKEv1 und IKEv2 mit RSA-Signature und digitalen Zertifikaten (X.509)
- Schlüsselaustausch über Oakley, Diffie-Hellman-Algorithmus mit Schlüssellänge 768 Bits, 1024 Bits, 1536 Bits, 2048 Bits, 3072 Bits und 4096 Bits (well known groups 1, 2, 5, 14, 15 und 16)

10.3 VPN-Verbindungen im Detail

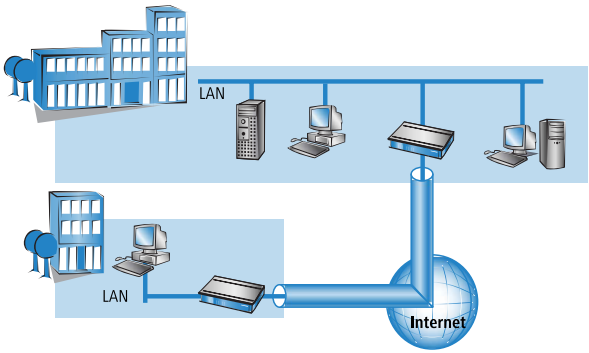
Es existieren zwei Arten von VPN-Verbindungen:

- VPN-Verbindungen zur Kopplung zweier lokaler Netzwerke. Diese Verbindungsart wird auch „LAN-LAN-Kopplung“ genannt.
- Den Anschluss eines einzelnen Rechners mit einem Netzwerk, in der Regel über Einwahlzugänge (Remote Access Service – RAS).

10.3.1 LAN-LAN-Kopplung

Als „LAN-LAN-Kopplung“ wird die Verbindung von zwei entfernten Netzen bezeichnet. Besteht eine solche Verbindung, dann können die Geräte in dem einen LAN auf Geräte des entfernten LANs zugreifen (sofern sie die notwendigen Rechte besitzen).

LAN-LAN-Kopplungen werden in der Praxis häufig zwischen Firmenzentrale und -niederlassungen oder zu Partnerunternehmen aufgebaut.



Auf jeder Seite des Tunnels befindet sich ein VPN-fähiger Router (VPN-Gateway). Die Konfiguration beider VPN-Gateways muss aufeinander abgestimmt sein.

Für die Rechner und sonstigen Geräte in den lokalen Netzwerken ist die Verbindung transparent, d. h., sie erscheint ihnen wie eine gewöhnliche direkte Verbindung. Nur die beiden Gateways müssen für die Benutzung der VPN-Verbindung konfiguriert werden.

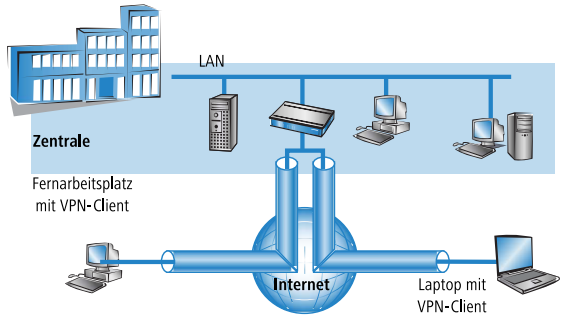
Parallele Internet-Nutzung

Die Internet-Verbindung, über die eine VPN-Verbindung aufgebaut wurde, kann weiterhin parallel für herkömmliche Internet-Anwendungen (Web, Mail etc.) verwendet werden. Aus Sicherheitsgründen kann die parallele Internet-Nutzung allerdings auch unerwünscht sein. So beispielsweise, wenn auch die Filiale nur über die zentrale Firewall auf das Internet zugreifen können soll. Für solche Fälle kann die parallele Internet-Nutzung auch gesperrt werden.

10.3.2 Einwahlzugänge (Remote Access Service)

Über Einwahlzugänge erhalten einzelne entfernte Rechner (Clients) Zugriff auf die Ressourcen eines LANs. Beispiele in der Praxis sind Heimarbeitsplätze oder Außendienstmitarbeiter, die sich in das Firmennetzwerk einwählen.

Soll die Einwahl eines einzelnen Rechners in ein LAN über VPN erfolgen, dann wählt sich der einzelne Rechner ins Internet ein. Eine spezielle VPN-Client-Software baut dann auf Basis dieser Internetverbindung einen Tunnel zum VPN-Gateway in der Zentrale auf.



Das VPN-Gateway in der Zentrale muss den Aufbau von VPN-Tunneln mit der VPN-Client-Software des entfernten Rechners unterstützen.

10.4 Was ist Dynamic VPN?

Dynamic VPN ist eine Technik, die den Aufbau von VPN-Tunneln auch zu solchen Gegenstellen ermöglicht, die keine statische, sondern nur eine dynamische IP-Adresse besitzen.

Wer benötigt Dynamic VPN und wie funktioniert es? Die Antwort erfolgt in zwei Schritten: Zunächst zeigt ein Blick auf die Grundlagen der IP-Adressierung das Problem dynamischer IP-Adressen. Der zweite Schritt zeigt die Lösung durch Dynamic VPN.

10.4.1 Ein Blick auf die IP-Adressierung

Im Internet benötigt jeder Teilnehmer eine eigene IP-Adresse. Er benötigt sogar eine besondere Art von IP-Adresse, nämlich eine öffentliche IP-Adresse. Die öffentlichen IP-Adressen werden von zentralen Stellen im Internet verwaltet. Jede öffentliche IP-Adresse darf im gesamten Internet nur ein einziges Mal existieren.

Innerhalb lokaler Netzwerke auf IP-Basis werden keine öffentlichen, sondern private IP-Adressen verwendet. Für diesen Zweck wurden einige Nummernbereiche des gesamten IP-Adressraums als private IP-Adressen reserviert.

Einem Rechner, der sowohl an ein lokales Netzwerk als auch direkt an das Internet angeschlossen ist, sind deshalb zwei IP-Adressen zugeordnet: Eine öffentliche für die Kommunkation mit dem Rest des Internets und eine private, unter der er in seinem lokalen Netzwerk erreichbar ist.

Statische und dynamischeIP-Adressen

Öffentliche IP-Adressen müssen beantragt und verwaltet werden, was mit Kosten verbunden ist. Es gibt auch nur einen begrenzten Vorrat an öffentlichen IP-Adressen. Aus diesem Grund verfügt auch nicht jeder Internet-Benutzer über eine eigene feste (statische) IP-Adresse.

Die Alternative zu statischen IP-Adressen sind die sogenannten dynamischen IP-Adressen. Eine dynamische IP-Adresse wird dem Internet-Benutzer von seinem Internet Service Provider (ISP) bei der Einwahl für die Dauer der Verbindung zugewiesen. Der ISP verwendet dabei eine beliebige unbenutzte Adresse aus seinem IP-Adress-Pool. Die zugewiesene IP-Adresse ist dem Benutzer nur temporär zugewiesen, nämlich für die Dauer der aktuellen Verbindung. Wird die Verbindung gelöst, so wird die zugewiesene IP-Adresse wieder freigegeben, und der ISP kann sie für den nächsten Benutzer verwenden.

Hinweis: Auch bei vielen Flatrate-Verbindungen handelt es sich oftmals um dynamische IP-Adressen. Dabei findet z. B. alle 24h eine Zwangstrennung der Verbindung statt. Nach dieser Zwangstrennung bekommt der Anschluss i.d.R. eine neue, andere IP-Adresse zugewiesen.

Vor- und Nachteile dynamischer IP-Adressen

Dieses Verfahren hat für den ISP einen wichtigen Vorteil: Er benötigt nur einen relativ kleinen IP-Adress-Pool. Auch für den Benutzer sind dynamische IP-Adressen günstig: Er muss nicht zuerst eine statische IP-Adresse beantragen, sondern kann sich sofort ins Internet einwählen. Auch die Verwaltung der IP-Adresse entfällt. Dadurch erspart er sich Aufwand und Gebühren. Die Kehrseite der Medaille: Ein Benutzer ohne statische IP-Adresse lässt sich aus dem Internet heraus nicht direkt adressieren.

Für den Aufbau von VPNs ergibt sich daraus ein erhebliches Problem. Möchte beispielsweise Rechner A einen VPN-Tunnel zu Rechner B über das Internet aufbauen, so benötigt er dessen IP-Adresse. Besitzt B nur eine dynamische IP-Adresse, so kennt A sie nicht, er kann B deshalb nicht ansprechen.

Hier bietet die Technik von Dynamic VPN die Patentlösung.

10.4.2 So funktioniert Dynamic VPN

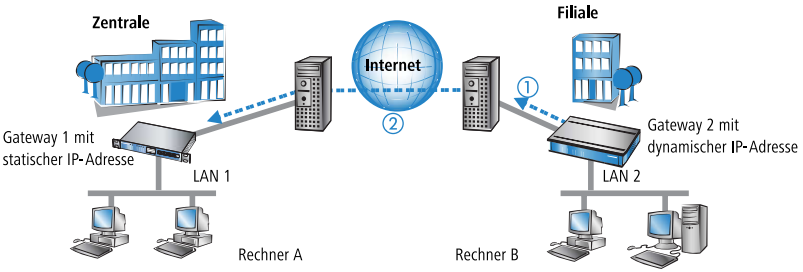
Verdeutlichen wir die Funktionsweise von Dynamic VPN an Hand dreier Beispiele (Bezeichnungen beziehen sich auf die IP-Adressart der beiden VPN-Gateways):

- dynamisch – statisch
- statisch – dynamisch
- dynamisch – dynamisch

Dynamisch – statisch

Möchte ein Benutzer an Rechner B im LAN 2 eine Verbindung zu Rechner A im LAN 1 aufbauen, dann erhält Gateway 2 die Anfrage und versucht, einen VPN-Tunnel zu Gateway 1 aufzubauen. Gateway 1 verfügt über eine statische IP-Adresse und kann daher direkt über das Internet angesprochen werden.

Problematisch ist, dass die IP-Adresse von Gateway 2 dynamisch zugeteilt wird, und Gateway 2 seine aktuelle IP-Adresse beim Verbindungsaufruf an Gateway 1 übermitteln muss. In diesem Fall sorgt Dynamic VPN für die Übertragung der IP-Adresse beim Verbindungsaufbau.



1. Gateway 2 baut eine Verbindung zu seinem Internet-Anbieter auf und erhält eine dynamische IP-Adresse zugewiesen.
2. Gateway 2 spricht Gateway 1 über dessen öffentliche IP-Adresse an. Über Funktionen von Dynamic VPN erfolgen Identifikation und Übermittlung der IP-Adresse an Gateway 2. Schließlich baut Gateway 1 den VPN-Tunnel auf.

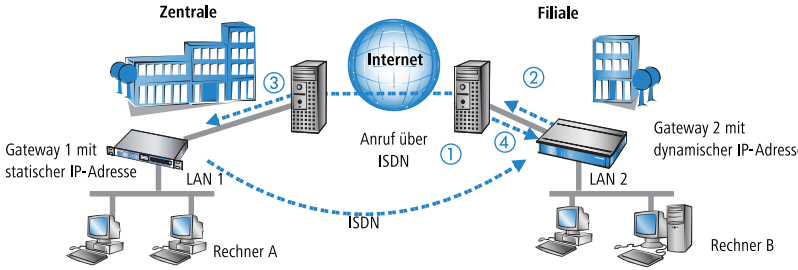
Der große Vorteil der Geräte bei dieser Anwendung: an Stelle des „Aggressive Mode“, der normalerweise für die Einwahl von VPN-Clients in eine Zentrale verwendet wird, kommt hier der wesentlich sicherere „Main Mode“ zum Einsatz. Beim Main Mode werden in der IKE-Verhandlungsphase deutlich mehr Nachrichten ausgetauscht als im Aggressive Mode.

Hinweis: Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

Statisch – dynamisch

Möchte umgekehrt Rechner A im LAN 1 eine Verbindung zu Rechner B im LAN 2 aufbauen, z. B. um alle Außenstellen aus der Zentrale heraus fernzuwarten, dann erhält Gateway 1 die Anfrage und versucht einen VPN-Tunnel zu Gateway 2 aufzubauen. Gateway 2 verfügt nur über eine dynamische IP-Adresse und kann daher nicht direkt über das Internet angesprochen werden.

Mit Hilfe von Dynamic VPN kann der VPN-Tunnel trotzdem aufgebaut werden. Dieser Aufbau geschieht in drei Schritten:



1. Gateway 1 wählt Gateway 2 über ISDN an. Es nutzt dabei die ISDN-Möglichkeit, kostenlos seine eigene Rufnummer über den D-Kanal zu übermitteln. Gateway 2 ermittelt anhand der empfangenen Rufnummer aus den konfigurierten VPN-Gegenstellen die IP-Adresse von Gateway 1.

   Für den Fall, dass Gateway 2 keine Rufnummer über den D-Kanal erhält (etwa weil das erforderliche ISDN-Leistungsmerkmal nicht zur Verfügung steht) oder eine unbekannte Rufnummer übertragen wird, nimmt Gateway 2 den Anruf entgegen, und die Geräte authentifizieren sich über den B-Kanal. Nach erfolgreicher Aushandlung übermittelt Gateway 1 seine IP-Adresse und baut den B-Kanal sofort wieder ab.

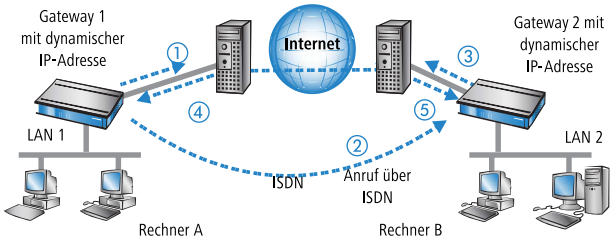
2. Nun ist Gateway 2 an der Reihe: Zunächst baut es eine Verbindung zu seinem ISP auf, von dem es eine dynamische IP-Adresse zugewiesen bekommt.
3. Gateway 2 authentifiziert sich bei Gateway 1, dessen statische Adresse ihm bekannt ist.
4. Gateway 1 kennt nun die Adresse von Gateway 2 und kann den VPN-Tunnel zu Gateway 2 jetzt aufbauen.

Der Vorteil der Geräte z. B. beim Aufbau der Verbindung aus der Zentrale zu den Filialen: Mit den Funktionen von Dynamic VPN können auch Netzwerke ohne Flatrate erreicht werden, die also nicht „allways online“ sind. Der ISDN-Anschluss ersetzt mit der bekannten MSN eine andere Adresse, z. B. eine statische IP-Adresse oder eine dynamische Adressauflösung über Dynamic-DNS-Dienste, die i.d.R. nur bei Flatrate-Anschlüssen zum Einsatz kommen.

Hinweis: Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

Dynamisch – dynamisch

Der Aufbau von VPN-Tunneln gelingt mit Dynamic VPN auch zwischen zwei Gateways, die beide nur über dynamische IP-Adressen verfügen. Passen wir das besprochene Beispiel an, so dass diesmal auch Gateway 1 nur über eine dynamische IP-Adresse verfügt. Auch in diesem Beispiel möchte Rechner A eine Verbindung zu Rechner B aufbauen:



1. Gateway 1 baut eine Verbindung zu seinem ISP auf, um eine öffentliche dynamische Adresse zu erhalten.
2. Es folgt der Anruf über ISDN bei Gateway 2 zur Übermittlung dieser dynamischen Adresse. Zur Übermittlung werden drei Verfahren verwendet:

   - **Als Information im** LLC-Element des D-Kanals. Über das D-Kanal-Protokoll von Euro-ISDN (DSS-1) können im sogenannten LLC-Element (**L**ower **L**ayer **C**ompatibility) beim Anruf zusätzliche Informationen an die Gegenstelle übermittelt werden. Diese Übermittlung findet vor dem Aufbau des B-Kanals statt. Die Gegenstelle lehnt nach erfolgreicher Übertragung der Adresse den Anruf ab. Eine gebührenpflichtige Verbindung über den B-Kanal kommt auf diese Weise nicht zustande. Die IP-Adresse wird aber trotzdem übertragen.

     Hinweis: Das LLC-Element steht normalerweise im Euro-ISDN ohne besondere Anmeldung oder Freischaltung zur Verfügung. Es kann allerdings von Telefongesellschaften, einzelnen Vermittlungsstellen oder Telefonanlagen gesperrt werden. Im nationalen ISDN nach 1TR6 gibt es kein LLC-Element. Das beschriebene Verfahren funktioniert daher nicht.

- Als Subadresse über den D-Kanal. Funktioniert die Adressübermittlung über das LLC-Element nicht, dann versucht Gateway 1 die Adresse als sogenannte Subadresse zu übermitteln. Die Subadresse ist wie das LLC-Element ein Informationselement des D-Kanal-Protokolls und ermöglicht wie dieses die kostenlose Übermittlung kurzer Informationen. Allerdings muss hier die Telefongesellschaft das ISDN-Merkmal 'Subadressierung' (normalerweise gegen Berechnung) freischalten. Wie beim LLC-Element wird der Anruf nach erfolgreicher Übertragung der IP-Adresse von der Gegenstelle abgelehnt und die Verbindung bleibt gebührenfrei.
- Über den B-Kanal. Scheitern beide Versuche, die IP-Adresse über den D-Kanal zu übertragen, dann muss für die Übertragung der IP-Adresse eine konventionelle Verbindung über den B-Kanal aufgebaut werden. Nach der Übertragung der IP-Adresse wird die Verbindung sofort abgebaut. Es fallen die üblichen Gebühren an.

3. Gateway 2 baut eine Verbindung zum ISP auf, der ihm eine dynamische IP-Adresse zuweist.
4. Gateway 2 authentifiziert sich bei Gateway 1 (dessen Adresse durch Schritt 2 bekannt ist).
5. Gateway 1 kennt nun die Adresse von Gateway 2 und kann so den VPN-Tunnel zu Gateway 2 aufbauen.

Hinweis: Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

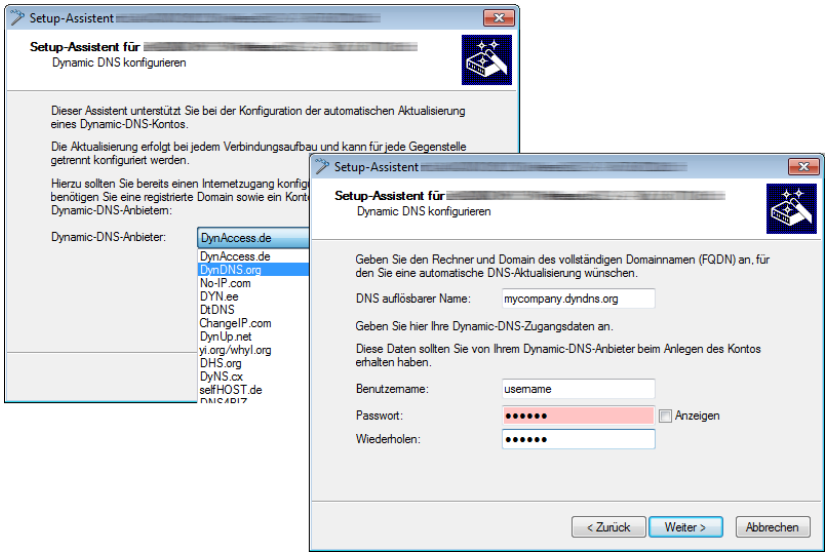
Dynamische IP-Adressen und DynDNS

Der Verbindungsaufbau zwischen zwei Stationen mit dynamischen IP-Adressen ist ebenfalls unter Verwendung eines so genannten Dynamic-DNS-Dienstes (DynDNS) möglich. Dazu wird die Tunnel-Endpunktadresse nicht in Form einer IP-Adresse angegeben (die ja dynamisch ist und häufig wechselt), sondern in Form eines statischen Namens (z. B. MyDevice@DynDNS.org).

Für die Namensauflösung zu einer jeweils aktuellen IP-Adresse werden zwei Dinge benötigt: Ein Dynamic-DNS-Server und ein Dynamic-DNS-Client:

- Ersterer ist ein Server, wie er von vielen Dienstleistern im Internet angeboten wird und der mit Internet-DNS-Servern in Verbindung steht.

- Der Dynamic-DNS-Client ist im Gerät integriert. Er kann zu einer Vielzahl von Dynamic-DNS-Serviceanbietern Kontakt aufnehmen und bei jeder Änderung seiner IP-Adresse automatisch ein vorher angelegtes Benutzerkonto zur DNS-Namensauflösung beim Dynamic-DNS-Anbieter aktualisieren. Die Einrichtung geschieht komfortabel mit einem Assistenten unter LANconfig:



Hinweis: Aus Sicherheits- und Verfügbarkeitsgründen empfehlen wir den Einsatz des Dynamic VPN Verfahrens gegenüber Dynamic DNS basierten VPN-Lösungen. Dynamic VPN basiert auf Verbindungen über das ISDN-Netz, das eine deutlich höhere Verfügbarkeit garantiert als die Erreichbarkeit eines Dynamic-DNS-Diensts im Internet.

10.5 Konfiguration von VPN-Verbindungen

Bei der Konfiguration von VPN-Verbindungen werden drei Fragen beantwortet:

- Zwischen welchen VPN-Gateways (Gegenstellen) wird die Verbindung aufgebaut?

- Mit welchen Sicherheitsparametern wird der VPN-Tunnel zwischen den beiden Gateways gesichert?
- Welche Netzwerke bzw. Rechner können über diesen Tunnel miteinander kommunizieren?

Hinweis: In diesem Abschnitt werden die grundsätzlichen Überlegungen zur Konfiguration von VPN-Verbindungen vorgestellt. Dabei bezieht sich die Beschreibung zunächst auf die einfache Verbindung von zwei lokalen Netzwerken. Sonderfälle wie die Einwahl in LANs mit einzelnen Rechnern (RAS) oder die Verbindung von strukturierten Netzwerken werden im weiteren Verlauf dargestellt.

10.5.1 VPN-Tunnel: Verbindungen zwischen den VPN-Gateways

In virtuellen privaten Netzwerken (VPNs) werden lokale Netzwerke über das Internet miteinander verbunden. Dabei werden die privaten IP-Adressen aus den LANs über eine Internet-Verbindung zwischen zwei Gateways mit öffentlichen IP-Adressen geroutet.

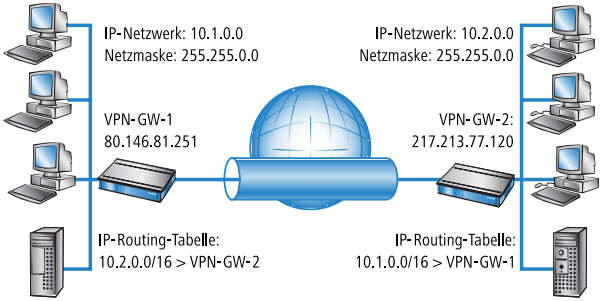
Um das gesicherte Routing der privaten IP-Adressbereiche über die Internet-Verbindung zu ermöglichen, wird zwischen den beiden LANs eine VPN-Verbindung etabliert, die auch als VPN-Tunnel bezeichnet wird.

Der VPN-Tunnel hat zwei wichtige Aufgaben:

- Abschirmen der transportierten Daten gegen den unerwünschten Zugriff von Unbefugten
- Weiterleiten der privaten IP-Adressen über eine Internet-Verbindung, auf der eigentlich nur öffentliche IP-Adressen geroutet werden können.

Die VPN-Verbindung zwischen den beiden Gateways wird durch die folgenden Parameter definiert:

- Die Endpunkte des Tunnels, also die VPN-Gateways, die jeweils über eine öffentliche IP-Adresse (statisch oder dynamisch) erreichbar sind
- Die IP-Verbindung zwischen den beide Gateways
- Die privaten IP-Adressbereiche, die zwischen den VPN-Gateways geroutet werden sollen
- Sicherheitsrelevante Einstellungen wie Passwörter, IPSec-Schlüssel etc. für die Abschirmung des VPN-Tunnels



Diese Informationen sind in den so genannten VPN-Regeln enthalten.

10.5.2 VPN-Verbindungen einrichten mit den Setup-Assistenten

Verwenden Sie für die Einrichtung der VPN-Verbindungen zwischen den lokalen Netzen nach Möglichkeit die Setup-Assistenten von LANconfig. Die Assistenten leiten Sie durch die Konfiguration und nehmen alle benötigten Einstellungen vor. Führen Sie die Konfiguration nacheinander an beiden Routern durch.

1. Markieren Sie Ihr Gerät im Auswahlfenster von LANconfig und wählen Sie die Schaltfläche **Setup Assistent** oder aus der Menüleiste den Punkt **Extras** / **Setup Assistent**.
2. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein. Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.
3. Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit `ping`) anzusprechen. Das Gerät sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

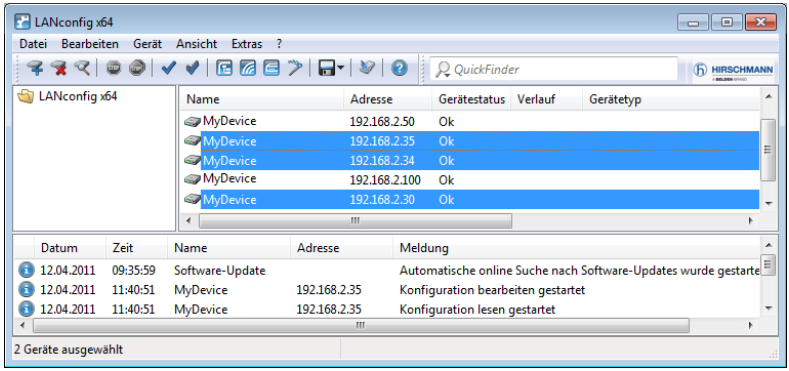
Mit diesem Assistenten werden für eine normale LAN-LAN-Kopplung alle notwendigen VPN-Verbindungen automatisch angelegt. Die manuelle Konfiguration der VPN-Verbindungen ist in den folgenden Fällen erforderlich:

- Wenn kein Windows-Rechner mit LANconfig zur Konfiguration verwendet werden kann. In diesem Fall nehmen Sie die Einstellung der erforderlichen Parameter über WEBconfig oder die Telnet-Konsole vor.
- Wenn nicht das komplette lokale LAN (Intranet) über die VPN-Verbindung mit anderen Rechnern kommunizieren soll. Das ist z. B. dann der Fall, wenn an das Intranet weitere Subnetze mit Routern angeschlossen sind, oder wenn nur Teile des Intranets auf die VPN-Verbindung zugreifen können sollen. In diesen Fällen werden die Parameter der Setup-Assistenten nachträglich um weitere Einstellungen ergänzt.
- Wenn VPN-Verbindungen zu Fremdgeräten konfiguriert werden sollen.

10.5.3 1-Click-VPN für Netzwerke (Site-to-Site)

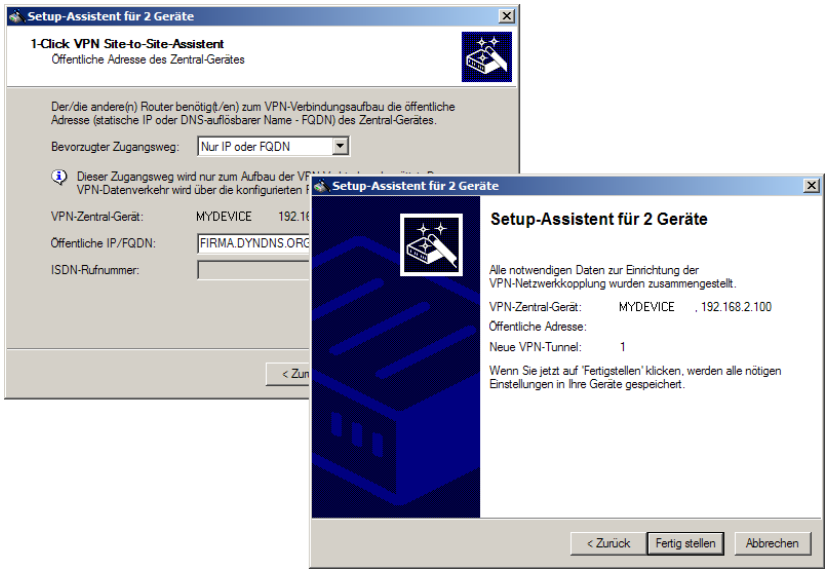
Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an ein zentrales Netzwerk gekoppelt werden.

1. Markieren Sie in LANconfig die Router der Filialen, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.
2. Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.



3. Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist

.



1. Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers oder über eine ISDN-Verbindung erfolgen soll. Geben Sie dazu die Adresse bzw. den Namen des zentralen Routers bzw. seine ISDN-Nummer an.
2. Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
   - Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht werden.
   - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

   Hinweis: Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

10.5.4 1-Click-VPN für LANCOM Advanced VPN Client

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Client in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM

Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des VPN-Routers entnommen und mit zufällig ermittelten Werten ergänzt (z. B. für den Preshared Key).

1. Starten Sie über LANconfig den Setup-Assistenten 'Zugang bereitstellen' und wählen Sie die 'VPN-Verbindung'.
2. Aktivieren Sie die Optionen 'LANCOM Advanced VPN Client' und 'Beschleunigen Sie das Konfigurieren mit 1-Click-VPN'.
3. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
4. Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:

   - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
   - Profil per E-Mail versenden
   - Profil ausdrucken

   Hinweis: Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte! Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

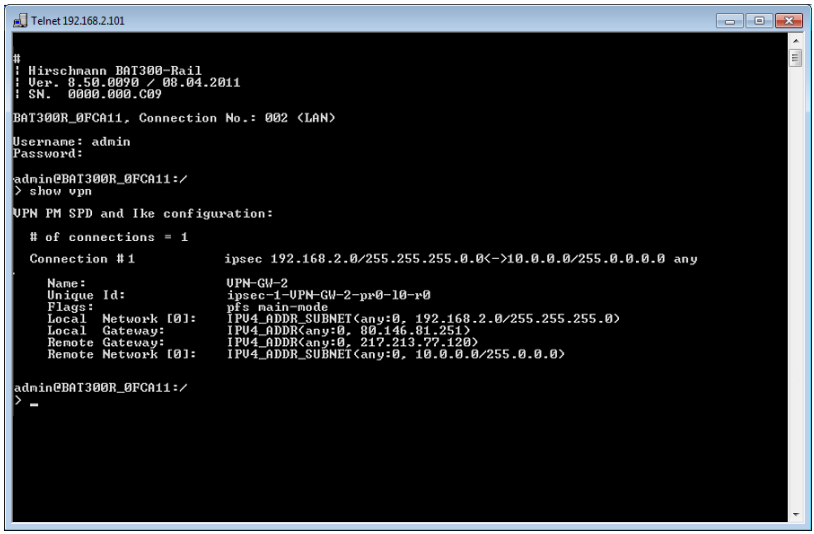
   Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z. B.:

   - Gateway: Sofern im VPN-Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
   - FQUN: Kombination aus dem Namen der Verbindung, einer fortlaufenden Nummer und der internen Domäne im VPN-Router
   - Domäne: Sofern im VPN-Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
   - VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
   - Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.

- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wir der 'Aggressive Mode' verwendet.
- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom VPN-Router zugewiesen.

10.5.5 VPN-Regeln einsehen

Die Informationen über die aktuellen VPN-Regeln im Gerät können Sie über die Telnet-Konsole abrufen. Stellen Sie dazu eine Telnet-Verbindung zu dem VPN-Gateway her und geben Sie an der Konsole den Befehl `show vpn` ein:



In der Ausgabe finden Sie die Informationen über die Netzbeziehungen, die für den Aufbau von VPN-Verbindungen zu anderen Netzwerken in Frage kommen.

In diesem Fall wird das lokale Netzwerk einer Filiale (Netzwerk `192.168.2.0` mit der Netzmaske `255.255.255.0`) und das Netz der Zentrale (Netzwerk `10.0.0.0` mit der Netzmaske `255.0.0.0`) angebunden. Die öffentliche IP-

Adresse des eigenen Gateways lautet `80.146.81.251`, die des entfernten VPN-Gateways ist die `217.213.77.120`.

Hinweis: Die Angabe `any:0` zeigt die über die Verbindung erlaubten Protokolle und Ports an.

Eine erweiterte Ausgabe wird über den Befehl `show vpn long` aufgerufen. Hier finden Sie neben den Netzbeziehungen auch die Informationen über die sicherheitsrelevanten Parameter wie IKE- und IPSec-Proposals.

10.5.6 Manuelles Einrichten der VPN-Verbindungen

Beim manuellen Einrichten der VPN-Verbindungen fallen die schon beschriebenen Aufgaben an:

- Definition der Tunnelendpunkte
- Definition der sicherheitsrelevanten Parameter (IKE und IPSec)
- Definition der VPN-Netzbeziehungen, also der zu verbindenden IP-Adressbereiche. Bei überschneidenden IP-Netzbereichen auf den beiden Seiten der Verbindung bitte auch den Abschnitt beachten.
- Bei Kopplung von Windows Netzwerken (NetBIOS/IP): Ohne WINS-Server auf beiden Seiten der VPN-Verbindung (z. B. bei der Anbindung von Home-Offices) kann das Gerät entsprechende NetBIOS-Proxy-Funktionen übernehmen. Dazu muss das NetBIOS-Modul des Gerätes aktiviert sein, und die entsprechende VPN-Gegenstelle muss im NetBIOS-Modul als Gegenstelle eingetragen sein. Sind jedoch bei einer Standortkopplung in beiden Netzwerken eigene WINS-Server vorhanden, dann sollte das NetBIOS-Modul deaktiviert werden, so dass das Gerät keine NetBIOS-Proxy-Funktionen mehr ausführt.

  Hinweis: Um den NetBIOS-Proxy des Gerätes nutzen zu können muss entweder Dynamic VPN verwendet werden, da dieses alle nötigen Adressen übermittelt, oder die IP-Adresse der Gegenstelle (hinter dem Tunnel, d.h. die dessen Intranet-Adresse) als primärer NBNS in der IP-Parameterliste (LANconfig: Kommunikation / Protokolle) eingetragen werden.

- Bei Nutzung von Dynamic VPN: Eintrag für die entsprechende Gegenstelle in der PPP-Liste mit einem geeigneten Passwort für die Dynamic VPN Verhandlung. Als Benutzername ist derjenige VPN-Verbindungsname

einzutragen, unter dem das Gerät in der VPN-Verbindungsliste der entfernten Gegenstelle angesprochen wird. Aktivieren Sie das „IP Routing“. Sollen auch Windows Netzwerke gekoppelt werden, so ist in diesem Eintrag zusätzlich NetBIOS zu aktivieren.

Als Tunnelendpunkt wird neben dem eigenen, lokalen VPN-Gateway jeweils eine VPN-Gegenstelle in der VPN-Verbindungsliste eingetragen.

Die manuelle Konfiguration der VPN-Verbindungen umfasst die folgenden Schritte:

1. Legen Sie das entfernte VPN-Gateway in der Verbindungsliste an und tragen Sie dabei die öffentlich erreichbare Adresse ein.
2. Die Sicherheitsparameter für die VPN-Verbindung werden in der Regel aus den vorbereiteten Listen entnommen, hier besteht neben der Definition eines IKE-Schlüssels kein weiterer Handlungsbedarf.
3. Bei einer Dynamic VPN-Verbindung erzeugen Sie einen neuen Eintrag in der PPP-Liste mit dem Namen des entfernten VPN-Gateways als Gegenstelle, mit dem Namen des lokalen VPN-Gateways als Benutzername und einem geeigneten Passwort. Für diese PPP-Verbindung aktivieren Sie auf jeden Fall das IP-Routing sowie je nach Bedarf auch das Routing von "NetBIOS über IP". Die restlichen PPP-Parameter wie das Verfahren für die Überprüfung der Gegenstelle können analog zu anderen PPP-Verbindungen definiert werden.
4. Die Hauptaufgabe bei der Einrichtung von VPN-Verbindungen liegt schließlich in der Definition der Netzbeziehungen: Welche IP-Adressbereiche sollen auf den beiden Seiten des VPN-Tunnels in die gesicherte Verbindung einbezogen werden?

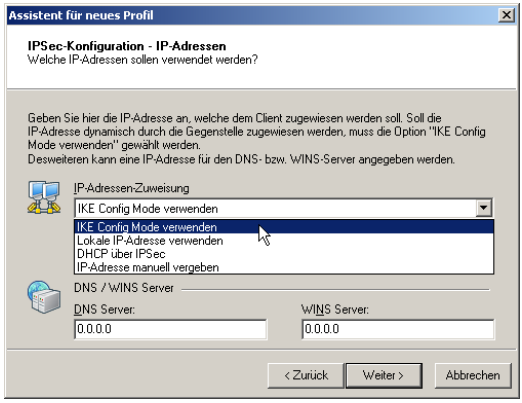
10.5.7 IKE Config Mode

Bei der Konfiguration von VPN-Einwahlzugängen kann alternativ zur festen Vergabe der IP-Adressen für die einwählenden Gegenstellen auch ein Pool von IP-Adressen angegeben werden. In den Einträgen der Verbindungsliste wird dazu der „IKE-CFG“-Modus angegeben. Dieser kann die folgenden Werte annehmen:

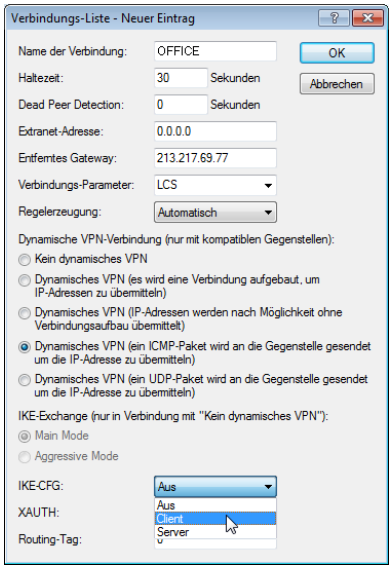
- **Server**: In dieser Einstellung fungiert das Gerät als Server für diese VPN-Verbindung. Für die Zuweisung der IP-Adresse an den Client gibt es zwei Möglichkeiten:

- Wenn die Gegenstelle in der Routing-Tabelle eingetragen ist, wird ihr die dort konfigurierte IP-Adresse zugewiesen.
- Wenn die Gegenstelle nicht in der Routing-Tabelle eingetragen ist, wird eine freie IP-Adresse aus dem IP-Pool für die Einwahlzugänge entnommen.

Hinweis: Die Gegenstelle muss dabei als IKE-CFG-Client konfiguriert sein und so vom Server eine IP-Adresse für die Verbindung anfordern.



- **Client**: In dieser Einstellung fungiert das Gerät als Client für diese VPN-Verbindung und fordert eine IP-Adresse für die Verbindung von der Gegenstelle (Server) an. Das Gerät verhält sich also so ähnlich wie ein VPN-Client.
- **Aus**: Ist der IKE-CFG-Modus ausgeschaltet, werden keine IP-Adressen für die Verbindung zugewiesen. Auf beiden Seiten der VPN-Strecke muss fest konfiguriert sein, welche IP-Adressen für diese Verbindung zu verwenden sind.



LANconfig: VPN / Allgemein / Verbindungs-liste

WEBconfig: HiLCOS-Menübaum / Setup / VPN E Name-Liste

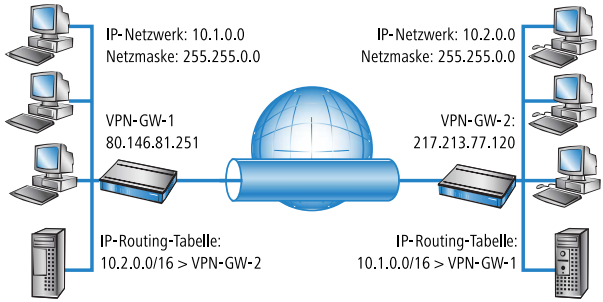
10.5.8 VPN-Netzbeziehungen erstellen

Mit der integrierten Firewall verfügen die Router über ein leistungsfähiges Instrument zur Definition von Quell- und Ziel-Adressbereichen, für die eine Datenübertragung (ggf. mit weiteren Einschränkungen) erlaubt bzw. verboten werden soll. Diese Funktionen werden auch für die Einrichtung der Netzbeziehungen für die VPN-Regeln verwendet.

Im einfachsten Fall kann die Firewall die VPN-Regeln automatisch erzeugen:

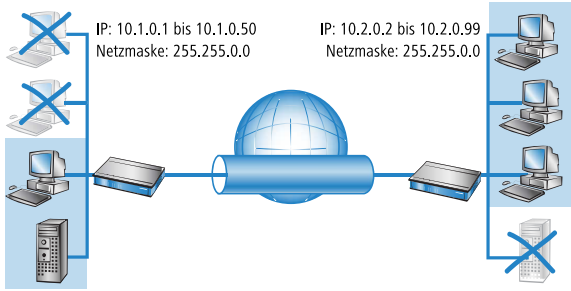
- Als Quellnetz wird dabei das lokale Intranet eingesetzt, also derjenige private IP-Adressbereich, zu dem das lokale VPN-Gateway selbst gehört.
- Als Zielnetze dienen für die automatisch erstellten VPN-Regeln die Netzbereiche aus der IP-Routing-Tabelle, für die als Router ein entferntes VPN-Gateway eingetragen ist.

Zum Aktivieren dieser automatischen Regelerzeugung reicht es aus, die entsprechende Option in der Firewall einzuschalten[1]. Bei der Kopplung von zwei einfachen lokalen Netzwerken kann die VPN-Automatik aus dem IP-Adressbereich des eigenen LANs und dem Eintrag für das entfernte LAN in der IP-Routing-Tabelle die erforderliche Netzbeziehung ableiten.



Etwas aufwändiger wird die Beschreibung der Netzbeziehungen dann, wenn die Quell- und Zielnetze nicht nur durch den jeweiligen Intranet-Adressbereich der verbundenen LANs abgebildet werden:

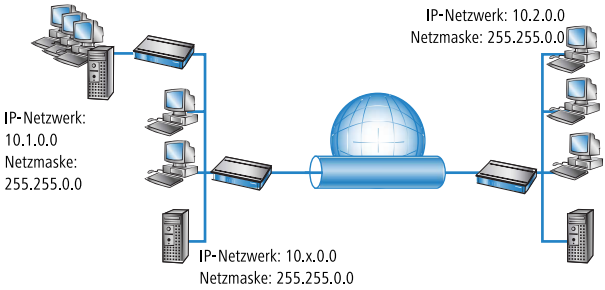
- Wenn nicht das gesamte lokale Intranet in die Verbindung mit dem entfernten Netz einbezogen werden soll, würde die Automatik einen zu großen IP-Adressbereich für die VPN-Verbindung freigeben.



- In vielen Netzstrukturen sind an das lokale Intranet über weitere Router noch andere Netzabschnitte mit eigenen IP-Adressbereichen angebunden.

[1] automatisch bei Verwendung des VPN-Installationsassistenten unter LANconfig

Diese Adressbereiche müssen über zusätzliche Einträge in die Netzbeziehung einbezogen werden.



In diesen Fällen müssen die Netzbeziehungen zur Beschreibung der Quell- und Zielnetze manuell eingetragen werden. Je nach Situation werden dabei die automatisch erzeugten VPN-Regeln erweitert, manchmal muss die VPN-Automatik ganz abgeschaltet werden, um unerwünschte Netzbeziehungen zu vermeiden.

Die erforderlichen Netzbeziehungen werden durch entsprechende Firewall-Regeln unter den folgenden Randbedingungen definiert:

- Für die Firewall-Regel muss die Option "Diese Regel wird zur Erzeugung von VPN-Regeln herangezogen" aktiviert sein.

  Hinweis: Die Firewall-Regeln zur Erzeugung von VPN-Regeln sind auch dann aktiv, wenn die eigentliche Firewall-Funktion im Gerät nicht benötigt wird und ausgeschaltet ist!

- Als Firewall-Aktion muss auf jeden Fall "Übertragen" gewählt werden.
- Als Quelle und Ziel für die Verbindung können einzelne Stationen, bestimmte IP-Adressbereiche oder ganze IP-Netzwerke eingetragen werden.

  Hinweis: Die Zielnetze müssen auf jeden Fall in der IP-Routing-Tabelle definiert sein, damit der Router in den Geräten die entsprechenden Datenpakete in das andere Netz weiterleiten kann. Die dort schon vorhandenen Einträge können Sie nutzen und nur ein übergeordnetes Netzwerk als Ziel eintragen. Die Schnittmenge aus dem Eintrag des Zielnetzes in

der Firewall und den untergeordneten Einträgen in der IP-Routing-Tabelle fließt in die Netzbeziehungen für die VPN-Regeln ein.

Beispiel: In der IP-Routing-Tabelle sind die Zielnetze 10.2.1.0/24, 10.2.2.0/24 und 10.2.3.0/24 eingetragen, die alle über den Router VPN-GW-2 erreichbar sind. In der Firewall reicht ein Eintrag mit dem Zielnetz 10.2.0.0/16, um die drei gewünschten Subnetze in die VPN-Regeln einzubeziehen.

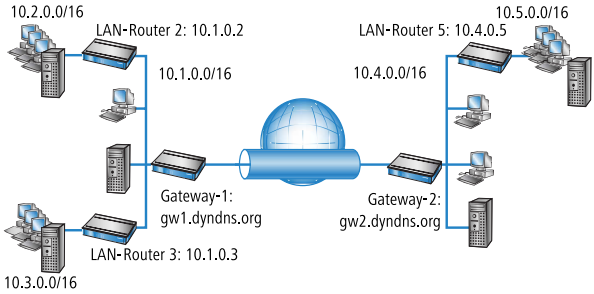
Hinweis: Die Quell- und Zielnetze müssen auf beiden Seiten der VPN-Verbindung übereinstimmend definiert werden. Es ist z. B. nicht möglich, einen größeren Ziel-Adressbereich auf einen kleineren Quell-Adressbereich auf der Gegenseite abzubilden. Maßgebend sind dabei die in den VPN-Regeln gültigen IP-Adressbereiche, nicht die in den Firewall-Regeln eingetragenen Netze. Diese können aufgrund der Schnittmengenbildung durchaus von den Netzbeziehungen in den VPN-Regeln abweichen.

- Je nach Bedarf kann die VPN-Verbindung zusätzlich auf bestimmte Dienste oder Protokolle eingeschränkt werden. So kann die VPN-Verbindung z. B. nur auf die Nutzung für ein Windows-Netzwerk reduziert werden.

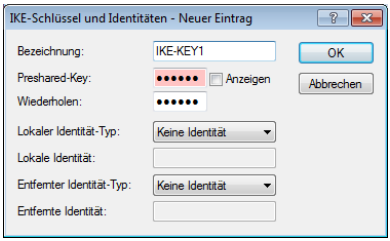
Hinweis: Verwenden Sie für diese Einschränkungen eigene Regeln, die nur für die Firewall gelten und nicht zur Erzeugung von VPN-Regeln herangezogen werden. Kombinierte Firewall/VPN-Regeln können sehr leicht komplex und schwer überschaubar werden.

10.5.9 Konfiguration mit LANconfig

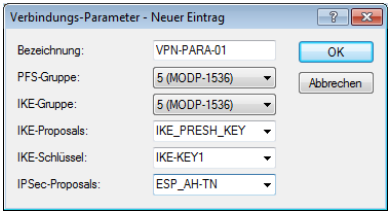
Dieser Anschnitt zeigt die Konfiguration einer LAN-LAN-Kopplung mit zusätzlichen Subnetzen mit Hilfe von LANconfig. In diesem Abschnitt wird das VPN-Gateway 1 konfiguriert, die Einstellung von Gateway 2 wird anschließend mit Hilfe von WEBconfig demonstriert.



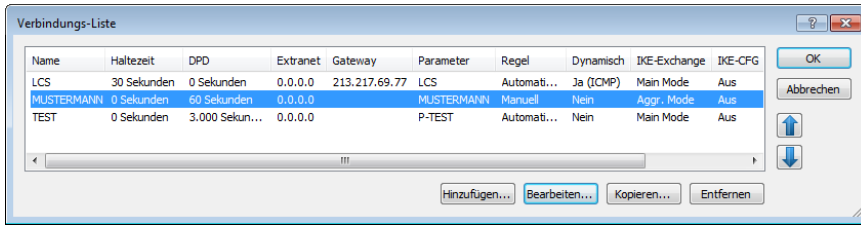
1. Legen Sie im Konfigurationsbereich VPN auf der Registerkarte „IKE-Auth." einen neuen IKE-Schlüssel für die Verbindung an:



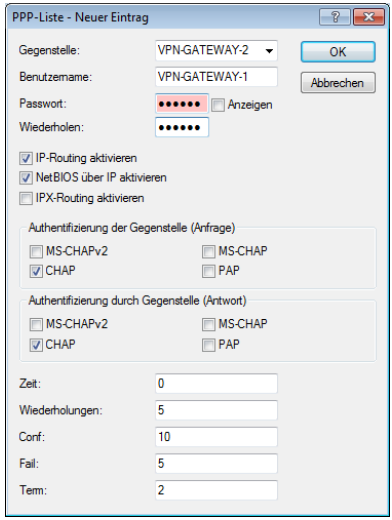
2. Erstellen Sie auf der Registerkarte „Allgemein" einen neuen Eintrag in der Liste der Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus. PFS- und IKE-Gruppe können Sie ebenso wie IKE- und IPSec-Proposals aus den vorbereiteten Möglichkeiten wählen.



3. Erstellen Sie dann einen neuen Eintrag in der Verbindungs-Liste mit dem Namen des entfernten Gateways als „Name der Verbindung". Für Dynamic VPN Verbindungen muss der Eintrag „Entferntes Gateway" leer bleiben. Andernfalls tragen Sie hier die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.

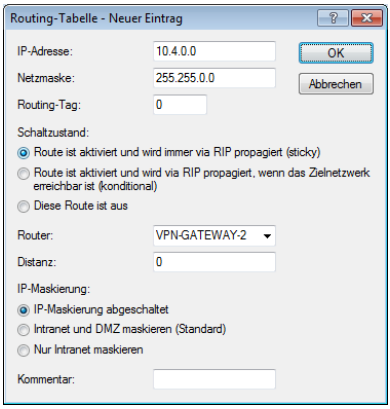


4. Bei Nutzung von Dynamic VPN: Wechseln Sie in den Konfigurationsbereich „Kommunikation“. Erstellen Sie auf der Registerkarte „Protokolle“ in der PPP-Liste einen neuen Eintrag. Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie ein geeignetes, auf beiden Seiten identisches Passwort ein, welches aus Sicherheitsgründen nicht identisch mit dem verwendeteten Pre-Shared Key sein sollte.



Aktivieren Sie auf jeden Fall das „IP-Routing“ und je nach Bedarf „NetBIOS über IP“.

5. Wechseln Sie in den Konfigurationsbereich „IP-Router“. Erstellen Sie auf der Registerkarte „Routing“ einen neuen Eintrag in der Routingtabelle für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.



Für das „VPN-Gateway-1“ sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

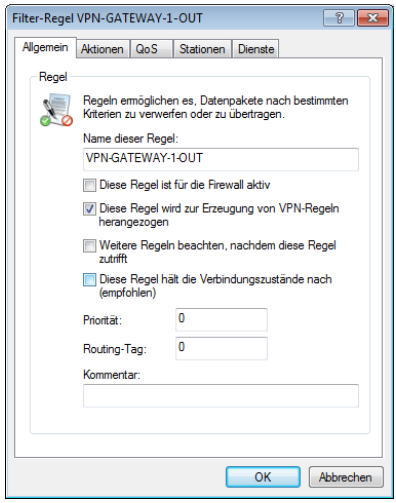
IP-Adresse	*Netzmaske*	*Router*	*IP-Masquerading*
10.4.0.0	255.255.0.0	VPN-Gateway-2	Nein
10.5.0.0	255.255.0.0	VPN-Gateway-2	Nein

Für die an das eigene LAN angebundenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	*Netzmaske*	*Router*	*IP-Masquerading*
10.2.0.0	255.255.0.0	10.1.0.2	Nein
10.3.0.0	255.255.0.0	10.1.0.3	Nein

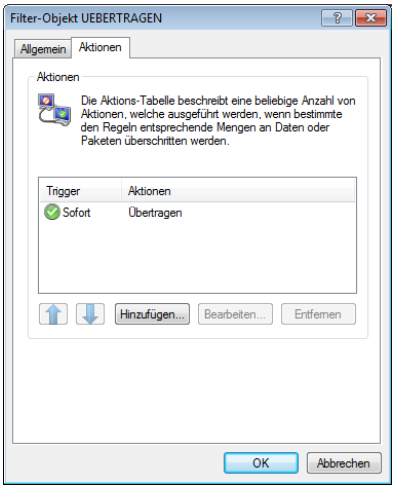
Mit diesen Einträgen ist das VPN-Gateway 1 in der Lage, auch die aus dem entfernten Netz eintreffen Pakete für die angebundenen Netzabschnitte richtig weiterzuleiten.

6. Wechseln Sie in den Konfigurationsbereich „Firewall/QoS“. Erstellen Sie auf der Registerkarte „Regeln“ eine neue Firewall-Regel mit dem Namen „VPN-GATEWAY-1-OUT“ und aktivieren Sie für diese Regel die Option „Diese Regel wird für die Erzeugung von VPN-Regeln herangezogen“. Damit legen Sie fest, dass die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.

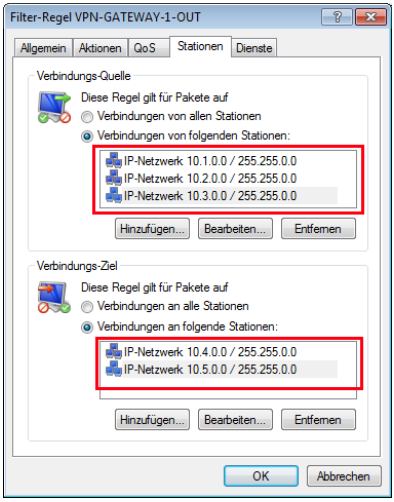


Hinweis: Die Firewall-Regeln zum Erzeugen von VPN-Netzbeziehungen mit Angabe der Tunnelendpunkte (IP-Quell- und Ziel-Adressen) sollten auf jeden Fall von Firewall-Regeln zum Filtern (z. B. der zu übertragenden bzw. der zu sperrenden Protokolle) getrennt werden. Die Verknüpfung dieser beiden Aspekte kann zu einer hohen Anzahl der intern verwalteten VPN-Beziehungen und damit zu Performanceverlusten in den VPN-Tunneln führen.

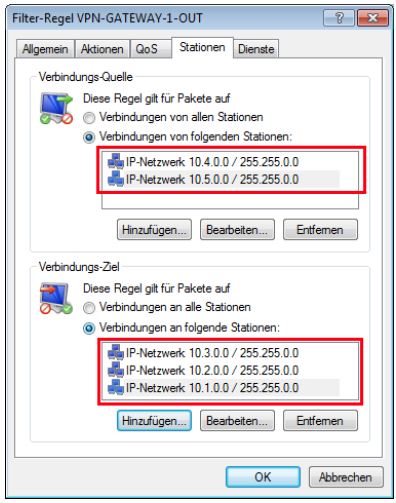
7. Auf der Registerkarte „Aktionen“ dieser Firewall-Regel stellen Sie als Paketaktion „Übertragen“ ein.



8. Auf der Registerkarte „Stationen“ dieser Firewall-Regel stellen Sie für die ausgehende Datenübertragung als Quelle die Teilnetze auf der lokalen Seite ein, als Ziel alle Teilnetze auf der entfernten Seite.

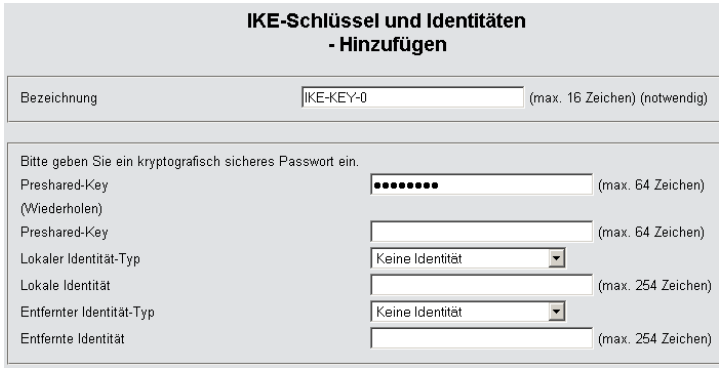


9. Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GATEWAY-1-IN“ mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:

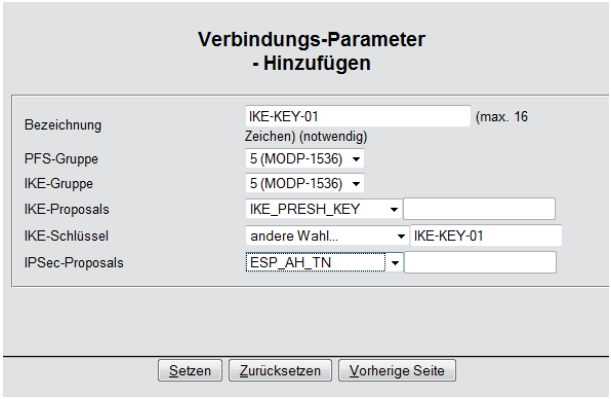


10.5.10 Konfiguration mit WEBconfig

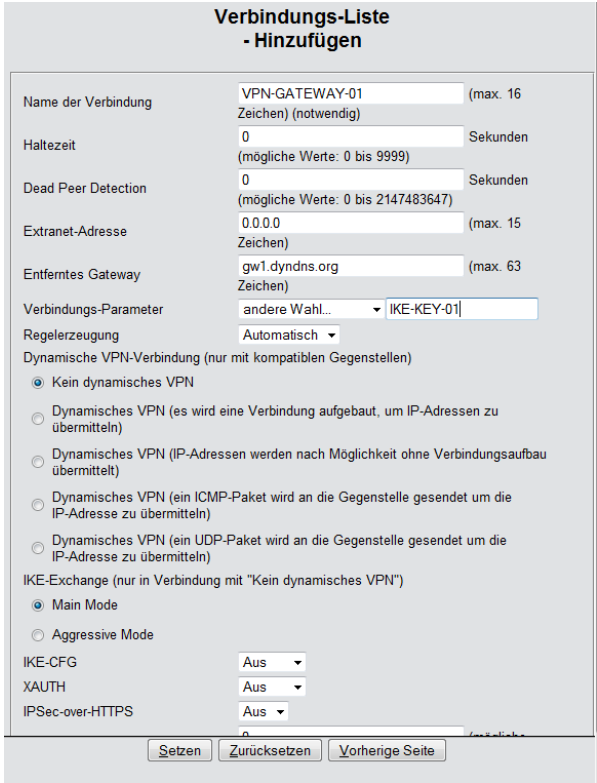
1. Legen Sie unter **Konfiguration** / **VPN** / **IKE-Auth./IKE-Schlüssel und Identitäten** einen neuen IKE-Schlüssel für die Verbindung an:



2. Erstellen Sie unter **Konfiguration** / **VPN** / **Allgemein** / **Verbindungsparameter** einen neuen „VPN-Layer“ für die Verbindungsparameter. Wählen Sie dabei den zuvor erstellten IKE-Schlüssel aus.

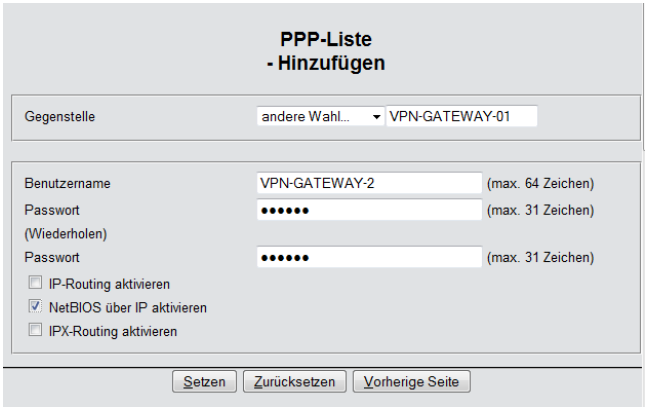


3. Erstellen Sie unter **Konfiguration** / **VPN** / **Verbindungsliste** einen neuen Eintrag mit dem Namen des entfernten Gateways als „Name“. Als „Entferntes Gateway“ tragen Sie die öffentliche Adresse der Gegenstelle ein: entweder die feste IP-Adresse oder den DNS-auflösbaren Namen.



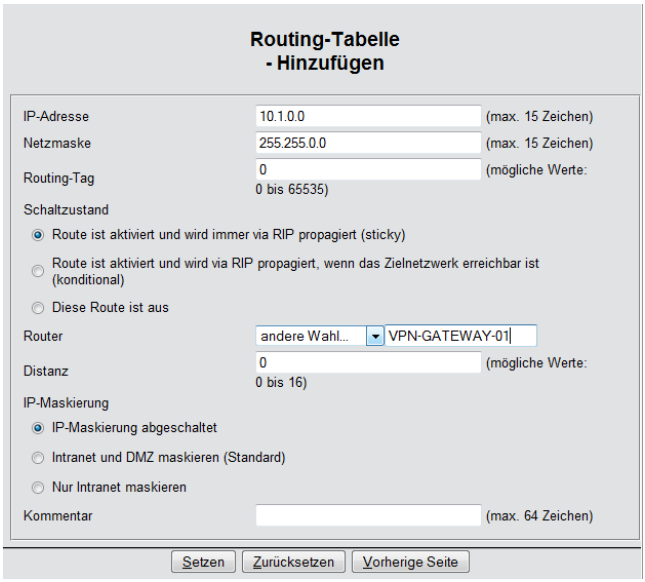
4. Bei Nutzung von Dynamic VPN: Erstellen Sie unter **Konfiguration** / **Setup** / **WAN** / **PPP** einen neuen Eintrag.

   Wählen Sie als Gegenstelle das entfernte VPN-Gateway aus, tragen Sie als Benutzernamen denjenigen VPN-Verbindungsnamen ein, mit dem das entfernte VPN-Gateway das lokale Gerät erreichen soll, und geben Sie geeignetes, auf beiden Seiten identisches Passwort ein.



Aktivieren Sie auf jeden Fall das „IP-Routing“ und je nach Bedarf „NetBIOS über IP“.

5. Erstellen Sie unter **Konfiguration** / **Setup** / **IP-Router** / **IP-Routing-Tabelle** einen neuen Eintrag für jeden Netzbereich, der im entfernten und im lokalen LAN erreicht werden soll. Verwenden Sie dabei jeweils als Router das entfernte VPN-Gateway und schalten Sie das IP-Masquerading aus.



Für das „VPN-Gateway-2“ sind die folgenden Einträge erforderlich, damit die entfernten Netzabschnitte erreicht werden:

IP-Adresse	*Netzmaske*	*Router*	*IP-Masquerading*
10.1.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.2.0.0	255.255.0.0	VPN-Gateway-1	Nein
10.3.0.0	255.255.0.0	VPN-Gateway-1	Nein

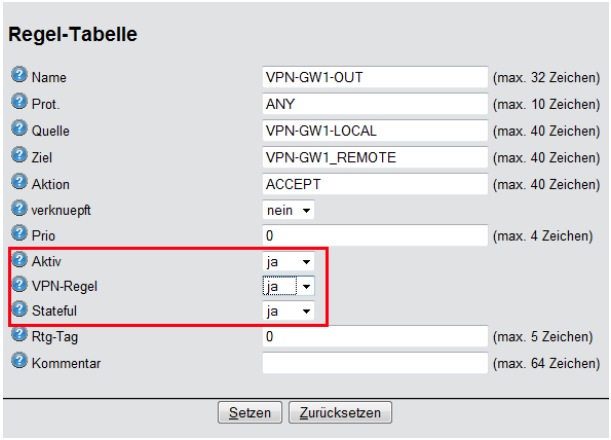
Für die an das eigene LAN angebundenen Teilnetze wird als Router die IP-Adresse des jeweiligen LAN-Routers eingetragen:

IP-Adresse	*Netzmaske*	*Router*	*IP-Masquerading*
10.5.0.0	255.255.0.0	10.4.0.5	Nein

Mit diesen Einträgen ist das VPN-Gateway 2 in der Lage, auch die aus dem entfernten Netz eintreffenden Pakete für die angebundenen Netzabschnitte richtig weiterzuleiten.

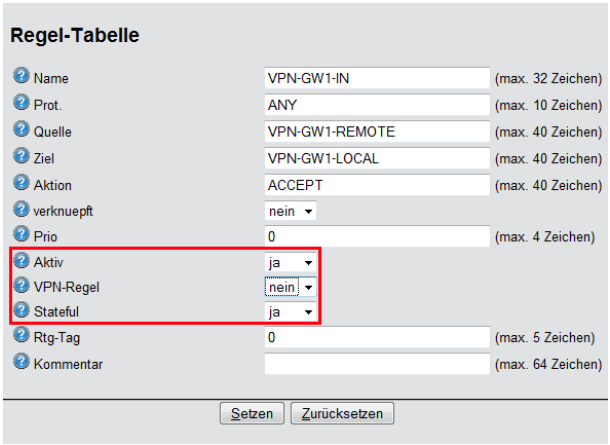
6. Erstellen Sie unter **Konfiguration** / **Firewall/QoS** / **Objekt-Tabelle** jeweils einen Eintrag für die Netzbereiche, die bei der VPN-Verbindung mit „VPN-GATEWAY-1“ als Quelle oder Ziel verwendet werden sollen („VPN-GW1-LOCAL“ und „VPN-GW1-REMOTE“). Geben Sie dabei die Netzbereiche z. B. in der Form „%A10.1.0.0 %M255.255.0.0“ ein.

7. Erstellen Sie unter **Konfiguration** / **Firewall/QoS** / **Regel-Tabelle** eine neue Firewall-Regel mit dem Namen „VPN-GW1-OUT“. Verwenden Sie dabei die Objekte „VPN-GW1-LOCAL“ und „VPN-GW1-REMOTE“, die Protokolle „ANY“ und die Aktion „ACCEPT“. Aktivieren Sie die Option „VPN-Regel“, damit die in dieser Regel beschriebenen IP-Netzwerke für die Bildung von VPN-Netzbeziehungen verwendet werden.



Hinweis: In der Regel empfiehlt sich die Trennung von Regeln, mit denen die VPN-Netzbeziehungen gebildet werden, und den Firewall-Regeln, die Auswirkungen z. B. auf die bei der Kommunikation zugelassenen Dienste haben.

1. Für die eingehende Datenübertragung erstellen Sie eine Firewall-Regel unter dem Namen „VPN-GW1-IN“ mit den gleichen Parametern wie die vorherige Regel. Nur bei den Stationen sind hier die Quell- und Zielnetze vertauscht:



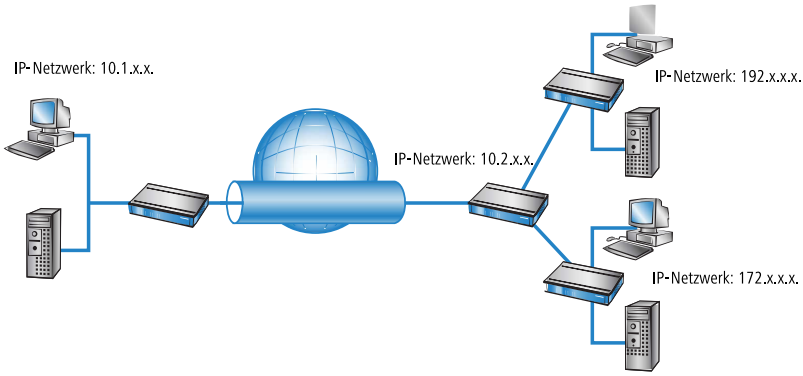
10.5.11 Gemeinsamer Aufbau von Security Associations

Die Basis für den Aufbau eines VPN-Tunnels zwischen zwei Netzwerken stellen die „Security Associations“ (SAs) dar. In einer SA sind u.a. folgende Parameter definiert:

- IP-Adressen von Quell- und Zielnetzwerk
- Verfahren zur Verschlüsselung, Integritätsprüfung und Authentifizierung
- Schlüssel für die Verbindung
- Gültigkeitsdauer der verwendeten Schlüssel

Die Security Associations werden durch automatisch oder manuell erzeugte VPN-Regeln definiert.

Der Aufbau der Security Associations wird normalerweise durch ein IP-Paket angestossen, das vom Quell- ins Zielnetz übertragen werden soll. Im Fall von Keep-Alive-Verbindungen ist dies ein ICMP-Paket, daß durch einen Eintrag in der Polling-Tabelle an die Gegenstelle verschickt wird.



In komplexen Netzwerk-Szenarien kommt es vor, dass zwischen zwei VPN-Gateways mehrere Netzbeziehungen definiert sind. Wird nun ein einzelnes IP-Paket übertragen, dann werden auch nur die SAs für genau diese eine, auf dieses Paket passende Netzbeziehung aufgebaut. Zum Aufbau der anderen SAs werden wiederum zu den anderen Netzbeziehungen passende IP-Pakete benötigt.

Der Aufbau von SAs aufgrund von Datenpaketen benötigt zum einen Zeit und zum anderen führt es zu Paketverlusten, solange die SAs noch nicht installiert sind. Aber gerade das ist – insbesondere bei Keep-Alive Verbindungen – oft nicht gewünscht. Stattdessen sollen **alle** SAs **sofort** aufgebaut werden, die zu den in der Gegenstelle definierten Netzbeziehungen passen. Da aber das Aushandeln aller SAs gerade in komplexen Szenarien viel CPU-Leistung benötigt, kann das Verhalten über den Parameter „SA-Aufbau-gemeinsam“ festgelegt werden.

- SA-Aufbau-gemeinsam
  - Ja: Alle im Gerät definierten SAs werden aufgebaut.
  - Nein [Default]: Nur die explizit durch ein zu übertragenes Paket angesprochene SA wird aufgebaut.
  - nur-bei-KeepAlive: Alle definierten SAs werden aufgebaut, für deren Gegenstelle in der VPN-Verbindungsliste eine Haltezeit von '9999' eingestellt ist (Keep Alive).

  WEBconfig: HiLCOS-Menübaum / Setup / VPN

  Hinweis: Die Voreinstellung für den ausschließlichen Aufbau von explizit angesprochenen SAs reicht in den meisten Fällen aus, insbesondere wenn nur automatisch erzeugte VPN-Regeln verwendet werden.

  Die aktuell vorhandenen SAs können unter /Status/VPN eingesehen werden.

10.5.12 Diagnose der VPN-Verbindungen

Wenn die VPN-Verbindungen nach der Konfiguration der entsprechenden Parameter nicht wie gewünscht zustande kommen, stehen folgende Möglichkeiten zur Diagnose zur Verfügung:

- Mit dem Befehl **show vpn spd** an der Telnet-Konsole rufen Sie die “Security Policy Definitions” auf.
- Mit dem Befehl **show vpn sadb** rufen Sie die Informationen über die ausgehandelten “Security Associations” (SAs) auf.
- Mit dem Befehl **trace + vpn** [status, packet] können Sie die Status- und Fehlermeldungen der aktuellen VPN-Verhandlung aufrufen.

- Die Fehlermeldung “No proposal chosen” deutet auf einen Fehler in der Konfiguration der Gegenstelle hin.
- Die Fehlermeldung “No rule matched” deutet hingegen auf einen Fehler in der Konfiguration des lokalen Gateways hin.

In der Standardeinstellung behält das Gerät VPN-Fehlermeldungen in der Statustabelle. Nach einiger Zeit zeigt der LANmonitor je nach Installation sehr viele offene Fehlermeldungen an, was die Anzeige unübersichtlich macht. Sie haben deshalb im WEBconfig unter **Setup** > **Config** > **Error-Aging-Minutes** die Möglichkeit, eine Zeitspanne in Minuten zu definieren, nach der das Gerät diese Fehlermeldungen automatisch aus der Statustabelle entfernt.

Hinweis: Um sporadisch auftretende Fehler zu dokumentieren, deaktivieren Sie diese Option mit dem Eintrag `0`.

10.6 Einsatz von digitalen Zertifikaten

Die Sicherheit der Kommunikation über VPN erfüllt im Kern drei Anforderungen:

- Vertraulichkeit: Die übertragenen Daten können von keinem Unbefugten gelesen werden (über Verschlüsselung).
- Integrität: Die Daten können während der Übertragung nicht unbemerkt verändert werden (über Authentifizierung).
- Authentizität: Der Empfänger kann sicher sein, dass die empfangenen Daten auch tatsächlich vom vermuteten Absender stammen (über Authentifizierung).

Für die Verschlüsselung und Authentifizierung von Daten stehen zahlreiche Verfahren zur Verfügung, mit denen die beiden ersten Aspekte – Vertraulichkeit und Integrität – ausreichend abgedeckt werden können. Der Einsatz von digitalen Zertifikaten verfolgt das Ziel, auch die Authentizität der Kommunikationspartner zu sichern.

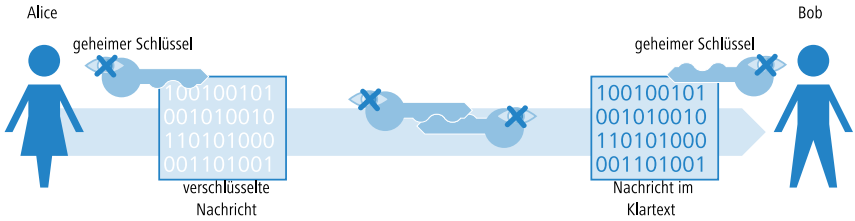
10.6.1 Grundlagen

Verschlüsselungsverfahren kann man in zwei Kategorien einteilen: Die symmetrische und die asymmetrische Verschlüsselung.

Die symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist seit Jahrtausenden bekannt und basiert darauf, dass sowohl der Sender als auch der Empfänger einer Nachricht über einen gemeinsamen, geheimen Schlüssel verfügen. Dieser Schlüssel kann sehr unterschiedliche Gestalt haben: Die Römer verwendeten zum Ver- und Entschlüsseln z. B. einen Stab mit einem ganz bestimmten Durchmesser.

In der heutigen digitalen Kommunikation handelt es sich bei dem Schlüssel meist um ein besonderes Passwort. Mit Hilfe dieses Passwortes und eines Verschlüsselungsalgorithmus werden die Daten vom Sender verändert. Der Empfänger verwendet den gleichen Schlüssel und einen passenden Entschlüsselungsalgorithmus, um die Daten wieder lesbar zu machen. Jede andere Person, die den Schlüssel nicht kennt, kann die Daten nicht lesen. Ein übliches symmetrisches Verschlüsselungsverfahren ist z. B. 3DES.



Beispiel:

- Alice möchte Bob eine vertrauliche Nachricht zukommen lassen. Dazu verschlüsselt sie die Nachricht mit einem geheimen Schlüssel und einem geeigneten Verfahren, z. B. 3DES. Die verschlüsselte Nachricht schickt sie an Bob und teilt ihm dabei mit, welches Verschlüsselungsverfahren sie verwendet hat.
- Bob verfügt über den gleichen Schlüssel wie Alice. Da er von Alice nun auch das Verschlüsselungsverfahren kennt, kann er die Nachricht entschlüsseln und in den Klartext zurückverwandeln.

Die symmetrische Verschlüsselung ist sehr einfach und effizient in der Handhabung, hat aber zwei gravierende Nachteile:

- Für jede geheime Kommunikationsbeziehung wird ein eigener Schlüssel benötigt. Wenn neben Alice und Bob noch Carol dazukommt, werden

schon drei Schlüssel benötigt, um die jeweiligen Datenübertragungen untereinander abzusichern, bei vier Teilnehmern sechs Schlüssel, bei 12 Teilnehmern 66 und bei 1000 Teilnehmern schon fast 500.000! In einem weltweiten Netz mit immer höheren Anforderungen an die gesicherte Kommunikation zahlreicher Teilnehmer wird das schon zu einem ernsthaften Problem.

- Während der erste Nachteil mit Hilfe der Technik evtl. zu lösen wäre, ist der Zweite ein Kernproblem der symmetrischen Verschlüsselung: Der geheime Schlüssel muss auf beiden Seiten der Datenübertragung bekannt sein und darf nicht in unbefugte Hände geraten. Alice kann den Schlüssel also nicht einfach per E-Mail an Bob schicken, bevor die Datenverbindung ausreichend gesichert ist, wozu genau dieser Schlüssel beitragen soll. Sie müsste den Schlüssel schon persönlich an Bob übergeben oder ihn zumindest über ein „abhörsicheres“ Verfahren übermitteln. Diese Aufgabe ist in Zeiten weltweiter dynamischer Datenkommunikation kaum zu bewältigen.

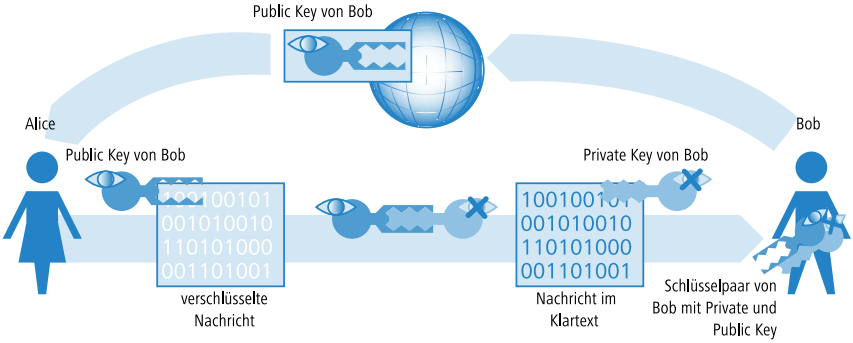
Das Verfahren der asymmetrischen Verschlüsselung

Als grundlegend neuer Ansatz wurde in den 1970er Jahren die asymmetrische Verschlüsselung entwickelt. Diese Variante setzt nicht mehr auf einen Schlüssel, der auf beiden Seiten bekannt und dabei geheim ist, sondern auf ein Schlüsselpaar:

- Der erste Teil des Schlüsselpaares wird zum **Ver**schlüsseln der Daten verwendet, die zum Eigentümer des Schlüssels gesendet werden. Dieser öffentliche Schlüssel (oder im Folgenden Public Key genannt) darf weltweit allen Interessenten öffentlich zur Verfügung gestellt werden.
- Der zweite Teil des Schlüsselpaares ist der private Schlüssel (Private Key), der nur zum **Ent**schlüsseln der empfangenen Botschaften verwendet wird. Dieser Schlüssel ist geheim und darf nicht in die Hände Unbefugter geraten.

Der große Unterschied gegenüber den symmetrischen Verschlüsselungen: Es wird ein öffentlich bekannter Schlüssel verwendet, daher spricht man hier auch vom „Public-Key-Verfahren“. Ein bekanntes asymmetrisches Verschlüsselungsverfahren ist z. B. RSA.

Sehen wir uns wieder das Beispiel von Alice und Bob an:



- Bob erzeugt für die gesicherte Kommunikation zunächst ein Schlüsselpaar mit einem Private Key und einem Public Key, die genau zueinander passen. Beim Erstellen dieser Schlüssel wird ein Verfahren verwendet, mit dem der Private Key nicht aus dem Public Key zurückgerechnet werden kann. Den Public Key kann Bob jetzt unbedenklich öffentlich bekannt machen. Er kann ihn per Mail an Alice schicken oder einfach auf seinem Webserver ablegen.
- Alice verschlüsselt nun die Nachricht an Bob mit dessen Public Key. Die so unkenntlich gemachte Botschaft kann nur noch mit dem Private Key von Bob entschlüsselt werden. Selbst wenn die Daten auf dem Weg von Alice zu Bob mitgehört werden, kann niemand außer Bob den Klartext entziffern!

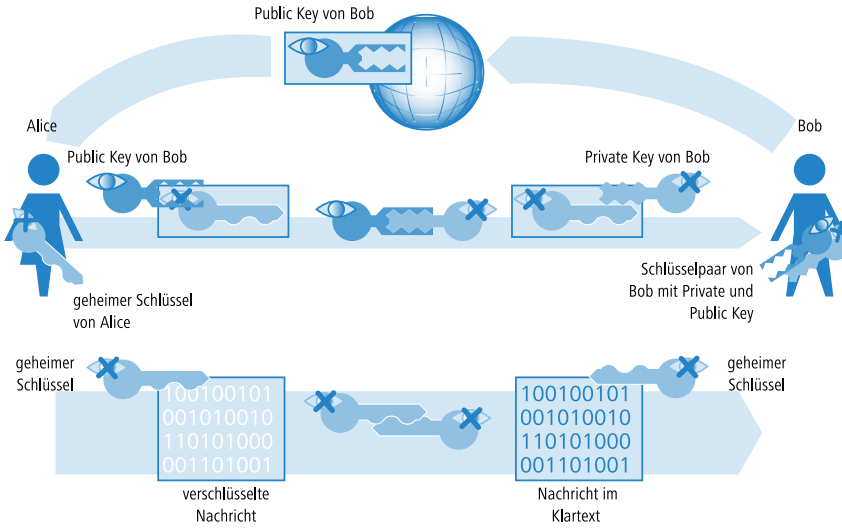
Die asymmetrische Verschlüsselung bietet gegenüber der symmetrischen Variante folgende Vorteile:

- Es wird nicht für jede Kommunikationsbeziehung ein Schlüsselpaar benötigt, sondern nur für jeden Teilnehmer. Bei 1000 Teilnehmern benötigt jeder nur sein eigenes Schlüsselpaar, von dem er den Public Key öffentlich zur Verfügung stellt. Anstelle der 500.000 geheimen Schlüssel werden beim Public Key-Verfahren also nur 1000 Schlüsselpaare verwendet.
- Die unsichere Übertragung des geheimen Schlüssels an die Kommunikationspartner entfällt, da nur der Public Key auf der jeweils anderen Seite der Kommunikationsbeziehung bekannt sein muss. Damit wird ein wesentliches Problem bei der dynamischen Verschlüsselung von Daten zwischen vielen Teilnehmern gelöst.

Kombination von symmetrischer und asymmetrischer Verschlüsselung

Aufgrund Ihrer Sicherheit konnten sich asymmetrische Verschlüsselungsverfahren schnell etablieren. Doch hat die Sicherheit auch Ihren Preis: Asymmetrische Verschlüsselungsverfahren sind langsam. Die mathematischen Verfahren zum Ver- und Entschlüsseln von Nachrichten sind sehr viel aufwändiger als bei symmetrischen Verschlüsselungsverfahren und brauchen daher auch mehr Rechenzeit, was bei der Übertragung von großen Datenmengen zum Ausschlusskriterium wird.

Die Vorteile von symmetrischer und asymmetrischer Verschlüsselung können in einer geeigneten Kombination ausgenutzt werden. Dabei wird die sichere asymmetrische Verschlüsselung dazu verwendet, die Übertragung des geheimen Schlüssels zu schützen. Die eigentlichen Nutzdaten der Verbindung werden anschließend mit den schnelleren symmetrischen Verfahren verschlüsselt.



- Bob erstellt im ersten Schritt sein Schlüsselpaar und stellt den Public Key öffentlich bereit.

- Alice verwendet den Public Key, um damit einen geheimen, symmetrischen Schlüssel zu **ver**schlüsseln und schickt ihn an Bob. Dieser geheime Schlüssel wird bei jeder Übertragung durch ein Zufallsverfahren neu bestimmt.
- Nur Bob kann den geheimen Schlüssel nun wieder mit Hilfe seines Private Keys **ent**schlüsseln.
- Alice und Bob verwenden dann den geheimen Schlüssel zum **Ver**- und **Ent**schlüsseln der deutlich größeren Nutzdaten-Volumina.

Public-Key-Infrastructure

Die Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren erlaubt es, auch über zunächst ungesicherte Verbindungen eine sichere Datenkommunikation aufzubauen. Dabei wurde bisher der Aspekt der Authentizität nicht beleuchtet: Woher weiß Alice, dass der verwendete Public Key auch tatsächlich von Bob stammt? Die Verwendung von Public-Keys hängt also vom Vertrauen an die Authentizität der Kommunikationspartner ab.

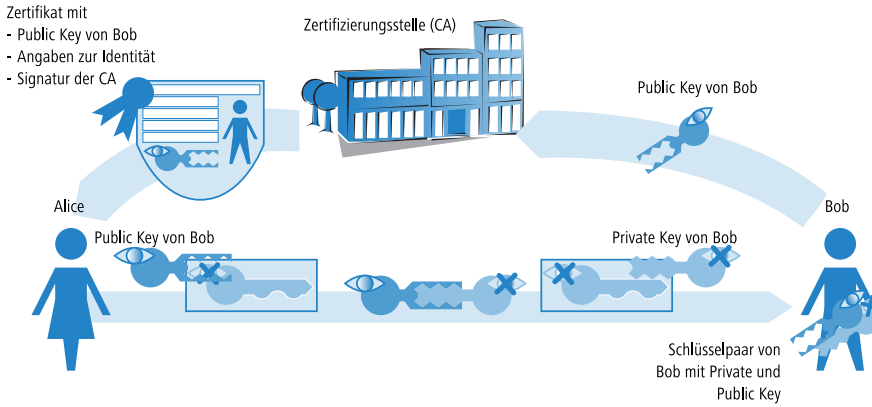
Um dieses Vertrauen zu sichern, können die verwendeten Schlüsselpaare der asymmetrischen Verschlüsselung von öffentlich anerkannten, vertrauenswürdigen Stellen bestätigt werden. So ist z. B. in Deutschland die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen die oberste vertrauenswürdige Instanz bei der Bestätigung von digitalen Schlüsseln. Diese wiederum vergibt Akkreditierungen an geeignete Dienstleister, die ebenfalls als vertrauenswürdig angesehen werden.

Hinweis: Auf der Webseite der Bundesnetzagentur (www.bundesnetzagentur.de) finden Sie ständig aktuelle Listen mit akkreditierten Zertifizierungsdiensteanbietern sowie Hinweise auf widerrufene Akkreditierungen. Unter den akkreditierten Dienstleistern befinden sich z. B. zahlreiche Steuerberater und Anwaltskammern.

Die Aufgabe dieser Stellen ist es, einen Public Key genau einer Person oder Organisation zuzuordnen. Diese Zuordnung wird in einem bestimmten Dokument – einem Zertifikat – festgehalten und öffentlich bekannt gemacht. Diese Anbieter werden daher auch als Zertifizierungsstellen bezeichnet, im Englischen als „Certification Authority“ oder kurz CA bezeichnet. Die oberste Zertifizierungsstelle gilt als die Stamm oder Wurzel-CA bzw. Root-CA.

An eine solche CA kann sich Bob nun wenden, wenn er seinen Public Key für seine eigene Person zertifizieren lassen möchte. Dazu reicht er seinen Public Key bei der CA ein, die die Zugehörigkeit des Schlüssels zu Bob bestätigt.

Die CA stellt über diese Bestätigung ein Zertifikat aus, das neben dem Public Key von Bob auch weitere Angaben u.a. über seine Identität enthält.



Das Zertifikat selbst wird von der CA wiederum signiert, damit auch die Bestätigung nicht angezweifelt werden kann. Da das Zertifikat nur aus einer kleinen Datenmenge besteht, kann dazu ein asymmetrisches Verfahren verwendet werden. Bei der Signatur wird das asymmetrische Verfahren jedoch in umgekehrter Richtung eingesetzt:

- Auch die CA verfügt über ein Schlüsselpaar aus Private und Public Key. Als vertrauenswürdige Stelle kann ihr eigenes Schlüsselpaar als zuverlässig angesehen werden.
- Die CA berechnet einen Hash-Wert über das Zertifikat, verschlüsselt diesen und signiert damit das Zertifikat von Bob. Dadurch wird die Zuordnung von Bobs Public Key zu seiner Identität bestätigt.

  Dieser Vorgang verhält sich genau umgekehrt wie bei der normalen asymmetrischen Verschlüsselung. Hier hat die Verschlüsselung aber nicht die Aufgabe, die Daten vor Unbefugten zu sichern, sondern die Signatur der CA zu bestätigen.

- Jeder Teilnehmer einer Datenkommunikation weltweit ist nun mit dem Public Key der CA in der Lage, das so signierte Zertifikat zu überprüfen.

  Nur die CA kann mit ihrem eigenen Private Key Signaturen erzeugen, die mit dem Public Key der CA wieder entschlüsselt werden können. Durch diese Signatur ist sichergestellt, dass das Zertifikat tatsächlich von der ausstellenden CA stammt.

10.6.2 Vorteile von Zertifikaten

Die Verwendung von Zertifikaten zur Absicherung von VPN-Verbindungen bietet sich in manchen Fällen als Alternative zum sonst eingesetzten Preshared-Key-Verfahren (PSK-Verfahren) an:

- Sicherere VPN-Client-Verbindungen (mit IKE Main Mode)

  Beim PSK-Verbindungsaufbau von Peers mit dynamischen IP-Adressen kann der Main Mode nicht eingesetzt werden. Hier muss der Aggressive Mode mit geringerer Sicherheit verwendet werden. Der Einsatz von Zertifikaten erlaubt auch bei Peers mit dynamischen IP-Adressen wie z. B. Einwahlrechnern mit LANCOM Advanced VPN Client die Verwendung des Main Mode und damit eine Steigerung der Sicherheit.

- Höhere Sicherheit der verwendeten Schlüssel bzw. Kennwörter

  Preshared Keys sind genau so anfällig wie alle anderen Kennwörter auch. Der Umgang der Anwender mit diesen Kennwörtern („menschlicher Faktor“) hat also erheblichen Einfluss auf die Sicherheit der Verbindungen. Bei einem zertifikatsbasierten VPN-Aufbau werden die in den Zertifikaten verwendeten Schlüssel automatisch mit der gewünschten Schlüssellänge erstellt. Darüber hinaus sind die von Rechnern erstellten, zufälligen Schlüssel auch bei gleicher Schlüssellänge sicherer gegen Angriffe (z. B. Wörterbuchangriffe) als die von Menschen erdachten Preshared Keys.

- Prüfung der Authentizität der Gegenseite möglich

  Beim VPN-Verbindungsaufbau über Zertifikate müssen sich die beiden Gegenstellen authentifizieren. In den Zertifikaten können dabei weitere Info-Elemente enthalten sein, die zur Prüfung der Gegenstellen herangezogen werden. Die zeitliche Befristung der Zertifikate gibt zusätzlichen Schutz z. B. bei der Vergabe an Anwender, die nur vorübergehend Zugang zu einem Netzwerk erhalten sollen.

- Unterstützung von Tokens und Smartcards

  Mit der Auslagerung der Zertifikate auf externe Datenträger gelingt auch die Integration in „Strong Security“-Umgebungen, das Auslesen von Kennwörtern aus Computern oder Notebooks wird verhindert.

Den Vorteilen von Zertifikaten steht allerdings der höhere Aufwand für die Einführung und Pflege einer Public Key Infrastructure (PKI) gegenüber.

10.6.3 Aufbau von Zertifikaten

Inhalte

Um seinen Aufgaben gerecht werden zu können, enthält ein Zertifikat diverse Informationen. Einige davon sind verpflichtend, andere sind optional. Es gibt verschiedene Formate, in denen ein Zertifikat gespeichert werden kann. Ein Zertifikat nach dem X.509-Standard beinhaltet z. B. folgende Informationen:

- Version: Dieser Eintrag enthält die Version des X.509-Standards. Die derzeit (06/2005) aktuelle Version ist 'v3'.
- Serial Number: Eine eindeutige Seriennummer, über die ein Zertifikat identifiziert werden kann.
- Signature Algorithm: Identifiziert den Algorithmus, mit dem der Aussteller das Zertifikat unterschreibt. Außerdem findet sich hier die digitale Unterschrift des Ausstellers.
- Validity: Zertifikate sind zeitlich begrenzt gültig. Validity enthält Informationen über die Dauer.
- Issuer: Daten zur Identifizierung des Ausstellers, z. B. Name, Email-Adresse, Nationalität etc.
- Subject: Daten zur Identifizierung des Eigentümers des Zertifikates, z. B. Name, Institution, Email-Adresse, Nationalität, Stadt etc.
- Subject Public Key: Informationen, welches Verfahren zum Generieren des öffentlichen Schlüssels des Zertifikatsinhabers verwendet wurde. Außerdem findet sich unter diesem Punkt der Public Key des Eigentümers.

Zielanwendung

Bei der Erstellung der Zertifikate wird üblicherweise ausgewählt, für welchen Zweck die Zertifikate eingesetzt werden können. Manche Zertifikate sind gezielt nur für Webbrowser oder E-Mail-Übertragung gedacht, andere sind allgemein für beliebige Zwecke einsetzbar.

Hinweis: Achten Sie bei der Erstellung der Zertifikate darauf, dass sie für den gewünschten Zweck ausgestellt werden.

Formate

Für die Form der Zertifikate ist der ITU-Standard X.509 weit verbreitet. In Textdarstellung sieht ein solches Zertifikat z. B. wie folgt aus:

```
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number: 1 (0x1)
 Signature Algorithm: md5WithRSAEncryption
 Issuer: CN=CA/Email=ca@trustme.dom, OU=Certificate Authority, O=TrustMe
Ltd, ST=Austria, L=Graz, C=XY,
 Validity
 Not Before: Oct 29 17:39:10 2000 GMT
 Not After : Oct 29 17:39:10 2001 GMT
 Subject: CN=anywhere.com/Email=xyz@anywhere.com, OU=Web Lab, O=Home,
L=Vienna, ST=Austria, C=DE
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 RSA Public Key: (1024 bit)
 Modulus (1024 bit):
 00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
 d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
 9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
 90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
 1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
 7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
 50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
 8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
 f0:b4:95:f5:f9:34:9f:f8:43
 Exponent: 65537 (0x10001)
```

```
X509v3 extensions:
X509v3 Subject Alternative Name:
email:xyz@anywhere.com
Netscape Comment:
mod_ssl generated test server certificate
Netscape Cert Type:
SSL Server
Signature Algorithm: md5WithRSAEncryption
12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
ff:8e
```

Dateitypen

Digitale Zertifikate und Private Keys liegen je nach Aussteller mit verschiedenen Dateiendungen vor. Üblich sind z. B. die Endungen:

- *.pfx und *.p12: PKCS#12-Dateien
- *.pem, *.cer und *.crt: BASE-64-codierte Zertifikate
- *.cer, *.crt und *.der: DER-codierte Zertifikate
- *.key: BASE64- oder DER-codierte Schlüssel
- *.pvk: Microsoft-spezifisches Schlüsselformat

Im Umfeld der zertifikatsgesicherten VPN-Verbindungen ist neben den reinen Zertifikaten noch ein weiterer Dateityp von großer Bedeutung: die PCKS#12-Dateien, in denen mehrere Komponenten enthalten sein können, u.a. ein Zertifikat und ein Private Key. Zur Verarbeitung der PKCS#12-Dateien ist ein Kennwort erforderlich, das beim Exportieren der Zertifikate festgelegt wird.

Hinweis: BASE64-codierte Zertifikate tragen im Header üblicherweise die Zeile:

```
----- BEGIN CERTIFICATE -----
```

Gültigkeit

Darüber hinaus kann optional ein Verweis auf eine so genannte Certificate Revocation List (CRL) eingefügt werden. In CRL's sind Zertifikate aufgelistet, die ungültig geworden sind, z. B. weil ein Mitarbeiter eine Firma verlassen hat und sein Zertifikat deshalb zurückgezogen wurde. Mit dieser Angabe kann bei der Prüfung der Zertifikate die richtige CRL verwendet werden.

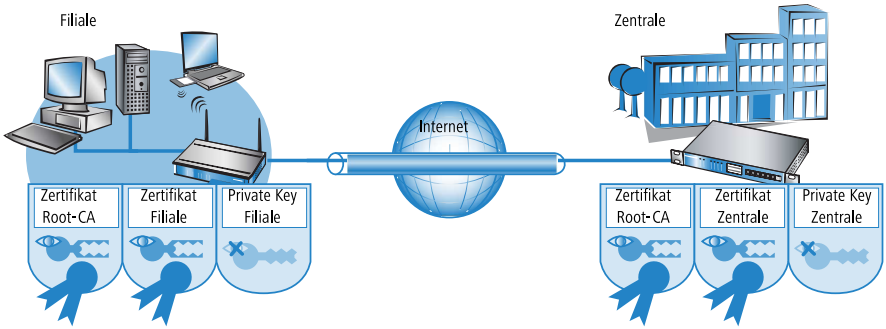
10.6.4 Sicherheit

Auch beim Umgang mit Zertifikaten sind bestimmte Sicherheitsaspekte zu beachten:

- Übertragen Sie die Private Keys nur über sichere Verbindungen, z. B. mit HTTPS.
- Verwenden Sie als Kennwörter für Schlüssel oder PKCS#12-Dateien nur ausreichend lange und sichere Passphrasen.

10.6.5 Zertifikate beim VPN-Verbindungsaufbau

Neben den grundlegenden Informationen zum Thema Zertifikate betrachten wir in diesem Abschnitt die konkrete Anwendung beim VPN-Verbindungsaufbau. Für einen solchen Verbindungsaufbau mit Zertifikatsunterstützung müssen auf beiden Seiten der Verbindung (z. B. Anbindung einer Filiale an das Netzwerk der Zentrale über einen Router) bestimmte Informationen vorhanden sein:



- Die Filiale verfügt über folgende Komponenten:
  - Zertifikat der Root-CA mit dem Public Key der CA
  - Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
  - Eigener Private Key
- Die Zentrale verfügt über folgende Komponenten:
  - Zertifikat der Root-CA mit dem Public Key der CA
  - Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
  - Eigener Private Key

Beim VPN-Verbindungsaustausch laufen vereinfacht dargestellt im Main Mode folgende Vorgänge ab (in beide Richtungen symmetrisch):

1. In einem ersten Paketaustausch handeln die Peers z. B. die verwendeten Verschlüsselungsmethoden und die Verfahren zur Authentifizierung aus. In dieser Phase haben beide Seiten noch keine gesicherte Kenntnis darüber, mit wem sie gerade verhandeln, das ist jedoch bis zu diesem Zeitpunkt nicht notwendig.
2. Im nächsten Schritt wird ein gemeinsames Schlüsselmaterial für die weitere Verwendung ausgehandelt, darin u.a. symmetrische Schlüssel und asymmetrische Schlüsselpaare. Auch in diesem Zustand können beide Seiten noch nicht sicher sein, mit wem sie die Schlüssel ausgehandelt haben.
3. Im nächsten Schritt wird mit Hilfe der Zertifikate geprüft, ob der Peer aus der Verhandlung des Schlüsselmaterials auch tatsächlich der beabsichtigte Kommunikationspartner ist:
   - Die Filiale errechnet aus dem Schlüsselmaterial der aktuellen Verhandlung eine Prüfsumme (Hash), die lediglich die beiden beteiligten Peers (Filiale und Zentrale) und nur während dieser Verbindung berechnen können.
   - Diesen Hash verschlüsselt die Filiale mit dem eigenen Private Key und erzeugt damit eine Signatur.
   - Diese Signatur übermittelt die Filiale zusammen mit dem eigenen Zertifikat dem Peer in der Zentrale.

- Die Zentrale prüft dann die Signatur für das empfangene Zertifikat der Filiale. Das kann sie mit Hilfe des Public Keys im Root-CA, welcher in beiden Peers identisch vorhanden ist. Kann die Signatur aus dem Filialen-Zertifikat (erstellt mit dem Private Key der CA) mit dem Public Key der CA entschlüsselt werden, dann ist die Signatur gültig und dem Zertifikat kann vertraut werden.
- Im nächsten Schritt prüft die Zentrale dann die Signatur der verschlüsselten Prüfsumme. Der Public Key der Filiale aus dem entsprechenden Zertifikat wurde im vorigen Schritt für gültig befunden. Daher kann die Zentrale prüfen, ob die signierte Prüfsumme mit dem Public Key der Filiale entschlüsselt werden kann. Die Zentrale kann die gleiche Prüfsumme aus dem Schlüsselmaterial der aktuellen Verbindung berechnen wie die Filiale. Wenn diese Prüfung erfolgreich ist, kann der Peer „Filiale“ als authentifiziert angesehen werden.

10.6.6 Zertifikate von Zertifikatsdiensteanbietern

Die von öffentlichen Zertifikatsstellen angebotenen Zertifikate können in der Regel in verschiedenen Sicherheitsklassen beantragt werden. Mit höherer Sicherheit steigt dabei jeweils der Aufwand des Antragstellers, sich gegenüber der CA mit seiner Identität zu authentifizieren. Die Trustcenter AG in Hamburg verwendet z. B. die folgenden Klassen:

- Class 0: Diese Zertifikate werden ohne Prüfung der Identität ausgestellt und dienen nur zu Testzwecken für Geschäftskunden.
- Class 1: Hier wird nur die Existenz einer E-Mail-Adresse geprüft. Diese Stufe eignet sich für private Anwender, die z. B. Ihre E-Mails signieren möchten.
- Class 2: Auch in dieser Stufe findet keine persönliche Identitätsprüfung statt. Die Übersendung eines Antrags mit einer Kopie z. B. eines Handelsregisterauszugs ist ausreichend. Diese Stufe eignet sich daher für die Kommunikation zwischen Unternehmen, die vorher untereinander bekannt sind.
- Class 3: In dieser Stufe wird die Person oder das Unternehmen persönlich überprüft. Dabei werden die Angaben in dem ausgestellten Zertifikat mit denen im Pass bzw. einer beglaubigten Kopie des Handelsregisterauszugs verglichen. Diese Stufe eignet sich für fortgeschrittene Anwendungen z. B. im e-Business oder Online-Banking.

Wenn Sie mit einem öffentlichen Zertifikatsdiensteanbieter zusammenarbeiten, prüfen Sie genau die angebotenen Sicherheitsstufen bzgl. der Prüfung der Identität. Nur so können Sie feststellen, ob die verwendeten Zertifikate auch tatsächlich Ihrer Sicherheitsanforderung entsprechen.

10.6.7 Aufbau einer eigenen CA

Die Nutzung von öffentlichen CAs ist für die sichere Unternehmenskommunikation nur bedingt empfehlenswert:

- Die Ausstellung von neuen Zertifikaten ist aufwändig und manchmal nicht schnell genug.
- Die verwendeten Schlüssel werden über unzureichend gesicherte Verbindungen übertragen.
- Die Kommunikation basiert auf dem Vertrauen gegenüber der CA.

Als Alternative eignet sich daher für die Unternehmenskommunikation der Aufbau einer eigenen CA. Hierfür bieten sich z. B. die Microsoft CA auf einem Microsoft Windows 2003 Server oder OpenSSL als OpenSource-Variante an. Mit einer eigenen CA können Sie ohne Abhängigkeit von fremden Stellen alle benötigten Zertifikate zur Sicherung des Datenaustauschs selbst erstellen und verwalten.

Der Einsatz einer eigenen CA ist für Unternehmen sicherlich eher zu empfehlen als die Nutzung öffentlicher Anbieter für Zertifizierungsdienste. Allerdings sind schon bei der Planung einer CA einige wichtige Punkte zu beachten. So werden z. B. schon bei der Installation einer Windows-CA die Gültigkeitszeiträume für die Root-CAs festgelegt, die nachträglich nicht mehr geändert werden können. Weitere Aspekte der Planung sind u.a.:

- Die Zertifikats-Policy, also die Sicherheitsstufe, die mit Hilfe der Zertifikate erreicht werden soll
- Der verwendete Namensraum
- Die Schlüssellängen
- Die Lebensdauer der Zertifikate
- Die Verwaltung von Sperrlisten

Eine genaue Planung zahlt sich auf jedem Fall aus, da spätere Korrekturen teilweise nur mit hohem Aufwand zu realisieren sind.

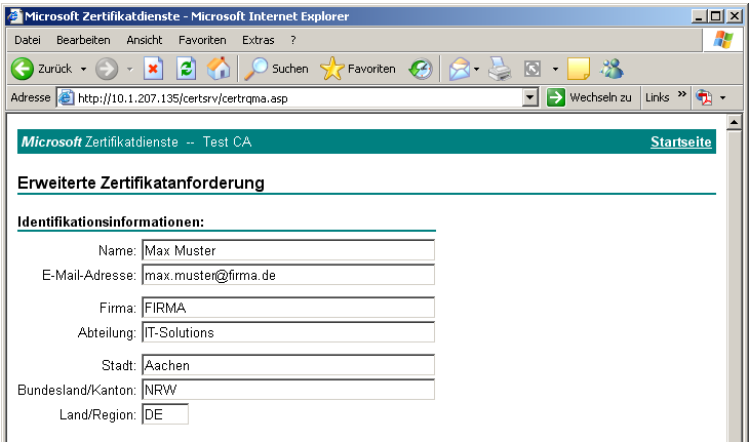
10.6.8 Anfordern eines Zertifikates mit der Stand-alone Windows CA

Hinweis: Für die Verwendung in einem Router leistet eine Kombination aus PKCS#12-Datei mit Root-Zertifikat, eigenem Geräte Zertifikat und Public Key des Gerätes die besten Dienste.

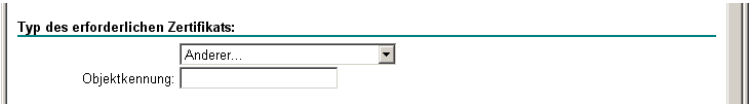
1. Rufen Sie in Ihrem Browser die Startseite des Microsoft Zertifikatsdienstes auf.
2. Wählen Sie als Zertifikatstyp die 'erweiterte Zertifikatanforderung'.
3. Wählen Sie im nächsten Schritt die Option 'Eine Anforderung an diese Zertifikatsstelle erstellen und einreichen'.

   Hinweis: Nur wenn das Root-Zertifikat schon in einer separaten Datei vorliegt, wählen Sie hier die Option 'BASE64'.

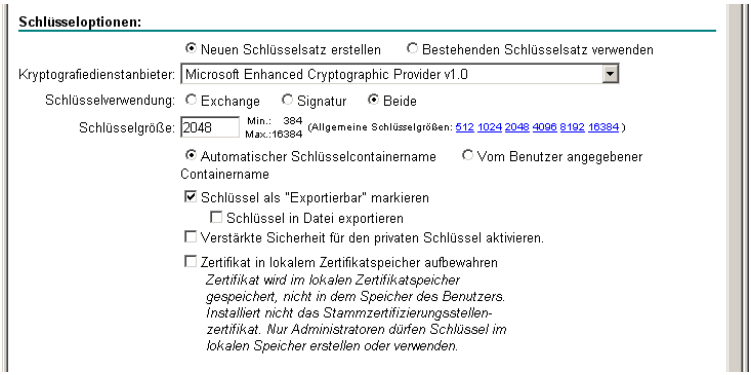
4. Im nächsten Schritt werden die Daten zur Identifikation eingetragen.



5. Wählen Sie im gleichen Dialog als Typ des Zertifikats die Option 'Anderer...' und löschen Sie den daraufhin erscheinenden Wert für die 'Objektkennung'.



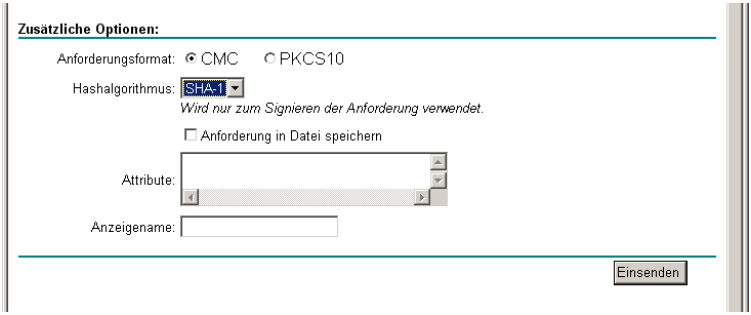
6. Markieren Sie die 'Automatische Schlüsselerstellung'. Damit werden Public und Private Key für den aktuellen Benutzer automatisch von der CA erstellt.



7. Wählen Sie eine geeignete Schlüssellänge (passend zur Zertifikats-Policy), aktivieren Sie die Option für exportierbare Schlüssel.

   Hinweis: Der Schlüssel wird an dieser Stelle nicht exportiert, daher muss auch kein Dateiname angegeben werden. Beim Exportieren würde eine Datei im Microsoft-spezifischen *.pvk-Format angelegt werden, die für die Weiterverarbeitung unter HiLCOS ungeeignet ist.

8. Wählen Sie zuletzt als Hash-Algorithmus 'SHA-1' und reichen Sie die Zertifikatanforderung mit **Einsenden** ein.



   Hinweis: Den Status der eingereichten Zertifikatanforderungen können Sie jederzeit über die Startseite der Windows-CA einsehen. Sie können die Zertifikatanforderungen nur vom gleichen Rechner aus einsehen, mit dem Sie die Anforderung eingereicht haben.

9. Sobald der Administrator der CA die Zertifikatanforderung geprüft und das Zertifikat erstellt hat, können Sie dieses auf Ihrem Rechner installieren.

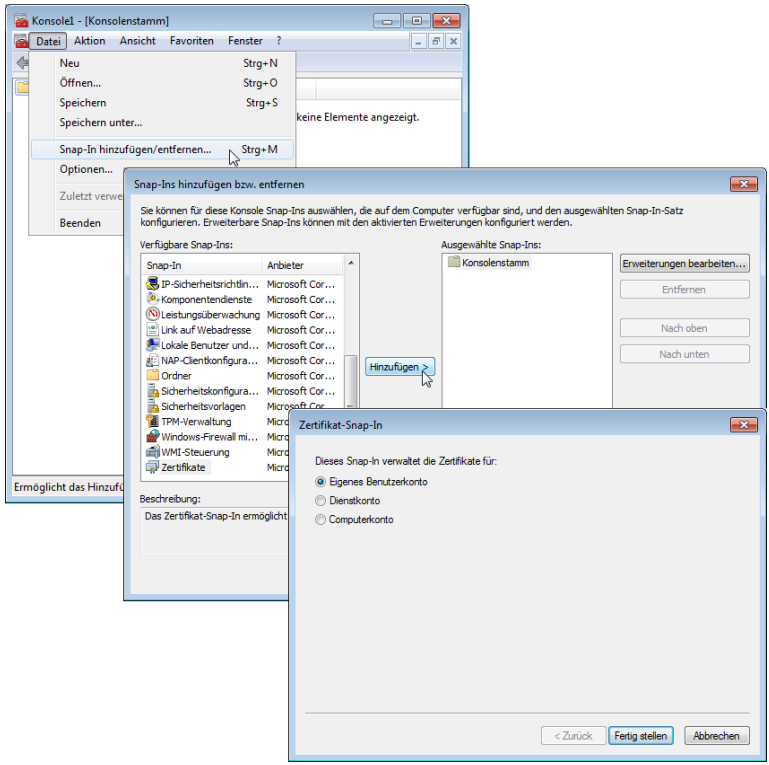
Hinweis: Sie können die Zertifikate nur auf dem gleichen Rechner installieren, mit dem Sie die Anforderung eingereicht haben.

10.6.9 Zertifikat in eine PKCS#12-Datei exportieren

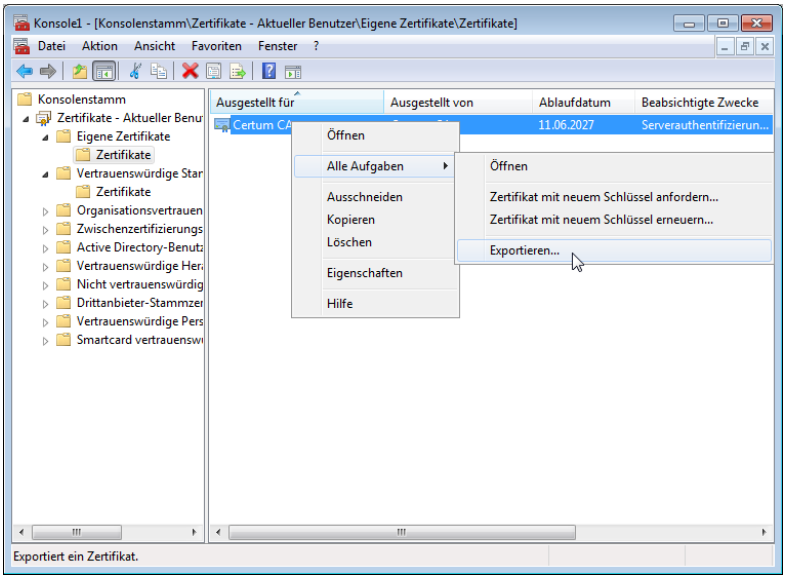
Mit der Installation wird das Zertifikat in Ihrem Betriebssystem gespeichert, es liegt noch nicht als separate Datei vor. Diese benötigen Sie jedoch für die Installation im Gerät. Um zu einem Zertifikat in Dateiform zu gelangen, müssen Sie es zunächst exportieren.

Export über den Windows-Konsolenstamm

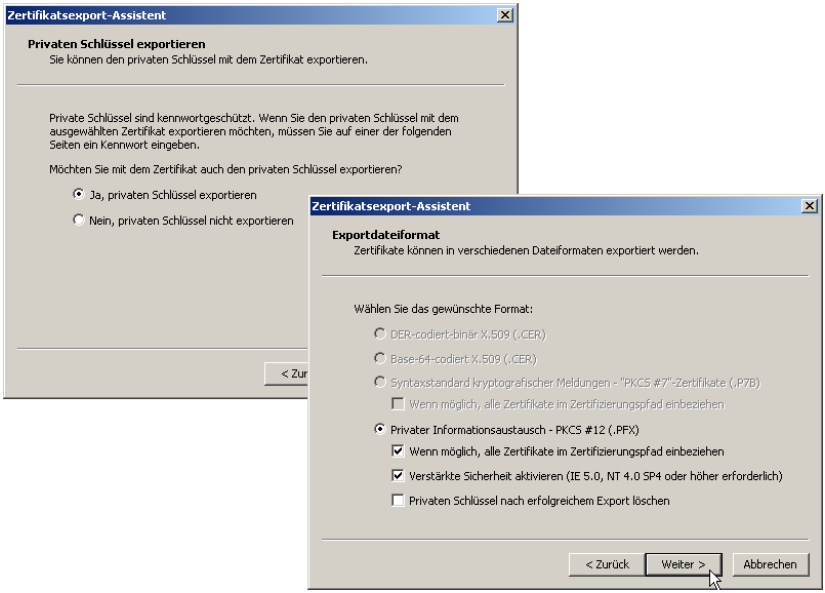
1. Öffnen Sie dazu die Management-Konsole über den Befehl `mmc` an der Eingabeaufforderung und wählen Sie den Menüpunkt **Datei** / **Snap-In hinzufügen/entfernen**.



2. Klicken Sie auf **Hinzufügen...** und wählen Sie den Eintrag 'Zertifikate'. Bestätigen Sie mit **Hinzufügen**, markieren Sie anschließend 'Eigenes Benutzerkonto' und klicken Sie auf **Fertig stellen**.
3. Um das gewünschte Zertifikat in eine Datei zu exportieren, klicken Sie anschließend in der Managementkonsole in der Gruppe **Zertifikate - Aktueller Benutzer** / **Eigene Zertifikate** / **Zertifikate** mit der rechten Maustaste und wählen im Kontextmenü den Eintrag **Alle Tasks** / **Exportieren**,



4. Aktivieren Sie im Verlaufe des Zertifikatsexportassistenten die Option zum Exportieren des privaten Schlüssels. Optional können Sie den privaten Schlüssel nach dem Export aus dem System löschen.



Hinweis: Die Option 'alle Zertifikate in den Zertifizierungspfad mit einbeziehen' muss aktiviert sein, damit das Root-Zertifikat mit in die PKCS#12-Datei exportiert wird.

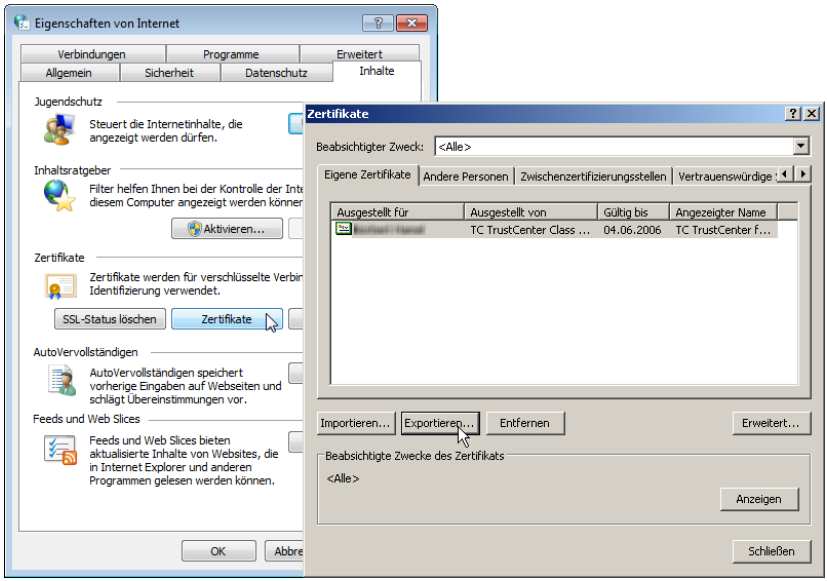
5. Beim Export werden Sie aufgefordert, ein Kennwort zum Schutz des privaten Schlüssels einzugeben. Wählen Sie hier ein sicheres Kennwort ausreichender Länge (Passphrase). Dieses Kennwort werden Sie bei der Installation der Zertifikate im Gerät wieder benötigen.

Hinweis: Für das Kennwort werden je nach Umgebung auch die synonymen Begriffe „Passwort“ oder „PIN“ verwendet.

Export über die Systemsteuerung

Alternativ können Sie die auf dem System installierten Zertifikate über die Systemsteuerung öffnen.

1. Wählen Sie dazu **Start** / **Systemsteuerung** / **Internetoptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.
2. Wählen Sie das gewünschte Zertifikat aus und klicken Sie auf **Exportieren**.



10.6.10 Zertifikate mit OpenSSL erstellen

Mit OpenSSL steht eine weitere Möglichkeit zur Verfügung, eigene Zertifikate zu erstellen und Zertifikats-Verbindungen zu testen. OpenSSL ist als Open-Source-Projekt kostenlos für Linux und Windows erhältlich, als Kommandozeilen-Tool jedoch auch weniger anwenderfreundlich als andere CA-Varianten.

Hinweis: Die Konfigurations-Datei openssl.cnf muss dabei an Ihre spezifischen Bedürfnisse angepasst werden. Nähere Informationen dazu finden Sie in der Dokumentation zu OpenSSL.

OpenSSL installieren

1. Laden Sie eine aktuelle OpenSSL-Version von http://www.slproweb.com/products/Win32OpenSSL.html.
2. Installieren Sie das Paket und erstellen Sie im Verzeichnis `./bin/PEM/demoCA` zusätzlich die Unterverzeichnisse:
   - `/certs`

- /newcerts
- /crl.

3. Ändern Sie in der Datei openssl.cnf den Pfad in der Gruppe [CA_default] auf: dir= ./PEM/demoCA
4. Starten Sie OpenSSL durch einen Doppelklick auf die openssl.exe im Verzeichnis ./bin.

Zertifikat für Root-CA ausstellen

1. Erstellen Sie einen Schlüssel für die CA mit dem Befehl:

   - genrsa -des3 -out ca.key 2048

   Hinweis: Merken Sie sich das Kennwort, das Sie nach der Aufforderung für den CA-Schlüssel eingeben, es wird später wieder benötigt!

   Dieser Befehl erstellt die Datei 'ca.key' im aktuellen Verzeichnis.

2. Erstellen Sie eine Zertifikatsanforderung (Request) für die CA mit dem Befehl:

   - req -key ca.key -new -subj /CN="Test_CA" -out ca.req

   Hinweis: Hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

   Dieser Befehl erstellt die Datei 'ca.req' im aktuellen Verzeichnis.

3. Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

   - x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt

   Hinweis: Auch hier werden Sie wieder zur Eingabe des Kennwortes für den CA-Schlüssel aufgefordert.

   Dieser Befehl signiert die Zertifikatsanforderung 'ca.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'ca.crt' aus.

Zertifikat für Benutzer oder Geräte ausstellen

1. Erstellen Sie einen Schlüssel für das Gerät oder den Benutzer mit dem Befehl:

   ▶ `genrsa -out device.key 2048`

   Dieser Befehl erstellt die Datei 'device.key' im aktuellen Verzeichnis.

2. Erstellen Sie eine Zertifikatsanforderung (Request) für das Gerät oder den Benutzer mit dem Befehl:

   ▶ req -key device.key -new -subj /CN=DEVICE -out device.req

   Dieser Befehl erstellt die Datei 'device.req' im aktuellen Verzeichnis.

   Hinweis: Neben diesem Befehl sind noch weitere Änderungen in der Datei „openssl.cnf“ zur Definition einer Extension notwendig.

3. Erstellen Sie ein Zertifikat aus der Zertifikatsanforderung mit dem Befehl:

   ▶ x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt

   Dieser Befehl signiert die Zertifikatsanforderung 'device.req' mit dem Schlüssel 'ca.key' und stellt damit das Zertifikat 'device.cert' aus. Zusätzlich wird dabei die Konfigurationsdatei openssl.cnf verwendet.

4. Exportieren Sie das Zertifikat für das Gerät oder den Benutzer mit dem Befehl:

   ▶ `pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12`

   Dieser Befehl fasst den Schlüssel 'device.key', das Geräte-Zertifikat 'device.crt' und das Root-Zertifikat 'ca.crt' zusammen und speichert sie gemeinsam in der Datei 'device.p12'. Diese PKCS#12-Datei können Sie direkt in das gewünschte Gerät laden.

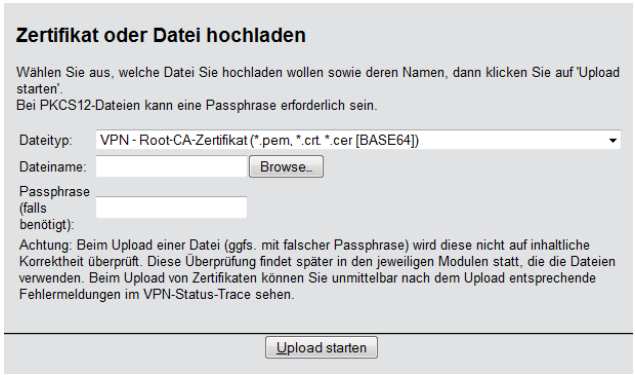
10.6.11 Zertifikate in das Gerät laden

Für den zertifikatgesicherten VPN-Verbindungsaufbau müssen in einem Gerät die folgenden Komponenten vorhanden sein:

- Zertifikat der Root-CA mit dem Public Key der CA
- Eigenes Geräte-Zertifikat mit dem eigenen Public Key und der Bestätigung der Identität. Die Prüfsumme dieses Zertifikats ist mit dem Private Key der CA signiert.
- Eigener Private Key

Sofern Sie die Anleitungen zur Ausstellung der Zertifikate über eine Windows-CA und den Export befolgt haben, liegen diese Informationen nun in Form einer gemeinsamen PKCS#12-Datei vor. Alternativ haben Sie ein anderes Verfahren verwendet und die einzelnen Komponenten liegen in separaten Dateien vor.

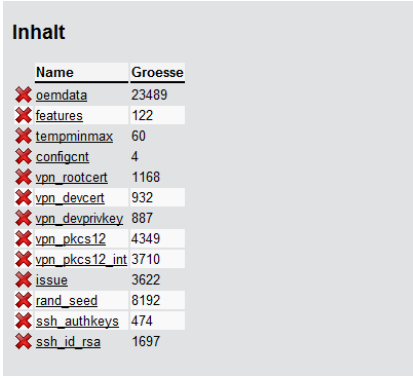
1. Melden Sie sich mit Administratorrechten über WEBconfig an dem gewünschten Gerät an.
2. Wählen Sie den Eintrag **Zertifikat oder Datei hochladen**.



3. Wählen Sie aus, welche Komponenten Sie in das Gerät laden wollen:
   - Root-Zertifikat
   - Geräte-Zertifikat
   - Private Key des Gerätes
   - PKCS#12-Datei mit einer Kombination aus Root-Zertifikat, Geräte-Zertifikat und Private Key

   Hinweis: Je nach Typ der hochgeladenen Datei muss ggf. das entsprechende Kennwort eingegeben werden.

Die hochgeladenen Dateien können anschließend in einer Liste unter **Expertenkonfiguration** / **Status** / **Datei-System** / **Inhalt** eingesehen werden.

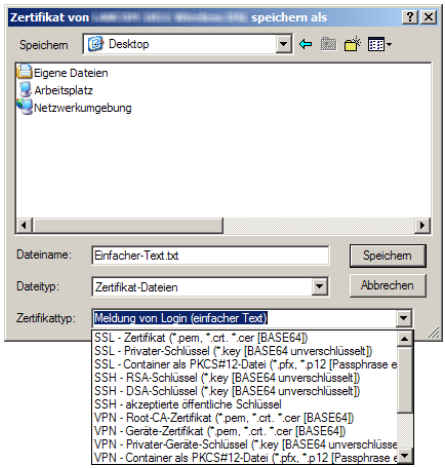


Hinweis: Eine kombinierte PKCS#12-Datei wird beim Upload automatisch in die benötigten Teile zerlegt.

10.6.12 Zertifikate sichern und hochladen mit LANconfig

In einem Gerät können unterschiedliche Zertifikate zur Verschlüsselung bestimmter Dienste verwendet werden. Diese Zertifikate können über LANconfig in die Geräte geladen werden. Außerdem können die im Gerät vorhandenen Zertifikate auch über LANconfig ausgelesen und in eine Datei gesichert werden.

1. Wählen Sie das Gerät aus, in das Sie ein Zertifikat einspielen bzw. aus dem Sie ein Zertifikat sichern wollen.
2. Klicken Sie die Auswahl mit der rechten Maustaste und wählen Sie im Kontextmenü **Konfigurations-Verwaltung** / **Zertifikat als Datei sichern** bzw. **Zertifikat als Datei hochladen**.

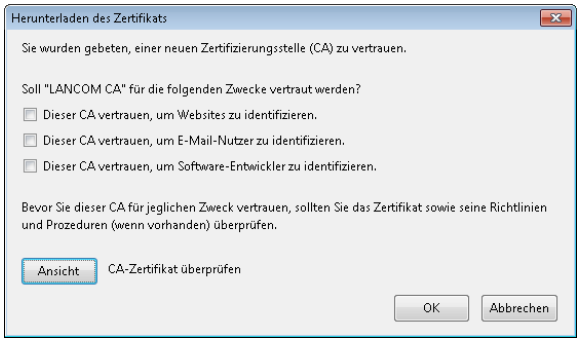


3. Wählen Sie Speicherort und den Typ des Zertifikats aus, der gesichert oder hochgeladen werden soll und bestätigen Sie die Auswahl mit **Speichern/Öffnen**.

Hinweis: Mit der Auswahl von mehreren Geräten kann durchaus eine Zertifikatsdatei in mehrere Geräte gleichzeitig hochgeladen werden. das gleichzeitige Sichern von Zertifikaten aus mehreren Geräten ist hingegen nicht möglich. Je nach Typ der Zertifikatsdatei ist beim Hochladen ggf. ein Kennwort (Passphrase) notwendig.

10.6.13 Downloadlink für den öffentlichen Teil des CA-Zertifikates

Sie können den öffentlichen Teil des CA-Zertifikates ohne Anmeldung über den Link `http://<URL>/getcacert/cacert.crt` herunterladen. Die Übertragung erfolgt mit dem Mime-Typ `application/x/x509-ca-cert`, so dass die verwendete Software je nach Fähigkeit die sofortige Installation des Zertifikates anbietet.



Hinweis: Der Download ist nur möglich bei aktivierter CA. Bei deaktivierter CA erscheint eine Fehlermeldung.

Bei aktivierter CA ist im WEBconfig der Zertifikats-Download auch über **Extras** > **Aktuelles CA Zertifikat herunterladen** möglich.

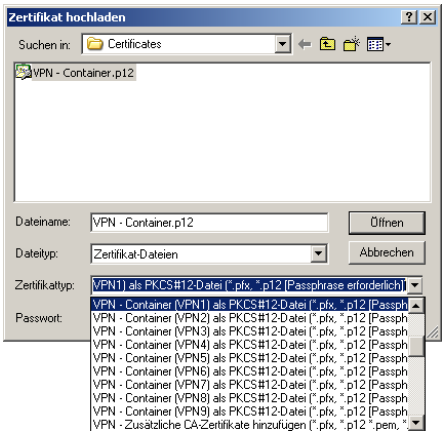
10.6.14 Erweiterte Zertifkats-Unterstützung

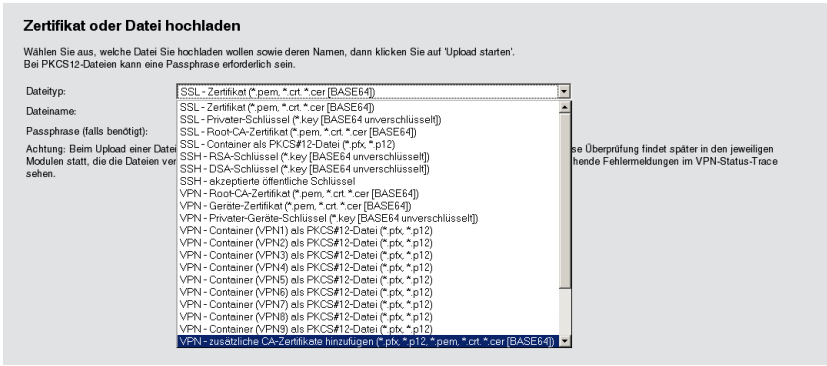
Mehrere Zertifikatshierarchien

Zur Unterstützung von mehreren Zertifikatshierarchien können ab der Firmware-Version 7.80 bis zu neun PKCS#12-Dateien in das Gerät geladen werden. Darüber hinaus können weitere Dateien mit zusätzlichen CA-Zertifikaten hochgeladen werden, in denen die Zertifikate einzeln oder als PKCS#12-Container enthalten sein können. Alle Zertifikatshierarchien können manuell oder per SCEP verwaltet werden und können CRLs verwenden.

LANconfig: Gerät / Konfigurations-Verwaltung / Zertifikat als Datei hochladen

WEBconfig: Dateimanagement / Zertifikat oder Datei hochladen





Die im Gerät vorhandenen Zertifikate können im Statusbereich eingesehen werden:

WEBconfig: HiLCOS-Menübaum / Status / Zertifikate / Geraetezertifikate

Die Gerätezertifikate werden im internen Dateisystem der Geräte den Verwendungszwecken “VPN1” bis “VPN9” zugeordnet.

Zur Nutzung der Zertifikate kann in den IKE-Schlüsseln mit dem Typ ASN.1-Distinguished Name als “lokale Identität” entweder das Subject des Zertifikats oder diese Kurzbezeichnung verwendet werden.

Hinweis: Durch die Referenzierung der Zertifikate über die Kurzbezeichnung können auch Subjects mit deutschen Umlauten oder anderen Sonderzeichen

verwendet werden, die ansonsten aufgrund der Einschränkungen der CLI-Konfiguration nicht angesprochen werden können.

Die Kurzbezeichnung wird bei der Konfiguration der Zertifikate für den SCEP-Client als “Verwendung” eingetragen.

Einstellbare Trace-Stufe für den SCEP-Client

Für den SCEP-Client-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Dazu wird ein Wert angegeben, bis zu welcher Stufe die Pakete im Trace ausgegeben werden sollen.

WEBconfig: Setup / Zertifikate / SCEP-Client / Trace-Stufe

- **Trace-Stufe**

  Mögliche Werte:

  - alles: alle Tracemeldungen, auch reine Info- und Debug-Meldungen
  - reduziert: nur Fehler- und Warnmeldungen
  - nur-Fehler: nur Fehlermeldungen

  Default:

  - alles

10.6.15 VPN-Verbindungen auf Zertifikatsunterstützung einstellen

Hinweis: VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das Gerät über die korrekte Uhrzeit verfügt. Wenn das Gerät keine aktuelle Uhrzeit hat, kann die Gültigkeit der Zertifikate nicht richtig beurteilt werden, die Zertifikate werden dann abgelehnt und es kommt keine Verbindung zustande.

Um VPN-Verbindungen auf die Unterstützung von Zertifikaten einzustellen, müssen verschiedene Teile der Konfiguration entsprechend vorbereitet werden:

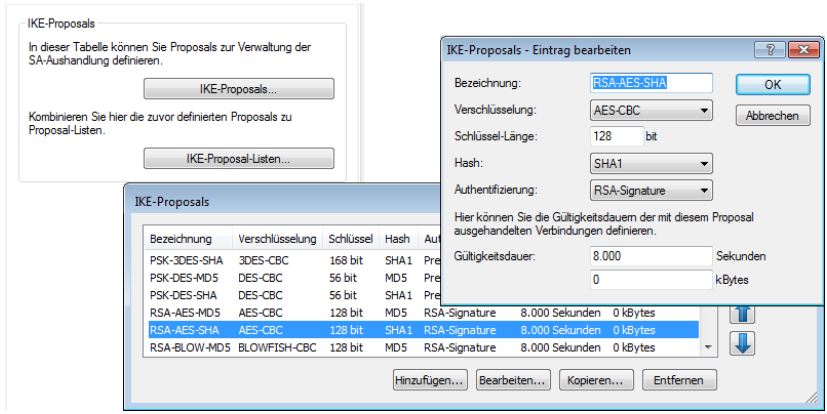
- IKE-Proposals
- IKE-Proposal-Listen

- IKE-Schlüssel
- VPN-Parameter
- Verbindungs-Parameter

Hinweis: Je nach Firmwarestand sind die benötigten Werte teilweise schon in Ihrem Gerät vorhanden. Prüfen Sie in diesem Fall nur die Werte auf richtige Einstellung.

Hinweis: Wenn Sie ein entferntes Gerät auf die nachfolgende beschriebene Weise auf Zertifikatsunterstützung umstellen wollen, das nur über einen VPN-Tunnel erreichbar ist, müssen Sie auf jeden Fall zuerst das entfernte Gerät umstellen, bevor Sie die Verbindung des lokalen Geräts ändern. Durch die Änderung der lokalen Konfiguration ist das entfernte Gerät ansonsten nicht mehr erreichbar!

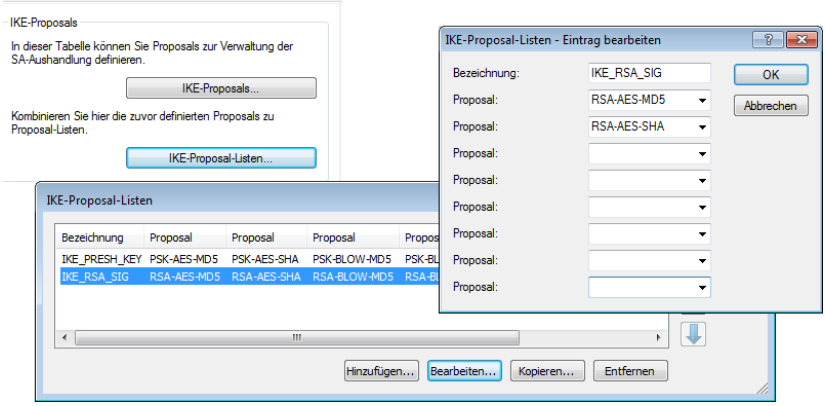
1. In den Listen der Proposals werden zwei neue Proposals mit den exakten Bezeichnung 'RSA-AES-MD5' und 'RSA-AES-SHA' benötigt, die beide als Verschlüsselung 'AES-CBC' und als Authentifizierungsmodus 'RSA-Signature' verwenden und sich nur im Hash-Verfahren (MD5 bzw. SHA1) unterscheiden.



LANconfig: VPN / IKE-Param. / IKE-Proposals

WEBconfig: HiLCOS-Menübaum / Setup / VPN / Proposals / IKE

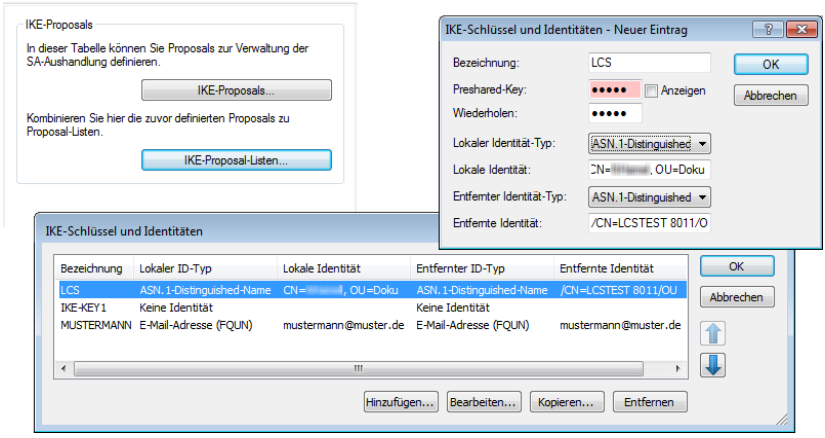
2. In den Proposal-Listen wird eine neue Liste benötigt mit der exakten Bezeichnung 'IKE_RSA_SIG', in der die beiden neuen Proposals 'RSA-AES-MD5' und 'RSA-AES-SHA' aufgeführt sind.



LANconfig: VPN / IKE-Param./ IKE-Proposallisten

WEBconfig: HiLCOS-Menübaum / Setup / VPN / Proposals / IKE-Proposal-Listen

3. In der Liste der IKE-Schlüssel müssen für alle Zertifikats-Verbindungen die entsprechenden Identitäten eingestellt werden.

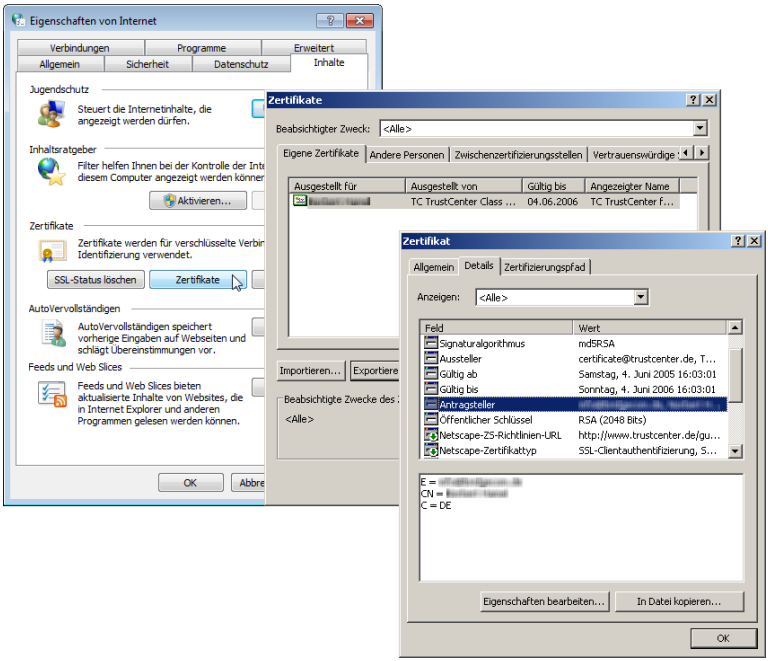


LANconfig: VPN / IKE-Param. / IKE-Schlüssel

- Der Preshared Key kann ggf. gelöscht werden, wenn er endgültig nicht mehr benötigt wird.
- Der Typ der Identitäten wird auf ASN.1 Distinguished Names umgestellt (lokal und remote).
- Die Identitäten werden exakt so eingetragen wie in den Zertifikaten. Die einzelnen Werte z. B. für 'CN', 'O' oder 'OU' können durch Kommata oder Slashes getrennt werden.

Es müssen alle in den Zertifikaten eingetragenen Werte aufgeführt werden, in der gleichen Reihenfolge. Prüfen Sie ggf. über die Systemsteuerung den Inhalt der Zertifikate. Wählen Sie dazu **Start** / **Systemsteuerung** / **Internetoptionen** und dort auf der Registerkarte 'Inhalte' die Schaltfläche **Zertifikate**.

Öffnen Sie das gewünschte Zertifikat und wählen Sie auf der Registerkarte 'Details' den entsprechenden Wert aus. Für den Antragsteller finden Sie hier z. B. die benötigten ASN.1 Distinguished Names mit den zugehörigen Kurzzeichen. Die in den Zertifikaten von oben nach unten aufgeführten Werte müssen in den IKE-Schlüssel von links nach rechts eingetragen werden. Beachten Sie auch die Groß- und Kleinschreibung!



Hinweis: Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Hinweis: Sonderzeichen in den ASN.1 Distinguished Names können durch die Angabe der ASCII-Codes in Hexadezimaldarstellung mit einem vorangestellten Backslash eingetragen werden. „\61“ entspricht z. B. einem kleinen „a“.

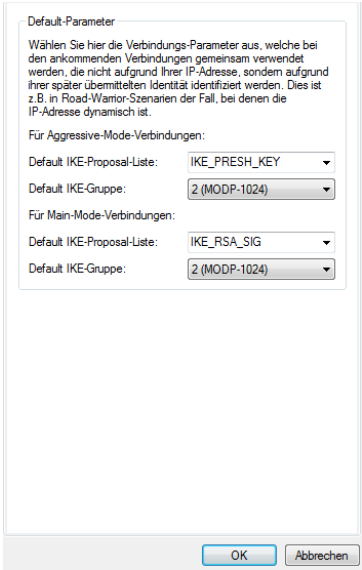
Unter WEBconfig oder Telnet finden Sie die IKE-Schlüssel an folgenden Stellen:

Konfigurations-tool	***Aufruf***
WEBconfig	HiLCOS-Menübaum / Setup / VPN / Zertifikate-Schluessel / IKE-Keys

Konfigurations-tool	*Aufruf*
Terminal/Telnet	`/Setup/VPN/Zertifikate-Schluessel/IKE-Keys`

4. In den IKE-Verbindungs-Parametern müssen die Default-IKE-Proposal-Listen für eingehende Aggressive-Mode- und Main-Mode-Verbindungen auf die Proposal-Liste 'IKE_RSA_SIG' eingestellt sein. Beachten Sie außerdem die Einstellung der Default-IKE-Gruppe, die im nächsten Schritt ggf. angepasst werden muss.

Die Default-IKE-Proposal-Listen und Default-IKE-Gruppen finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Defaults':

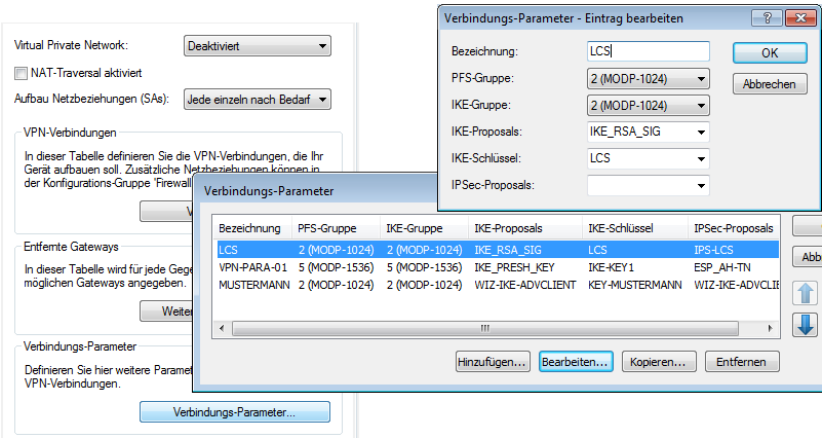


Unter WEBconfig oder Telnet finden Sie die Default-IKE-Proposal-Listen und Default-IKE-Gruppen an folgenden Stellen:

Konfigurationstool	*Aufruf*
WEBconfig	HiLCOSMenübaum / Setup / VPN
Terminal/Telnet	`/Setup/VPN`

In den VPN-Verbindungs-Parametern müssen zum Schluss die VPN-Verbindungen auf die Verwendung der richtigen IKE-Proposals eingestellt werden ('IKE_RSA_SIG'). Dabei müssen die Werte für 'PFS-Gruppe' und 'IKE-Gruppe' mit den in den IKE-Verbindungs-Parametern eingestellten Werten übereinstimmen.

Die VPN-Verbindungs-Parameter finden Sie unter LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein' mit einem Klick auf die Schaltfläche **Verbindungs-Parameter**:



Unter WEBconfig oder Telnet finden Sie die VPN-Verbindungs-Parameter an folgenden Stellen:

Konfigurationstool	*Aufruf*
WEBconfig	HiLCOS-Menübaum / Setup / VPN / VPN-Layer
Terminal/Telnet	`/Setup/VPN/VPN-Layer`

10.6.16 Zertifikatsbasierte VPN-Verbindungen mit dem Setup-Assistenten erstellen

Mit dem Setup-Assistenten von LANconfig können Sie schnell und bequem zertifikatsbasierte LAN-Kopplungen oder RAS-Zugänge über VPN einrichten.

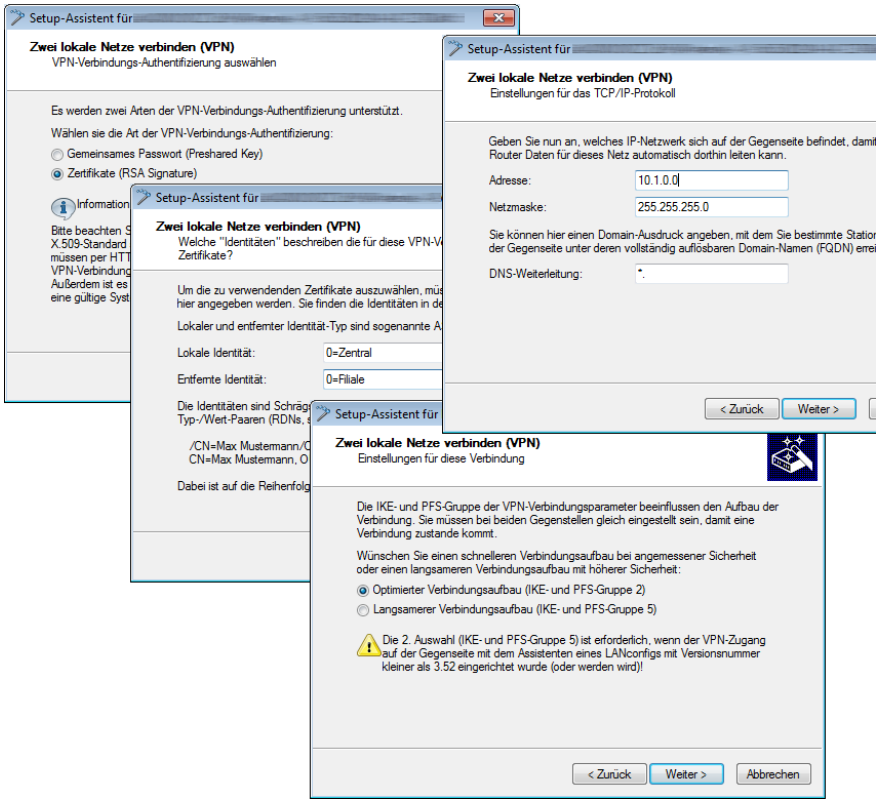
Hinweis: VPN-Verbindungen mit Zertifikatsunterstützung können nur aufgebaut werden, wenn das Gerät über die korrekte Uhrzeit verfügt und die entsprechenden Zertifikate in das Gerät geladen wurden.

LAN-Kopplungen

1. Wählen Sie den Assistenten zum Verbinden von Netzwerken über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature).
2. Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.

Hinweis: Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Hinweis: Der Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem Gerät, u.a. dabei die eingetragenen Relative Distinguished Names (RDN) unter „Subject“.



1. Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit IKE- und PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 für IKE und PFS, wenn dies von der Gegenstelle verlangt wird.
2. Tragen Sie den Namen der VPN-Gegenstelle, die IP-Adresse und die Netzmaske des entfernten Netzes sowie die ggf. verwendeten Domain für die DNS-Weiterleitung ein. Aktivieren Sie je nach Bedarf die „Extranet“-Funktion und das „NetBIOS-Routing“.

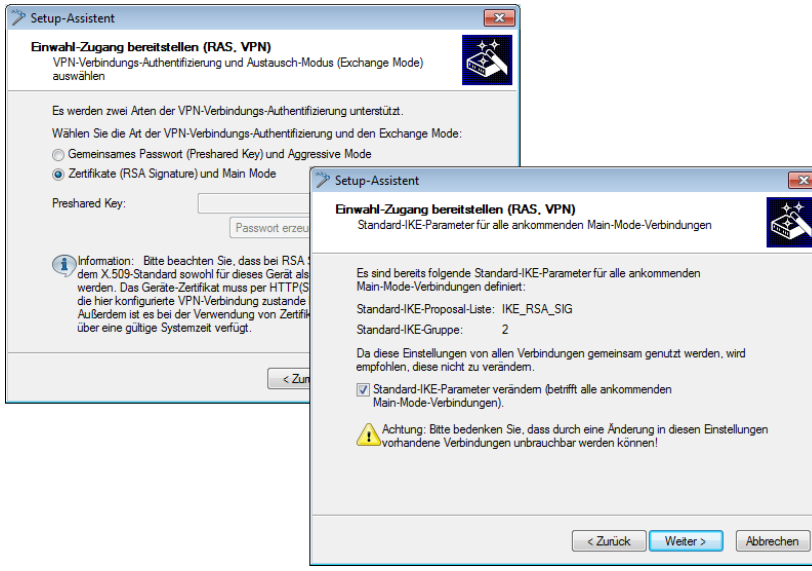
RAS-Zugänge

RAS-Zugänge mit Zertifikatsunterstützung können für den LANCOM Advanced VPN Client oder für einen anderen VPN-Client mit benutzerdefinierten Para-

metern eingerichtet werden. Der Standard VPN-Client bietet keine Unterstützung für Zertifikate an.

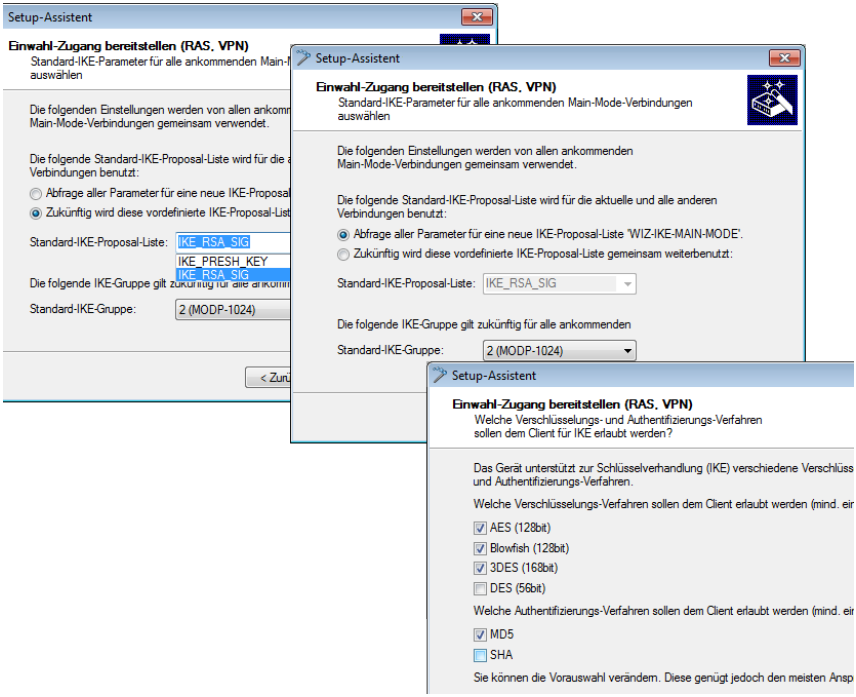
Hinweis: Die abgefragten Parameter unterscheiden sich je nach Auswahl des Clients bzw. der Optionen während der Dialoge. Diese Beschreibung zeigt vollständig alle evtl. auftretenden Dialoge des Assistenten, von denen nicht alle für Ihre Anwendung relevant sein müssen.

1. Wählen Sie den Assistenten zum Bereitstellen von Zugängen über VPN. Wählen Sie dann im entsprechenden Dialog die VPN-Verbindungsauthentifizierung über Zertifikate (RSA-Signature). Als „Exchange Mode“ wird dabei automatisch der Main Mode verwendet.

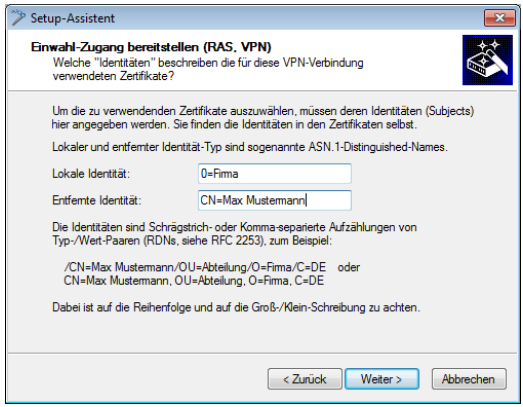


2. In der Konfiguration sind üblicherweise bereits Standard-IKE-Parameter für ankommende Main-Mode-Verbindungen in der Standard-IKE-Proposal-Liste 'IKE_RSA_SIG' definiert. Verwenden Sie nach Möglichkeit diese Liste mit den vorbereiteten IKE-Parametern.
3. Wenn Sie gezielt andere Parameter für die ankommenden Main-Mode-Verbindungen nutzen möchten, können Sie die Standard-IKE-Parameter an Ihre Bedürfnisse anpassen. Sie können entweder über die Abfrage der benötigten Parameter eine neue Liste 'WIZ-IKE-MAIN-MODE' erstellen oder eine der vorhandenen IKE-Proposal-Listen als neue „Standard-IKE-

Proposal-Liste“ auswählen. Die hier definierte Liste wird in Zukunft von allen ankommenden Main-Mode-Verbindungen verwendet. Für eine neue IKE-Proposal-Liste können Sie auswählen, welche Verschlüsselungsverfahren und Authentifizierungsverfahren der Client während der IKE-Verhandlung verwenden kann.



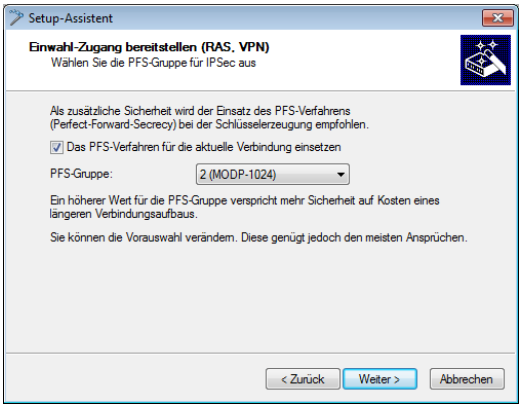
4. Tragen Sie die Identitäten aus dem lokalen und entfernten Geräte-Zertifikat ein. Übernehmen Sie dabei die vollständigen Angaben aus den jeweiligen Zertifikaten in der richtigen Reihenfolge: die in den Zertifikaten unter Windows von oben nach unten aufgeführten ASN.1-Distinguished Names werden in LANconfig von links nach rechts eingetragen.



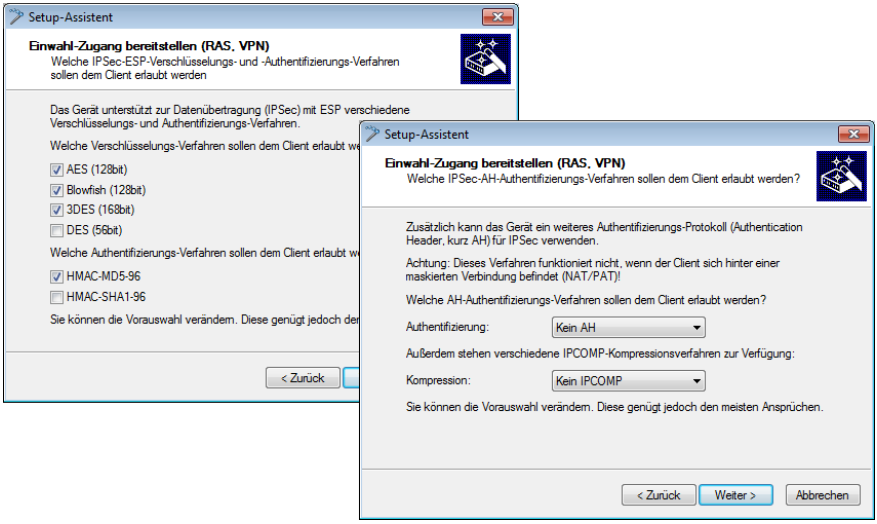
Hinweis: Die Anzeige von Zertifikaten unter Microsoft Windows zeigt für manche Werte ältere Kurzformen an, beispielweise 'S' anstelle von 'ST' für 'stateOrProvinceName' (Bundesland) oder 'G' anstelle von 'GN' für 'givenName' (Vorname). Verwenden Sie hier ausschließlich die aktuellen Kurzformen 'ST' und 'GN'.

Hinweis: Der Telnetbefehl `show vpn cert` zeigt die Inhalte des Geräte-Zertifikates in einem Gerät, u.a. dabei die eingetragenen Relative Distinguished Names (RDN) unter „Subject“.

5. Wählen Sie nach Möglichkeit den optimierten Verbindungsaufbau mit PFS-Gruppe 2. Wählen Sie nur dann die Gruppe 5 als PFS-Gruppe, wenn dies vom Client verlangt wird.



6. Für die Übertragung der Nutzdaten mit IPSec können in den folgenden Dialogen die Verschlüsselungs- und Authentifizierungsverfahren sowie die „Authentication Header“ und die Datenkompression festgelegt werden, die der Client verwenden kann. Verwenden Sie nach Möglichkeit die voreingestellten Werte, sofern der Client keine anderen Einstellungen erwartet.

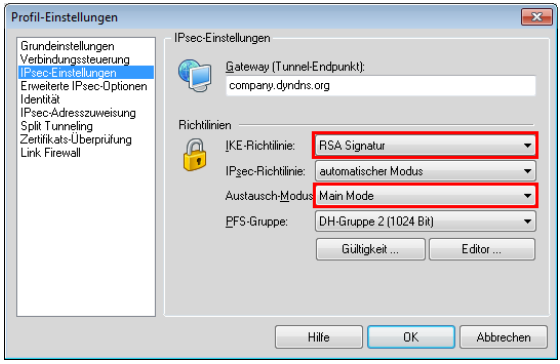


7. Tragen Sie die IP-Adresse für den Client und den für den Zugriff erlaubten Adress-Bereich im lokalen Netzwerk ein. Aktivieren Sie je nach Bedarf das „NetBIOS-Routing“.

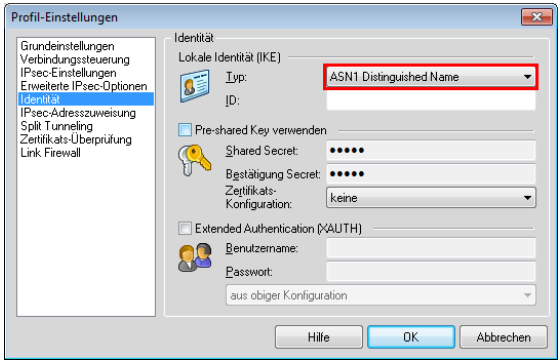
10.6.17 Advanced VPN Client auf Zertifikatsverbindungen einstellen

Bei der Einwahl mit dem Advanced VPN Client in einen Router müssen die entsprechenden Profil-Einstellungen an die Verwendung von Zertifikaten angepasst werden.

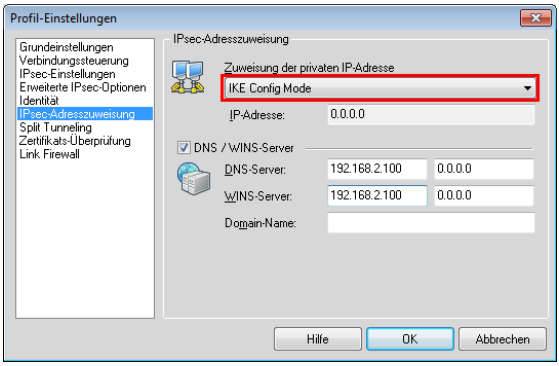
1. Stellen Sie in den IPSec-Einstellungen des Profils die IKE-Richtlinie auf 'RSA-Signatur' um.



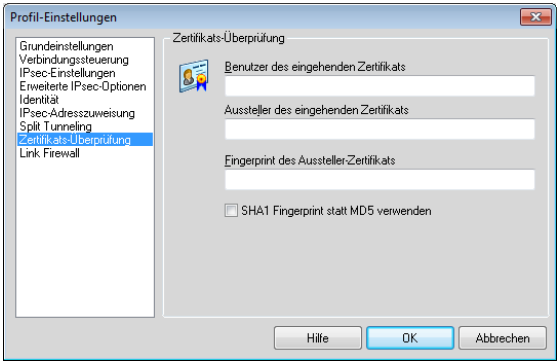
2. Stellen Sie die Identität auf 'ASN1 Distinguished Names' um. Die 'Identität' kann frei bleiben, da diese Information aus dem Zertifikat ausgelesen wird.



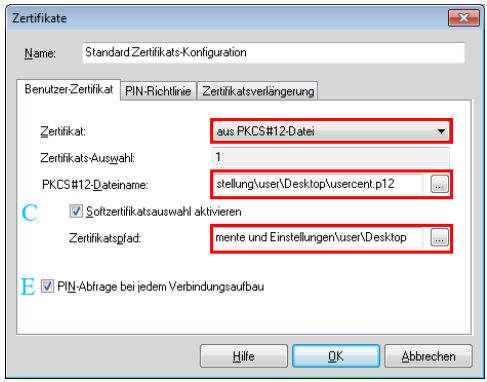
3. Verwenden Sie bei der IP-Adress-Zuweisung den 'IKE Config Mode'.



4. Bei der Zertifikatsüberprüfung können Sie optional die Zertifikate einschränken, die der LANCOM Advanced VPN Client akzeptiert. Dazu geben Sie den Benutzer und/oder den Aussteller des eingehenden Zertifikats und ggf. den zugehörigen „Fingerprint“ an.



5. Nachdem Sie das geänderte Verbindungsprofil gespeichert haben, öffnen Sie über den Menüpunkt **Konfiguration** / **Zertifikate** die Einstellungen für die Benutzerzertifikate.



6. Wählen Sie als Zertifikatetyp die 'PKCS#12-Datei aus **1** und geben Sie die gewünschte Zertifikatsdatei an **2**.

   - Wenn Sie mit verschiedenen Zertifikaten arbeiten möchten, aktivieren Sie die Option 'Softzertifikatsauswahl' **3** und geben den Pfad zum Ordner an, in dem die Zertifikatsdateien abgelegt sind **4**.
   - Wählen Sie aus, ob die PIN (das Kennwort) für das Zertifikat bei jedem Verbindungsaufbau abgefragt werden soll **5**. Alternativ können Sie die PIN über den Menüpunkt **Verbindung** / **PIN eingeben** fest im LANCOM Advanced VPN Client speichern.

   - Bei aktivierter Softzertifikatsauswahl können Sie beim Verbindungsaufbau im Hauptfenster des LANCOM Advanced VPN Client jeweils das gewünschte Zertifikat aus der Liste auswählen, passend zum gewählten Profil.

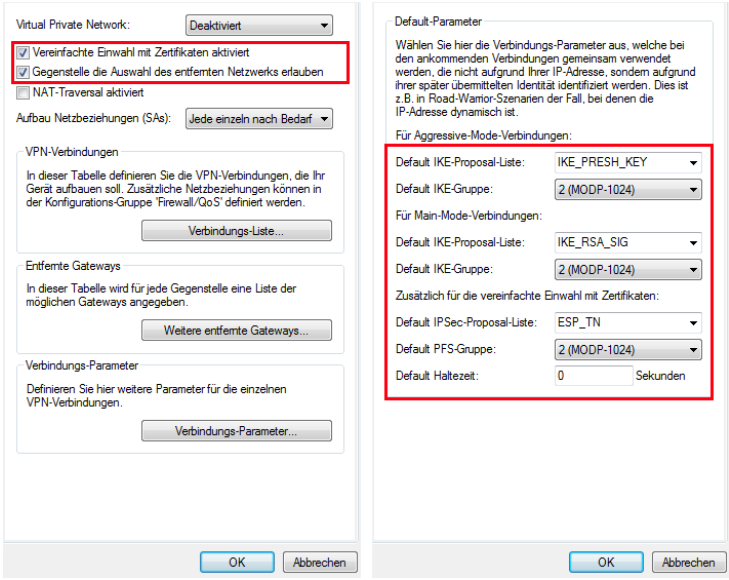
10.6.18 Vereinfachte Einwahl mit Zertifikaten

Bei der Einwahl von Rechnern mit wechselnden IP-Adressen ist zu Beginn der IKE-Verhandlung (Phase 1) die Identität der Gegenstelle noch nicht bekannt, zur Kommunikation werden Defaultwerte für IKE-Proposal-Listen und IKE-Proposal-Gruppen verwendet. Während der Verhandlung wird die Identität übermittelt, anhand derer die Parameter für die Phase 2 bestimmt werden können (IPSec-Proposal-Liste und PFS-Gruppe). Um diese Zuordnung zu ermöglichen, muss allerdings jeder einzelne Benutzer separat in der Konfiguration des VPN-Routers eingetragen werden.

Bei der zertifikatsbasierten Einwahl wird über das Zertifikat eine Identität übermittelt. Um nicht jeweils eigene Benutzereinträge in der Router-Konfiguration anlegen zu müssen, können für alle über Zertifikate identifizierbaren Benutzer gemeinsame Parameter für Phase 2 definiert werden. Bei dieser vereinfachten Einwahl muss der Benutzer nur über ein gültiges Zertifikat verfügen, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

Hinweis: Informationen über die Konfiguration des VPN-Clients entnehmen Sie bitte der entsprechenden Dokumentation des Software-Herstellers.

Zur Konfiguration der vereinfachten Einwahl wird diese Funktion aktiviert. Die Default-Parameter können bei Bedarf verändert werden.



Konfigurationstool	*Aufruf*
LANconfig	VPN / Allgemein und VPN / Allgemein / Defaults
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > VPN

Hinweis: Durch das Aktivieren der vereinfachten Zertifikate-Einwahl können sich **alle** Clients mit einem gültigen Zertifikat, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist, in das entsprechende Netzwerk einwählen. Es ist keine weitere Konfiguration des Routers erforderlich! Unerwünschte Einwahlen können ausschließlich über das Sperren der Zertifikate und die Verwendung einer CRL verhindert werden.

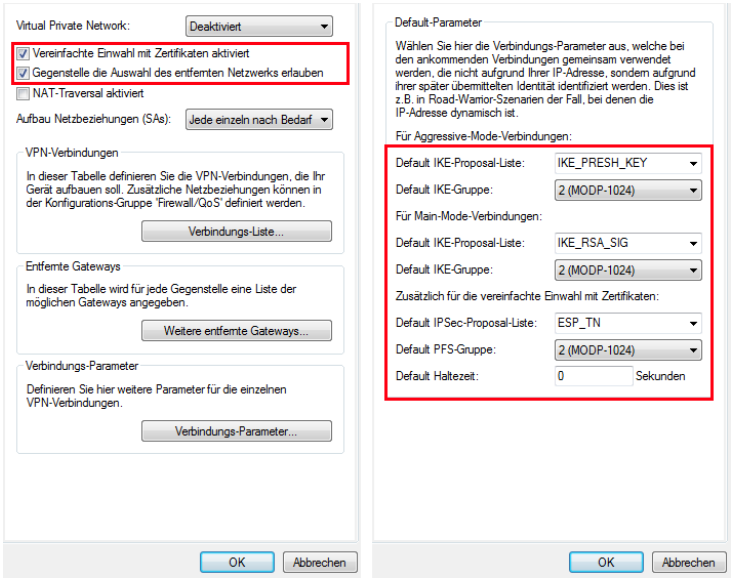
10.6.19 Vereinfachte Netzwerkanbindung mit Zertifikaten – Proadaptives VPN

Bei VPN-Kopplung von großen Netzwerkstrukturen ist oft gewünscht, dass der Konfigurationsaufwand bei der Einrichtung eines neuen Teilnetzwerks auf den dortigen VPN-Router beschränkt wird und die Konfiguration der zentralen Einwahl-Router unverändert bleiben kann. Um diese vereinfachte Netzwerkan-

bindung zu erreichen, übermitteln die einwählenden Geräte ihre Identität mit Hilfe eines Zertifikates.

Wenn die vereinfachte Einwahl mit Zertifikaten für den Router in der Zentrale aktiviert ist, können die entfernten Router während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, dass für die Anbindung verwendet werden soll. Dieses Netzwerk wird z. B. bei der Einrichtung der VPN-Verbindung in den entfernten Router eingetragen. Der Router in der Zentrale akzeptiert das vorgeschlagene Netzwerk, wenn die Option 'Gegenstelle Auswahl des entfernten Netzwerks erlauben' aktiviert ist. Darüber hinaus müssen die vom Client bei der Einwahl verwendeten Parameter mit den Defaultwerten des VPN-Routers übereinstimmen.

Hinweis: Achten Sie bei der Konfiguration der einwählenden Gegenstellen darauf, dass jede Gegenstelle ein spezielles Netzwerk anfordert, damit es nicht zu Konflikten der Netzwerkadressen kommt.



Konfigurationstool	*Aufruf*
LANconfig	VPN / Allgemein und VPN / Allgemein / Defaults
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > VPN

Hinweis: Durch das Aktivieren der vereinfachten Zertifikate-Einwahl können sich **alle** entfernten Router mit einem gültigen Zertifikat, das vom Herausgeber des im Gerät befindlichen Root-Zertifikats signiert ist, in das entsprechende Netzwerk einwählen. Es ist keine weitere Konfiguration des Routers erforderlich! Unerwünschte Einwahlen können ausschließlich über das Sperren der Zertifikate und die Verwendung einer CRL verhindert werden. Die vereinfachte Anbindung von Netzwerken mit Zertifikaten ist daher auf Router beschränkt, die Certification Revocation Lists (CRL) unterstützen.

10.6.20 Anfrage von Zertifikaten mittels CERTREQ

Einige VPN Gateways erwarten bei einer mittels RSA-Signature authentifizierten IPSec-Aushandlung, dass die zu übermittelnden Zertifikate über einen „Certificate Request“ (CERTREQ) von der Gegenstelle angefragt werden. Dies ermöglicht unter anderem eine Auswahl des zu verwendenden Zertifikats, sofern das Gateway mehreren CAs vertraut.

Um den Aufbau zu solchen VPN-Gateways zu ermöglichen, senden VPN-Router beim Verbindungsaufbau einen entsprechenden CERTREQ, der den Herausgeber des im Router gespeicherten Root-Zertifikates enthält.

10.6.21 Certificate Revocation List - CRL

Zertifikate für VPN-Verbindungen enthalten eine Gültigkeitsdauer in Form von Start- und Enddatum. Während dieser Zeit kann über dieses Zertifikat eine VPN-Verbindung aufgebaut werden. Scheidet ein Mitarbeiter aus dem Unternehmen aus, der ein solches Zertifikat z. B. für einen mobilen VPN-Zugang verwendet, möchte man in der Regel das Zertifikat vorzeitig für ungültig erklären, damit der Zugang zum Firmennetzwerk auch bei unveränderter Konfiguration der VPN Router nicht mehr möglich ist.

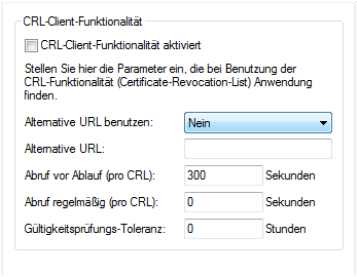
Da sich das Zertifikat selbst beim Mitarbeiter befindet und nicht verändert werden kann, wird eine Zertifikatsperrliste verwendet. In einer solchen Zertifikatsperrliste (Certificate Revocation List – CRL), wie sie z. B. von der Microsoft CA oder von OpenSSL unterstützt werden, sind die ungültigen Zertifikate eingetragen. Die CRL wird auf einem geeigneten Server bereitgestellt. Die URL, von der ein Router die CRL in seinen Speicher laden kann, wird im Root-Zertifikat des VPN-Routers und/oder in der Konfiguration des Geräts selbst eingetragen.

Die CRL wird von der CA regelmäßig erneuert, damit Änderungen in der CRL durch zurückgezogene Zertifikate von den VPN-Routern rechtzeitig erkannt werden können. Beim Aufsetzen der CA wird üblicherweise eine Zeitspanne festgelegt, nach der die CRL regelmäßig erneuert werden soll. Nach dem Erneuern der CRL und der Ablage der CRL auf dem Server (manuell oder automatisiert) muss der VPN-Router diese neuen Informationen aktualisieren. Dazu liest der Router die Gültigkeitsdauer der CRL aus und versucht kurz vor deren Ablauf eine aktuelle CRL zu laden. Alternativ kann auch ein regelmäßiges Update – unabhängig von der Gültigkeitsdauer der CRL – in einem Router definiert werden.

Beim Verbindungsaufbau prüft der VPN-Router, ob das Zertifikat der Gegenstelle in der aktuellen CRL enthalten ist. So können Verbindungen zu Gegenstellen mit ungültigen Zertifikaten abgelehnt werden.

Konfiguration der CRL-Funktion

Bei der Konfiguration der CRL-Funktion werden neben dem Pfad der CRL zusätzliche Parameter wie das Update-Intervall angegeben.



Konfigurationstool	*Aufruf*
LANconfig	Zertifikate / CRL-Client
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Zertifikate > CRLs

- CRL-Funktionalität [Default: Aus]
  - Aktiviert: Bei Prüfung eines Zertifikats wird die CRL (falls vorhanden) ebenfalls herangezogen.

Hinweis: Wenn diese Option aktiviert ist und keine gültige CRL gefunden werden kann, weil z. B. der Server nicht erreichbar ist, werden alle Verbindungen abgelehnt und bestehende Verbindungen unterbrochen.

- Alternative URL benutzen [Default: Nein]
  - Nein: Es wird nur die im Root-Zertifikat angegebene URL verwendet.
  - Ja, immer: Die alternative URL wird immer benutzt, auch wenn im Root-Zertifikat eine URL eingetragen ist.
  - Ja, alternativ: Die alternative URL wird nur benutzt, wenn im Root-Zertifikat keine URL eingetragen ist.
- Alternative URL
  - Diese URL kann (alternativ) benutzt werden, um eine CRL abzuholen.
- Abruf vor Ablauf [Default: 300 Sekunden]
  - Der Zeitpunkt vor dem Ablauf der CRL, ab dem versucht wird, eine neue CRL zu laden. Dieser Wert wird um einen Zufallskomponente erhöht, um gehäufte Anfragen an den Server zu vermeiden. Be Erreichen dieses Zeitpunkts wird ein evtl. aktiviertes regelmäßiges Update angehalten.

Hinweis: Wenn die CRL im ersten Versuch nicht geladen werden kann, werden in kurzen Zeitabständen neue Versuche gestartet.

- Abruf regelmäßig [Default: 0 Sekunden]
  - Die Länge des Zeitraums, nach dessen Ablauf periodisch versucht wird, eine neue CRL zu erhalten. Hiermit können eventuell außer der Reihe veröffentlichte CRLs frühzeitig heruntergeladen werden. Mit einem Eintrag von '0' wird das regelmäßige Abrufen ausgeschaltet.

Hinweis: Wenn die CRL bei regelmäßigen Update nicht geladen werden kann, werden keine Versuche bis zum nächsten regelmäßigen Termin gestartet.

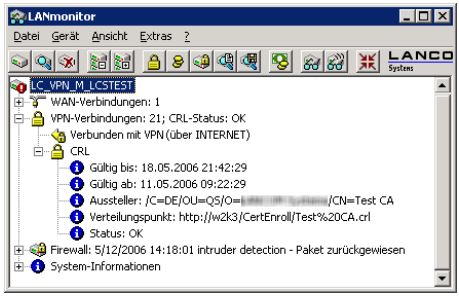
- Gültigkeitstoleranz

– Zertifikatsbasierte Verbindungen werden auch nach Ablauf der CRL-Gültigkeit noch innerhalb des hier eingetragenen Zeitraums zugelassen. Mit dieser Toleranz-Zeit kann verhindert werden, dass z. B. bei kurzfristig nicht erreichbarem CRL-Server die Verbindungen abgelehnt oder getrennt werden.

Hinweis: Innerhalb des hier eingestellten Zeitraums kann mit Hilfe der in der CRL bereits gesperrten Zertifikate weiterhin eine Verbindung aufrecht erhalten bzw. eine neue Verbindung aufgebaut werden.

Anzeige des CRL-Status im LANmonitor

Informationen über die Gültigkeitsdauer und den Herausgeber der aktuellen CRL im Router können im LANmonitor eingesehen werden.



Alternative URLs für CRLs

Einleitung

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als crlDistributionPoint) angegeben. In der Firmware können in einer Tabelle alternative URLs angegeben werden. Nach dem Systemstart werden die entsprechenden CRLs automatisch von diesen URLs abgeholt und zusätzlich zu den in den Zertifikaten angegebenen Listen verwendet.

Konfiguration

Die Tabelle für die alternativen CRL-URLs finden Sie auf folgenden Pfaden:

LANconfig: Zertifikate / CRL-Client / Alternative-URLs

WEBconfig: HiLCOS-Menübaum / Setup / Zertifikate / CRLs / Alternative-URL-Tabelle

- Alternative-URL

  Geben Sie hier die URL an, von der eine CRL abgeholt werden kann.

  – Mögliche Werte:

  Gültige URL, max. 251 Zeichen.

  – Default:

  Leer

10.6.22 Wildcard Matching von Zertifikaten

Einleitung

Bei zertifikatsbasierten VPN-Verbindungen werden in der Regel die Subjects (Antragsteller) der verwendeten Zertifikate als lokale und entfernte Identität verwendet. Diese werden in der VPN-Konfiguration in Form von (oftmals komplexen) ASN.1 Distinguished Names (DN) hinterlegt. In der VPN-Verhandlung wird dann die konfigurierte lokale Identität zur Auswahl des eigenen Zertifikates benutzt und an die Gegenstelle übermittelt, während die konfigurierte entfernte Identität mit der empfangenen Identität der Gegenstelle und mit dem Subject des empfangenen Zertifikates verglichen wird.

Die lokale und die entfernte Identität müssen in der VPN-Konfiguration bisher immer vollständig angegeben werden. Dies ist zum einen fehleranfällig, und zum anderen ist es manchmal gewünscht, nur einen Teil des Subjects angeben zu müssen. Praktisch ist dies beispielsweise, um bei einem Zertifikatswechsel oder bei gleichzeitiger Verwendung mehrerer paralleler Zertifikatshierarchien verschiedene Zertifikate mit ähnlichem Subject automatisch zu akzeptieren.

Um dies zu ermöglichen, kann ein flexiblerer Identitätsvergleich verwendet werden. Die in den konfigurierten Identitäten enthaltenen Komponenten eines

ASN.1-Distinguished Name (DN) (Relative Distinguished Names – RDNs) müssen in den relevanten Subjects dabei nur enthalten sein. Die Reihenfolge der RDNs ist dabei beliebig. Darüber hinaus können die Werte der RDNs die Wildcards '?' und '*' beinhalten. Werden die Wildcards als Teil des RDNs benötigt, müssen sie in Form von '\?' bzw. '*' angegeben werden. Beispiele:

- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/CN=Max?Muster*'
- Subject = '/CN=Max Mustermann/O=*ACME*', DN = '/O=*ACME*'

Konfiguration

Der flexible Identitätsvergleich kann in der VPN-Konfiguration aktiviert bzw. deaktiviert werden.

WEBconfig: HiLCOS-Menübaum / Setup / VPN

- **Flexible-ID-Comparison**

  Mögliche Werte:

  – Ja, Nein

  Default:

  – Nein

Der flexible Identitätsvergleich wird sowohl bei der Prüfung der (empfangenen) entfernten Identität als auch bei der Zertifikatsauswahl durch die lokale Identität eingesetzt.

10.6.23 Diagnose der VPN-Zertifikatsverbindungen

Die folgenden Befehle an der Telnet-Konsole können hilfreiche Aufschlüsse geben, sollte der VPN-Verbindungsaufbau nicht wie gewünscht funktionieren:

- `trace + vpn-status`

  Zeigt einen Trace der aktuellen VPN-Verbindungen.

- `show vpn long`

  Zeigt die Inhalte der VPN-Konfiguration, u.a. dabei die eingetragenen Distinguished Names (DN).

- `show vpn ca`

Zeigt den Inhalt des Root-Zertifikats.

- `show vpn cert`

  Zeigt den Inhalt des eigenen Geräte-Zertifikats.

  Hinweis: Die Relative Distinguished Names werden in dieser Darstellung bis Firmware-Version 6.00 in umgekehrter Reihenfolge, ab Firmware-Version 6.10 in der üblichen Reihenfolge angezeigt!

10.6.24 OCSP Client zur Zertifikatsüberprüfung

Einleitung

Das Online Certificate Status Protocol (OCSP) bietet eine Möglichkeit, den Status von Zertifikaten z. B. für den Aufbau von VPN-Verbindungen zu prüfen. Die Geräte nutzen dieses Protokoll, um zu untersuchen, ob der Herausgeber das verwendete Zertifikat evtl. schon vor dem Ablauf der Gültigkeit gesperrt und damit als ungültig markiert hat.

Der Herausgeber der Zertifikate pflegt den Status aller herausgegebenen Zertifikate auf einem speziellen Server, dem OCSP-Responder. Der OCSP-Client (also z. B. ein VPN-Router, der eine Verbindung aufbauen möchte) sendet einen OCSP-Request über das HTTP-Protokoll an den Responder, um den Status des Zertifikats zu ermitteln. Der Responder beantwortet diese Anfrage mit einer signierten Antwort, die der OCSP-Client auf ihre Gültigkeit hin prüft. Die Antwort des OCSP-Responders beschreibt einen der folgenden Zustände:

- good: Das überprüfte Zertifikat ist nicht gesperrt.
- evoked: Das überprüfte Zertifikat ist gesperrt und darf für den Aufbau von VPN-Verbindungen nicht mehr genutzt werden.
- unknown: Der OCSP-Responder kann den Status des Zertifikats nicht ermitteln, z. B. weil der OCSP-Responder den Herausgeber des Zertifikates nicht kennt oder weil das Zertifikat gefälscht und damit nicht in der Datenbasis des OCSP-Responders eingetragen ist.

Sie können das OCSP als Ergänzung oder als Ersatz für die Überprüfung der Zertifikate mit Zertifikatfsrückruflisten (Certificate Revocation Lists – CRL) verwenden. OCSP bietet gegenüber dem Ansatz der CRL folgende Vorteile:

- Die Herausgeber erstellen die CRLs in bestimmten zeitlichen Intervallen und sorgen idealerweise für die Verteilung der CRLs in die Geräte, welche die Zertifikate für den Aufbau der VPN-Verbindungen einsetzen. Die Zuverlässigkeit dieser Überprüfung ist daher an die zeitliche Aktualisierung der CRLs in den Geräten gekoppelt. Die Überprüfung der Zertifikate mit Hilfe eines OCSP-Responders ist dagegen immer "online", also automatisch auf dem aktuellen Stand. Der Betreiber des OCSP-Responders kann die dort vorgehaltenen Daten z. B. über eine automatische Synchronisierung mit den Daten der CA oder CAs abgleichen und so für einen jederzeit aktuellen Stand sorgen.
- Die Prüfung der Zertifikate gegen die Zertifikatfsrückruflisten belastet insbesondere bei großen CRLs den Speicher der Geräte. Die Abfrage des Zertifikatsstatus von einem OCSP-Responder ist dagegen unabhängig von der Anzahl der verwendeten CAs und Zertifikate und daher besser skalierbar.
- Das CRL-Verfahren liefert bei unbekannten Zertifikaten kein Ergebnis – damit kann dieses Verfahren keine gefälschten Zertifikate erkennen. Der OCSP-Responder beantwortet je nach Konfiguration die Anfrage nach unbekannten Zertifikaten mit einer negativen Bewertung.

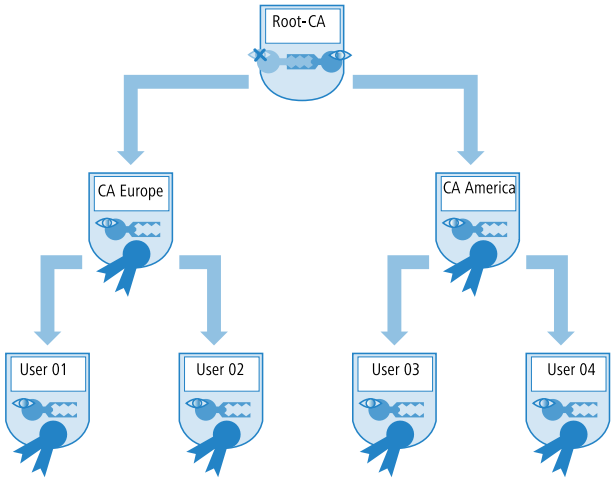
10.7 Mehrstufige Zertifikate für SSL/TLS

Neu mit LCOS 7.6:

- Mehrstufige Zertifikate für SSL/TLS

10.7.1 Einleitung

Bei großen oder räumlich verteilten Organisationen werden häufig mehrstufige Zertifikatshierarchien genutzt, bei der Endzertifikate durch eine oder mehrere Zwischen-CAs herausgegeben werden. Die Zwischen-CAs selbst sind dabei durch Root CA zertifiziert.



Für die Authentifizierung der Endzertifikate muss die Prüfung der gesamten Zertifikatshierarchie möglich sein.

10.7.2 SSL/TLS mit mehrstufigen Zertifikaten

Bei Anwendungen, die auf SSL/TLS basieren, (z. B. EAP/802.1x, HTTPS oder RADSEC) wird das SSL-(Server-)Zertifikat samt privatem Schlüssel und den CA-Zertifikat(en) der Zwischenstufen als PKCS#12-Container in das Gerät geladen.

Die Gegenstellen müssen dann beim Verbindungsaufbau nur das eigene Gerätezertifikat an das Gerät senden. Die Zertifikatskette wird im Gerät auf Gültigkeit geprüft.

10.7.3 VPN mit mehrstufigen Zertifikaten

Für den zertifikatsbasierten Aufbau von VPN-Verbindungen werden im Dateisystem des Gerätes ein privater Schlüssel, ein Gerätezertifikat und das Zertifikat der CA abgelegt. Bei einstufigen Zertifikatslösungen können dazu sowohl die einzelnen Dateien, als auch eine PKCS#12-Datei verwendet werden. Nach dem Hochladen und der Eingabe des Kennworts wird ein solcher Container in die drei genannten Bestandteile zerlegt.

Bei einer mehrstufigen Zertifikatshierarchie muss hingegen ein PKCS#12-Container mit den Zertifikaten der CAs aller Stufen in der Zertifikatskette verwendet werden. Hier wird nach dem Hochladen und der Eingabe des Kennworts neben dem privaten Schlüssel und dem Gerätezertifikat das Zertifikat der nächsten CA „oberhalb“ des Gerätes entpackt – die restlichen Zertifikat verbleiben im PKCS#12-Container. Beim Aktualisieren der VPN-Konfiguration werden die entpackten Zertifikate und die Zertifikate aus dem Container eingelesen. Beim Aufbau einer VPN-Verbindung übermittelt die Gegenstelle dann nur das eigene Geräte-Zertifikat, nicht jedoch die ganze Kette. Das Gerät kann dieses Zertifikat dann gegen die vorhandene Hierarchie prüfen.

Hinweis: Die Zertifikatsstrukturen müssen bei beiden Gegenstellen zueinander passen, d. h. die Hierarchie des anfragenden VPN-Gerätes darf keine Zertifikate erfordern, die in der Hierarchie des anderen VPN-Gerätes nicht enthalten sind.

10.8 Zertifikatsenrollment über SCEP

Zur Sicherung der Kommunikation über öffentlich zugängliche Netzwerke werden immer mehr zertifikatsbasierte VPN-Verbindungen eingesetzt. Dem hohen Sicherheitsanspruch der digitalen Zertifikate steht dabei ein deutlicher Mehraufwand für die Verwaltung und Verteilung der Zertifikate gegenüber. Dieser Aufwand entsteht dabei überwiegend in den Filialen oder Home-Offices einer verteilten Netzwerkstruktur.

Zum Aufbau einer zertifikatsbasierten VPN- Verbindung von einer Außenstelle zum Netzwerk einer Zentrale benötigt ein VPN-Router die folgenden Komponenten:

- Zertifikat der Root-CA mit dem Public Key der CA. In der Zentrale muss ebenfalls ein Zertifikat vorliegen, welches von derselben CA ausgestellt worden ist.
- Eigenes Geräte-Zertifikat mit dem eigenen Public Key. Dieses Zertifikat ist mit dem Private Key der CA signiert und stellt die Bestätigung der Identität dar.
- Eigenen privaten Schlüssel (Private Key).

Hinweis: Der SCEP-Client unterstützt ein Zertifikat pro Verwendungszweck (VPN, WLAN-Controller). Bei den CAs kann neben dem konkreten Verwendungszweck auch die Einstellung 'Allgemein' gewählt werden. Wenn eine allgemeine CA eingetragen wird, wird diese CA für alle Zertifikate verwendet.

Beim herkömmlichen Aufbau einer VPN-Struktur mit Zertifikaten müssen die Schlüssel und Zertifikate manuell in die einzelnen Geräte geladen werden und rechtzeitig vor Ablauf getauscht werden. Das Simple Certificate Enrollment Protocol (SCEP) erlaubt die sichere und automatisierte Verteilung von Zertifikaten über einen entsprechenden Server und reduziert so den Aufwand für den Roll-Out und die Pflege von zertifikatsbasierten Netzwerkstrukturen. Dabei wird u.a. das Schlüsselpaar für das Gerät nicht in einer externen Anwendung erstellt und später in das Gerät übertragen, sondern das Schlüsselpaar wird direkt im VPN-Router selbst erzeugt – der private Teil des Schlüssels muss also niemals das Gerät verlassen, was einen deutlichen Sicherheitsgewinn darstellt. Sowohl das Root-Zertifikat der CA als auch das eigene Geräte-Zertifikat kann ein VPN-Router über SCEP automatisiert von einer zentralen Stelle abrufen.

10.8.1 SCEP-Server und SCEP-Client

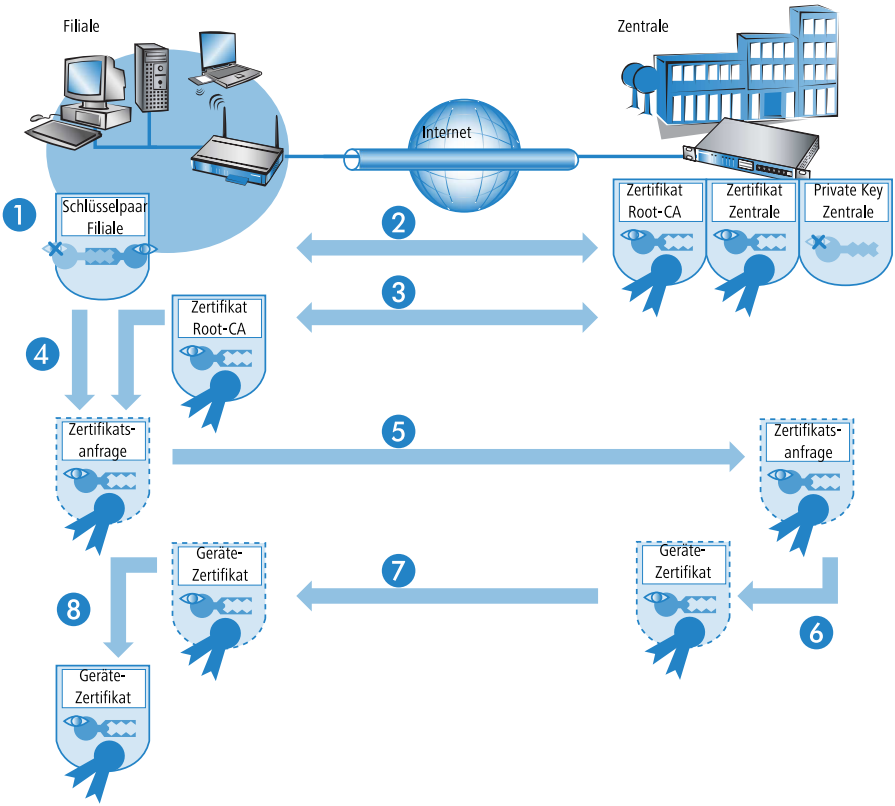
Die Bereitstellung und Verwaltung der Zertifikate wird von einem SCEP-Server vorgenommen, der neben der Funktion einer üblichen Certification Authority (CA) um die SCEP-Funktionalität erweitert ist. Dieser Server kann z. B. als Windows 2003 Server CA mit einem speziellen Plug-In (der mscep.dll) realisiert werden. Es existieren daneben eine Vielzahl von CA-Lösungen die SCEP beherrschen, so beispielsweise die OpenSource-Lösung OpenCA (www.openca.org).

Die SCEP-Erweiterung, also z. B. die mscep.dll, bildet eine zusätzliche Instanz auf dem Server, welche die Anfragen der SCEP-Clients bearbeitet und an die eigentliche CA weiterreicht. Diese Instanz wird als Registration Authority (RA) bezeichnet.

Als SCEP-Clients treten die VPN-Router auf, die vom zentralen Server die benötigten Zertifikate automatisiert abrufen wollen. Für den SCEP-Vorgang werden i.d.R. auch die von der CA signierten Zertifikate der RA (Registration Authority) benötigt. Für den eigentlichen VPN-Betrieb benötigen die VPN-Router dabei vor allem gültige Systemzertifikate (Gerätezertifikate). Die anderen ggf. genutzten Zertifikate werden nur für den SCEP-Vorgang benötigt.

10.8.2 Der Ablauf einer Zertifikatsverteilung

Im Überblick verläuft die Verteilung von Zertifikaten über SCEP nach folgendem Schema ab:



1. Schlüsselpaar im VPN-Router erzeugen.

   Im VPN-Router wird ein Schlüsselpaar erzeugt. Der öffentliche Teil dieses Schlüsselpaares wird später zusammen mit der Anfrage an den SCEP-Server übermittelt. Der private Teil des Schlüsselpaares verbleibt im SCEP-Client (VPN-Router). Die Tatsache, dass der private Schlüssel das Gerät zu keiner Zeit verlassen muss, stellt einen Sicherheitsgewinn gegenüber der manuellen Zertifikatsverteilung über z. B. PKCS#12-Container dar.

2. CA- und RA-Zertifikate abrufen.

Zur Kommunikation mit der RA/CA müssen im VPN-Router die entsprechenden RA- und CA-Zertifikate vorhanden sein. Bei einem Abruf des CA-Zertifikates über SCEP kann mit dem im Vorfeld konfigurierten Fingerprint automatisch geprüft werden, ob die abgerufenen Zertifikate auch tatsächlich von der gewünschten CA stammen. SCEP bietet selbst keinen Mechanismus zur automatischen Authentifizierung der CA-Zertifikate auf Seiten des SCEP-Clients. Wenn der Administrator der VPN-Router nicht selbst Zugriff auf die CA hat, muss er den Fingerprint z. B. per Telefon mit dem CA-Admin überprüfen.

3. Request für ein Geräte-Zertifikat erstellen und verschlüsseln.

Für die Beantragung eines System- bzw. Gerätezertifikats stellt der SCEP-Client die konfigurierten Informationen zusammen, u.a. die Identität des anfragenden Gerätes (Requester) und ggf. die „Challenge Phrase“, das Kennwort für die automatische Bearbeitung der Anfrage auf dem SCEP-Server. Diese Anfrage wird mit dem privaten Teil des Schlüsselpaares signiert.

4. Request an den SCEP-Server übermitteln.

Anschließend übermittelt der SCEP-Client die Anfrage mitsamt seinem öffentlichen Schlüssel an den SCEP-Server.

5. Prüfen der Zertifikatsanfrage auf dem SCEP-Server und Ausstellen des Geräte-Zertifikats.

Der SCEP-Server kann die erhaltene Anfrage entschlüsseln und daraufhin ein System- bzw. Gerätezertifikat für den Requester ausstellen. SCEP unterscheidet dabei folgende Methoden für die Bearbeitung der Anfragen:

- Bei der automatischen Bearbeitung muss die Authentizität des Requesters über die Challenge Phrase sichergestellt sein. Die Challenge Phrase wird z. B. auf einem Windows CA-Server mit mscep.dll automatisch erzeugt und ist für eine Stunde gültig. Stimmt die Challenge Phrase in der Zertifikatsanfrage mit dem aktuell gültigen Wert auf dem Server überein, kann das Systemzertifikat automatisch ausgestellt werden.
- Im manuellen Fall stellt der SCEP-Server die Zertifikatsanfrage in einen Wartezustand, bis die Bewilligung oder Ablehnung des CA-Administrators feststeht. Während dieser Wartezeit prüft der SCEP-Client regel-

mäßig ab, ob inzwischen beim SCEP-Server das angeforderte Systemzertifikat ausgestellt wurde.

- Bei RA-AutoApprove wird der Client über ein gültiges von der CA ausgestelltes Zertifikat authentifiziert.

6. Geräte-Zertifikat vom SCEP-Server abrufen

   Sobald das Zertifikat ausgestellt ist, stellt der Client durch regelmäßiges Polling fest, dass er das Zertifikat abrufen kann.

7. Geräte-Zertifikat prüfen und für VPN-Betrieb bereitstellen

10.8.3 Konfiguration von SCEP

Zur Konfiguration von SCEP werden globale Parameter für den SCEP-Betrieb und die CAs definiert, von denen die Geräte-Zertifikate abgerufen werden können.

Hinweis: Neben der Konfiguration des SCEP-Parameter ist ggf. eine Anpassung der VPN-Konfigurationen erforderlich.

Konfigurationstool	*Aufruf*
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Zertifikate > SCEP-Client

Globale SCEP-Parameter

- Aktiv

  Schaltet die Nutzung von SCEP ein oder aus.

  - Mögliche Werte: Ja, Nein
  - Default: Nein

- Wiederholen-Nach-Fehler-Intervall

  Intervall in Sekunden für Wiederholungen nach jeglicher Art von Fehler.

  - Default: 22

- Ausstehende-Anfragen-Prüfen-Intervall

  Intervall in Sekunden für das Prüfen von ausstehenden Zertifikatsanfragen.

- Default: 101

- Systemzertifikate-Aktualisieren-Vor-Ablauf

  Vorlaufzeit in Tagen zur rechtzeitigen Beantragung neuer Systemzertifikate (Gerätezertifikate).

  - Default: 2

- CA-Zertifikate-Aktualisieren-Vor-Ablauf

  Vorlaufzeit in Tagen zur rechtzeitigen Abholung neuer RA/CA-Zertifikate.

  - Default: 1

Aktionen

- Reinit

  Startet die manuelle Re-Initialisierung der SCEP-Parameter. Dabei werden wie bei der gewöhnlichen SCEP-Initialisierung auch die notwendigen RA- und CA-Zertifikate von der CA abgerufen und so im Dateisystem des VPN-Routers abgelegt, dass sie noch **nicht** für die Nutzung im VPN-Betrieb bereit stehen.

  - Sofern das vorhandene Systemzertifikat zum abgerufenen CA-Zertifikat passt, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.
  - Sofern die vorhandenen Systemzertifikate **nicht** zum abgerufenen CA-Zertifikat passen, muss zunächst eine neue Zertifikatsanfrage beim SCEP-Server gestellt werden. Erst wenn so ein neues, zum CA-Zertifikat passendes Systemzertifikat ausgestellt und abgerufen wurde, können Systemzertifikat, CA-Zertifikat und privater Geräteschlüssel für den VPN-Betrieb genutzt werden.

- Aktualisieren

  Startet manuell die Anfrage nach einem neuen Systemzertifikat, unabhängig von der verbleibenden Gültigkeitsdauer. Dabei wird ein neues Schlüsselpaar erzeugt.

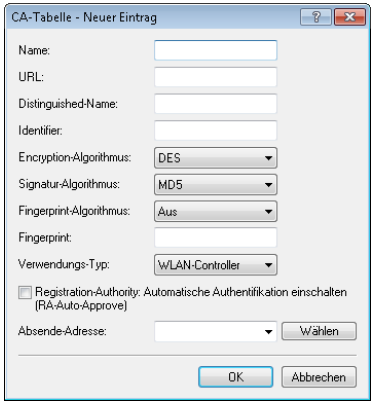
- Bereinige-SCEP-Dateisystem

  Startet die Bereinigung des SCEP-Dateisystems.

- gelöscht werden: RA-Zertifikate, ausstehende Zertifikatsanfragen, neue und inaktive CA-Zertifikate, neue und inaktive private Schlüssel.
- erhalten bleiben: aktuell im VPN-Betrieb genutzte Systemzertifikate, private Schlüssel dazu und die aktuell im VPN-Betrieb genutzten CA-Zertifikate.

Konfiguration der CAs

Die Konfiguration erfolgt in LANconfig unter **Zertifikate** > **SCEP-Client** mit der Schaltfläche **CA-Tabelle**.



Name

Konfigurationsname der CA.

URL

URL der CA.

Distinguished-Name

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene oder vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen Firmware-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

Identifier

CA-Identifier (wird von manchen Webservern benötigt, um die CA zuordnen zu können).

Encryption-Algorithmus

Mit diesem Algorithmus wird die Nutzlast des Zertifikatsantrages verschlüsselt. Mögliche Werte sind:

- DES (Default)
- 3-DES
- Blowfish
- AES128
- AES192
- AES256

Signatur-Algorithmus

Mit diesem Algorithmus wird der Zertifikatsantrag signiert. Mögliche Werte sind:

- MD5 (Default)

- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint-Algorithmus

Algorithmus zum Signieren der Fingerprints. Legt fest, ob eine Überprüfung der CA-Zertifikate anhand des Fingerprints vorgenommen wird und mit welchem Algorithmus. Der CA-Fingerprint muss mit der Prüfsumme übereinstimmen, die sich bei Verwendung des Algorithmus ergibt. Mögliche Werte sind:

- Aus (Default)
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint

Anhand der hier eingetragenen Prüfsumme (Fingerprint) kann die Authentizität des erhaltenen CA-Zertifikates überprüft werden (entsprechend des eingestellten CA-Fingerprintalgorithmus).

Verwendungs-Typ

Gibt den Verwendungszweck der eingetragenen CA an. Die hier eingetragene CA wird dann nur für den entsprechenden Verwendungszweck abgefragt. Mögliche Werte sind:

- VPN
- EAP/TLS
- WLAN-Controller
- Allgemein

Hinweis: Wenn eine allgemeine CA vorhanden ist, lässt sich keine weitere konfigurieren, da sonst die Wahl der CA nicht eindeutig ist.

RA-Autoapprove

Manche CAs bieten die Möglichkeit, ein bereits von dieser CA ausgestelltes Zertifikat als Nachweis der Authentizität für nachfolgende Anträge zu benutzen. Mit dieser Option wird festgelegt, ob bei bereits vorliegendem Systemzertifikat Neuanträge mit dem vorhandenen Systemzertifikat unterschrieben werden. Mögliche Werte sind:

- Ja
- Nein (Default)

Absende-Adresse

Hier konfigurieren Sie optional eine Absendeadresse, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Des Weiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Hinweis: Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Konfiguration der Systemzertifikate

Name

Konfigurationsname des Zertifikats.

CADN

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits

spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen Firmware-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

Subject

Distinguished Name des Subjects des Antragstellers.

ChallengePwd

Kennwort (für das automatische Ausstellen der Geräte-Zertifikate auf dem SCEP-Server).

SubjectAltName

Weitere Angaben zum Requester, z. B. Domain oder IP-Adresse.

KeyUsage

Beliebige kommaseparierte Kombination aus:

- digitalSignature
- nonRepudiation

- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly
- critical (möglich aber nicht empfohlen)

extended Key Usage

Beliebige kommaseparierte Kombination aus:

- critical
- serverAuth
- clientAuth
- codeSigning
- emailProtection
- timeStamping
- msCodeInd
- msCodeCom
- msCTLSign
- msSGC
- msEFS
- nsSGC
- 1.3.6.1.5.5.7.3.18 für WLAN-Controller
- 1.3.6.1.5.5.7.3.19 für Access Points im Managed-Modus

Systemzertifikate-Schlüssellänge

Länge der Schlüssel, die für das Gerät selbst erzeugt werden.

- Mögliche Werte: 31 oder größer.

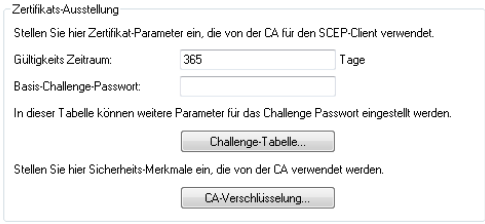
Verwendung

Gibt den Verwendungszweck der eingetragenen Zertifikate an. Die hier eingetragenen Zertifikate werden dann nur für den entsprechenden Verwendungszweck abgefragt.

- Mögliche Werte: VPN, WLAN-Controller

Challenge-Passwörter konfigurieren

Im LANconfig konfigurieren Sie unter **Zertifikate** > **Zertifikats-Behandlung** im Abschnitt **Zertifikats-Ausstellung** die Zertifikats-Parameter.



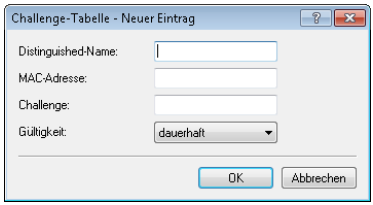
Gültigkeitszeitraum

Bestimmen Sie hier die Gültigkeitsdauer des Zertifikates in Tagen.

Basis-Challenge-Passwort

Hier kann ein weiteres “Passwort” eingetragen werden, das an die CA übertragen wird. Dieses kann standardmäßig zur Authentifizierung von Rücknahme-Anträgen benutzt werden. Auf CAs mit Microsoft-SCEP (mscep) können (falls dort aktiviert) die von der CA vergebenen Einmal-passwörter zur Antragsauthentifizierung eingetragen werden.

Die **Challenge-Tabelle** verwaltet die eigenen Passwörter der Zertifikat-Nehmer (Client).



Distinguished-Name

Hier muss der “Distinguished Name” eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene oder vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auf-listung, in der Name, Abteilung, Bundesland und Land des Gateways

angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=HIRSCHMANN CA/O=HIRSCHMANN/C=DE`

MAC-Adresse

Tragen Sie hier die MAC-Adresse des Clients ein, dessen Passwort in der Challange-Passwort-Tabelle verwaltet wird.

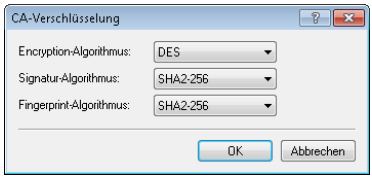
Challenge

Geben Sie hier die Challenge (Passwort) für den Client an.

Gültigkeit

Geben Sie hier die Gültigkeit des Passwortes an. Wenn Sie “einmalig” auswählen, handelt es sich bei diesem Passwort um ein One-Time-Passwort (OTP), das nur für die einmalige Verwendung z. B. bei einer Authentifizierung gültig ist.

Unter **CA-Verschlüsselung** konfigurieren Sie die Sicherheitsmerkmale der CA-Verschlüsselung.



Encryption-Algorithmus

Wählen Sie hier den Verschlüsselungs-Algorithmus zur Verschlüsselung innerhalb des SCEP-Protokolls aus. Sowohl die Zertifizierungsstelle (CA) als auch der Zertifikatnehmer (Client) müssen den Algorithmus unterstützen. Die folgenden Verfahren stehen zur Auswahl:

- DES
- 3DES
- BLOWFISH
- AES128
- DES192
- DES256

Signatur-Algorithmus

Wählen Sie hier den Signatur-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die CA als auch der Zertifikatnehmer (Client) müssen das Verfahren unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen die folgenden kryptographischen Hash-Funktionen zur Auswahl:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

Fingerprint-Algorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die CA als auch der Zertifikatnehmer (Client) müssen das Verfahren unterstützen.

Der Fingerprint ist ein Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann. Es stehen die folgenden kryptographischen Hash-Funktionen zur Auswahl:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

10.8.4 Verwendung digitaler Zertifikate (Smart Certificate)

Die Konfiguration des SCEP-Clients für die Erstellung und Verteilung von Zertifikaten wird in einer komplexen und ausgedehnten Netz-Infrastruktur schnell aufwändig. Durch vordefinierte, auswählbare Profile und den Zugriff über eine Web-Schnittstelle lässt sich dieser Aufwand reduzieren.

Mit einem LANCOM Router haben Sie die Möglichkeit, hochsichere Zertifikate zu generieren und zuzuweisen. Sie verwalten die Zertifikate bequem über die WEBconfig-Oberfläche des entsprechenden Gerätes. Eine externe Zertifizie-

rungsstelle ist somit nicht mehr erforderlich, was gerade bei kleineren Infrastrukturen vorteilhaft ist.

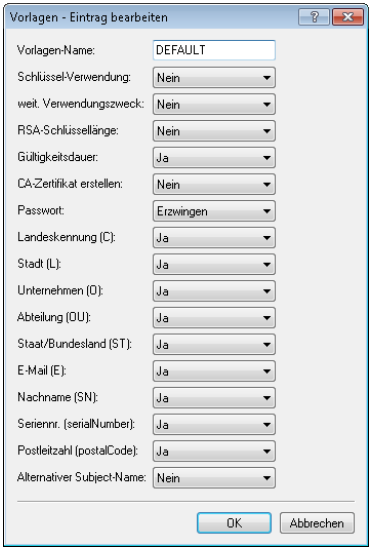
Mit dem Zertifikats-Wizard von LANCOM können selbst Anwender ohne Zertifikats-Knowhow in wenigen Schritten Zertifikate erstellen.

Der Geräte-Administrator erstellt das Profil als Sammlung von Zertifikats-Eigenschaften. Es enthält einerseits die Konfiguration des Zertifikates sowie eine eindeutige Zertifikats-ID. Statt also alle Zertifikats-Parameter einzugeben, genügt es von da an, eines der angezeigten Profile auszuwählen, um ein Zertifikat zu erstellen und zu verteilen.

Die Verwaltung von Profilen erfolgt auch im LANconfig unter **Zertifikate** > **Zertifikatsbehandlung** im Abschnitt **Web-Interface der CA**.

Vorlagen für Zertifikats-Profile erstellen

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Vorlagen**.



Hinweis: Standardmäßig ist bereits eine Vorlage “DEFAULT” angelegt.

Der Adminstrator legt fest, welche der Profileigenschaften erforderlich und welche durch den Anwender zu editieren sind. Die folgenden Optionen stehen zur Auswahl:

- Nein: Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.
- Fest: Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.
- Ja: Das Feld ist sichtbar und durch den Anwender änderbar.
- Erzwingen: Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

Diese Zugriffsrechte gelten für die folgenden Profil- und ID-Felder:

Profilfelder

- Schlüssel-Verwendung
- weit. Verwendungszweck
- RSA-Schlüssellänge
- Gültigkeitsdauer
- CA-Zertifikat erstellen
- Passwort

Identifier

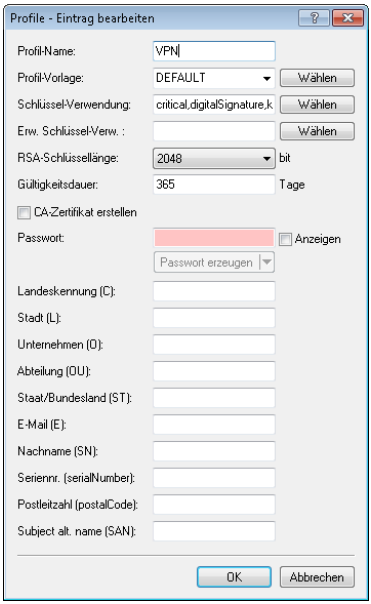
- Landeskennung (C)
- Stadt (L)
- Unternehmen (O)
- Abteilung (OU)
- Staat / Bundesland (ST)
- E-Mail (E)
- Nachname (SN)
- Seriennr. (serialNumber)
- Postleitzahl (postalCode)
- Subject alt. name

Tipp: Bei leerer Vorlagen-Tabelle sieht der Anwender nur Eingabefelder für die Profilnamen, die allgemeinen Namen (CN) sowie das Passwort. Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

Erstellen eines Profils in LANconfig

Hinweis: Der Anwender benötigt für Erstellung, Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Profile**.



Hinweis: Standardmäßig sind bereits drei Profile für gängige Anwendungsszenarien angelegt.

Profil-Name

Der eindeutige Name des Profils.

Profil-Vorlage

Wählen Sie hier ggf. eine passende Profil-Vorlage aus.

In der Profil-Vorlage ist festgelegt, welche Zertifikatsangaben notwendig und welche änderbar sind. Die Vorlagen-Erstellung erfolgt unter **Zertifikate** > **Zertifikats-Behandlung** > **Vorlagen**.

Schlüssel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen über die Schaltfläche **Wählen** zur Auswahl:

Wert	*Bedeutung*
critical	Ist diese Einschränkung gesetzt, ist es immer erforderlich, die Schlüsselverwendungs-Erweiterung zu beachten. Wird die Erweiterung nicht unterstützt, wird das Zertifikat als nicht gültig abgelehnt.
digitalSignature	Ist diese Option gesetzt, wird der öffentliche Schlüssel für digitale Signaturen verwendet.
nonRepudiation	Ist diese Option gesetzt, wird der Schlüssel für digitale Signaturen eines Nichtabstreitbarkeitsservice verwendet. d. h. eher langfristigen Charakter besitzt, z. B. Notariatsservice.
keyEncipherment	Ist diese Option gesetzt, wird der Schlüssel für die Verschlüsselung von anderen Schlüsseln oder Sicherheitsinformation verwendet. Es ist möglich, die Verwendung mit **encipher only** und **decipher only** einzuschränken.
dataEncipherment	Ist diese Option gesetzt, wird der Schlüssel zur Verschlüsselung von Benutzerdaten (außer andere Schlüssel) verwendet.
keyAgreement	Ist diese Option gesetzt, wird der "Diffie-Hellman" Algorithmus für die Schlüsselvereinbarung verwendet.
keyCertSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf Zertifikaten verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
cRLSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf CRLs verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
encipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.
decipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.

Tabelle 23: Zur Verfügung stehende Schlüssel-Verwendungen

Hinweis: Eine kommagetrennte Mehrfachauswahl ist möglich.

Erw. Schlüssel-Verw.

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen über die Schaltfläche **Wählen** zur Auswahl:

Wert	*Bedeutung*
critical	
serverAuth	SSL/TLS-Web-Server-Authentifizierung
clientAuth	SSL/TLS-Web-Client-Authentifizierung
codeSigning	Signierung von Programmcode
emailProtection	E-Mail-Schutz (S/MIME)
timeStamping	Daten mit zuverlässigen Zeitstempeln versehen
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto
msEFS	Microsoft Encrypted File System
nsSGC	Netscape Server Gated Crypto

Tabelle 24: Erweiterte Verwendungen

Hinweis: Eine kommagetrennte Mehrfachauswahl ist möglich.

RSA-Schlüssellänge

Gibt die Länge des Schlüssels an.

Gültigkeitsdauer

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

CA-Zertifikat erstellen

Gibt an, ob es sich um ein CA-Zertifikat handelt.

Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

Die folgenden Eingaben dienen zur Erstellung einer Zertifikats-ID. Zur Auswahl stehen die folgenden Optionen:

Landeskennung (C)

Geben Sie die Staatenkennung ein (z. B. “DE” für Deutschland).

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `C=` (**C**ountry).

Stadt (L)

Geben Sie den Ort ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `L=` (**L**ocality).

Unternehmen (O)

Geben Sie das Unternehmen an, welches das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `O=` (**O**rganization).

Abteilung (OU)

Geben Sie die Abteilung an, die das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `OU=` (**O**rganization **U**nit).

Staat / Bundesland (ST)

Geben Sie das Bundesland ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `ST=` (**ST**ate).

E-Mail (E)

Geben Sie eine E-Mail-Adresse ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `emailAddress=`.

Nachname (SN)

Geben Sie einen Nachnamen ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `SN=` (**S**ur**N**ame).

Seriennr. (serialNumber)

Geben Sie eine Seriennummer ein.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

Postleitzahl (postalCode)

Geben Sie die Postleitzahl des Ortes ein.

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `postalCode=`.

Subject alt. Name (SAN)

Mit dem “Subject-Alternative-Name” (SAN) verknüpfen Sie weitere Daten mit diesem Zertifikat. Die folgenden Daten sind möglich:

- E-Mail-Adressen
- IPv4- oder IPv6-Adressen
- URIs
- DNS-Namen
- Verzeichnis-Namen
- Beliebige Namen

Im Subject oder Issuer des Zertifikates erscheint dieser Eintrag unter `subjectAltName=` (z. B. `subjectAltName=IP:192.168.7.1`).

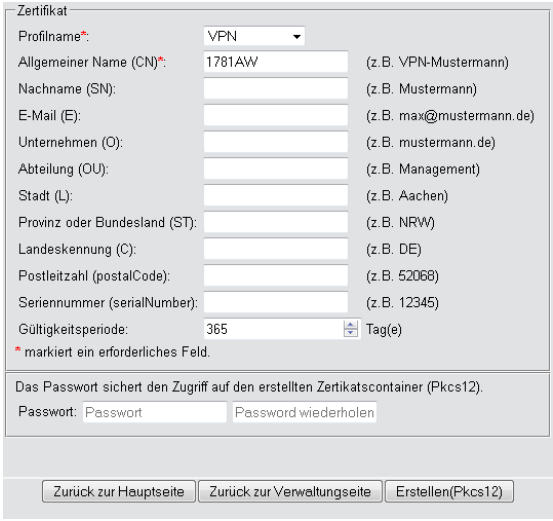
Hinweis: Der Zertifikatersteller vergibt den allgemeinen Namen "CN". Die Angabe des "CN" ist mindestens erforderlich.

Zertifikaterstellung über WEBconfig

Hinweis: Sie benötigen für Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

Zur Zertifikaterstellung wechseln Sie in die WEBconfig des OpenBAT-Gerätes.

1. Um über die Webschnittstelle ein Zertifikat zu erstellen, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten** und wählen Sie **Neues Zertifikat erstellen**.



2. Wählen Sie im Dropdown-Menü **Profilname** das Profil aus, auf dem das Zertifikat beruhen soll.

   Tipp: Leere Vorlagen enthalten nur Felder mit der Auswahl “Nein”. Wählt der Anwender ein Profil aus, das auf einer leeren Vorlage basiert, erscheint in der Eingabemaske nur der allgemeine Name (Common-name). Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

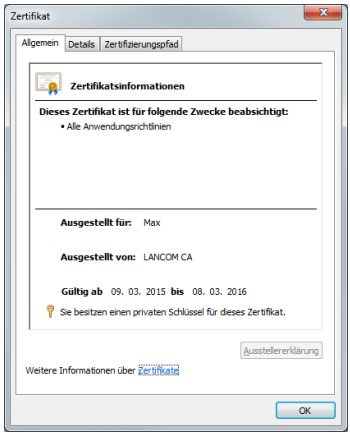
3. Füllen Sie das Feld **Allgemeiner Name (CN)** aus. Definieren Sie eine Gültigkeitsperiode für das Zertifikat und vergeben Sie ein sicheres Passwort (PIN). Die übrigen Felder wie **E-Mail**, **Unternehmen** etc. sind optionale Informationen. Sie erleichtern jedoch ggf. die schnellere Suche des Zertifikat-Empfängers, wenn es zu Problemen mit dem Zertifikat kommen sollte.

   Hinweis: Für das Passwort sind folgende Zeichen zulässig: [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

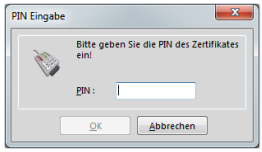
4. Zum Abschluss der Änderungen klicken Sie auf die Schaltfläche **Erstellen (PKCS12)**. Im darauf folgenden Speicherdialog haben Sie die Möglichkeit, den Namen und Speicherort der Datei festzulegen.

Hinweis: Die so neu erstellten Zertifikate erscheinen in der Zertifikate-Status-Tabelle unter **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate**.

5. Übergeben Sie dem Empfänger das erstellte Zertifikat zusammen mit dem Zugangspasswort, das Sie in Schritt 3 vergeben haben.



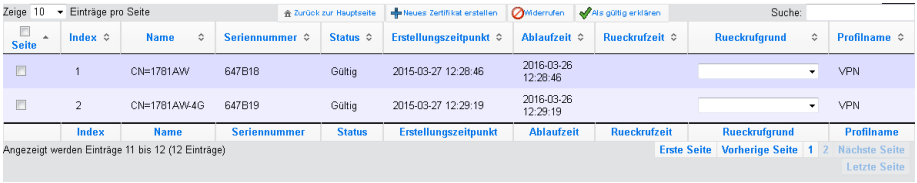
6. Der Empfänger hat jetzt die Möglichkeit einer sicheren VPN-Einwahl. Für eine erfolgreiche Einwahl ist die Eingabe des Zugangspasswortes (PIN) erforderlich, das Sie in Schritt 3 vergeben haben.



Zertifikatverwaltung über die WEBconfig

Hinweis: Sie benötigen für die Verwaltung der Zertifikate die entsprechenden Zugriffsrechte.

Um über die Webschnittstelle ein Zertifikat zu verwalten, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten**. Hier erhalten Sie eine Übersicht der erstellten Zertifikate und können diese auch widerrufen.



Die Tabellenspalten haben die folgenden Bedeutungen:

Seite

In dieser Spalte markieren Sie den Eintrag.

Index

Zeigt den fortlaufenden Index des Eintrages an.

Name

Zeigt den Namen des Zertifikates an.

Seriennummer

Enthält die Seriennummer des Zertifikates.

Status

Zeigt den aktuellen Status des Zertifikates an. Mögliche Werte sind:

- V: Gültig (valid)
- R: Widerrufen (revoked)
- P: Angefragt (pending)

Erstellungszeitpunkt

Zeigt den Zeitpunkt der Zertifikaterstellung an (Datum, Uhrzeit).

Ablaufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat regulär abläuft.

Rückrufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat vorzeitig widerrufen wurde.

Rückrufgrund

Gibt den Grund für einen vorzeitigen Widerruf an. Die Auswahl erfolgt über eine Drop-Down-Auswahlliste.

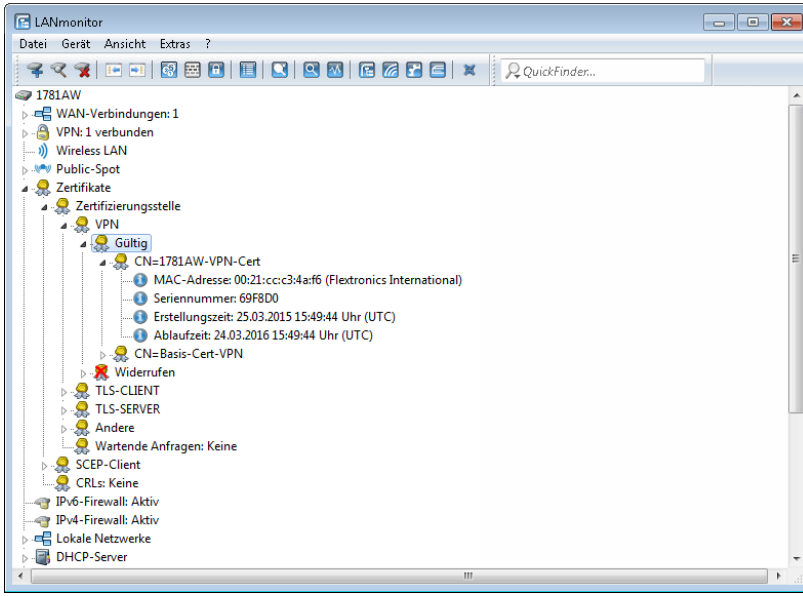
Um ein Zertifikat zu widerrufen, markieren Sie es in der Spalte **Seite**, geben in der Spalte **Rückrufgrund** an, warum Sie das Zertifikat widerrufen und klicken auf **Widerrufen**.

Die Spalteneinträge von **Status**, **Rückrufzeit** und **Rückrufgrund** ändern sich entsprechend.

Um ein zuvor widerrufenes Zertifikat wieder für gültig zu erklären, markieren Sie es wieder in der ersten Spalte und klicken auf **Als gültig erklären**.

Zertifikate verwalten im LANmonitor

Der LANmonitor zeigt die aktiven und widerrufenen Zertifikate sowie die Zertifikatsanfragen der SCEP-Clients an.



Um ein Zertifikat zu widerrufen, klicken Sie mit der rechten Maustaste auf das entsprechende Zertifikat und wählen Sie im Kontextdialog den Punkt **Zertifikat widerrufen** aus.

Eine Übersicht aller widerrufenen Zertifikate sehen Sie im Abschnitt **Widerrufen**.

Zertifikatanfragen von SCEP-Clients sehen Sie im Abschnitt **Wartende Anfragen**. Klicken Sie mit der rechten Maustaste auf die entsprechende Anfrage und wählen Sie im Kontextdialog entweder **Ablehnen** oder **Akzeptieren** aus.

Zertifikate über URL-API erstellen

Die Erstellung von Zertifikaten ist in einer komplexen und ausgedehnten Netz-Infrastruktur komfortabel über eine spezielle API möglich.

Durch den Aufruf einer URL mit angehängten Parametern lässt sich die Erstellung z. B. über ein Skript automatisieren. Die folgenden Parameter sind möglich:

- `a`: Gibt den Profilnamen an.
- `b`: Gibt den allgemeinen Namen (common name) an.
- `c`: Gibt den Familiennamen (surname) an.
- `d`: Gibt die E-Mail (email) an.
- `e`: Gibt die Organisation an.
- `f`: Gibt die Organisations-Einheit (organization unit) an.
- `g`: Gibt den Ort (locality) an.
- `h`: Gibt das Bundesland (state) an.
- `i`: Gibt den Staat (country) an.
- `j`: Gibt die Postleitzahl (postal code) an.
- `k`: Gibt die Seriennummer an.
- `l`: Gibt den Subject-Alternative-Name an.
- `m`: Gibt die Verwendung (key usage) an.
- `n`: Gibt die erweiterte Verwendung (extended key usage) an.
- `o`: Gibt die Schlüssellänge (key length) an.
- `p`: Gibt die Gültigkeitsdauer (validity period) in Tagen an.
- `q`: Gibt das Passwort für die PKCS12-Datei an.
- `r`: Gibt an, ob es sich um ein CA-Zertifikat handelt.

- 1: CA-Zertifikat
- 0: kein CA-Zertifikat

Wichtig: Der Wizard verarbeitet nur die Parameter, für die in der Presets-Tabelle die entsprechenden Zugriffsrechte gesetzt sind.

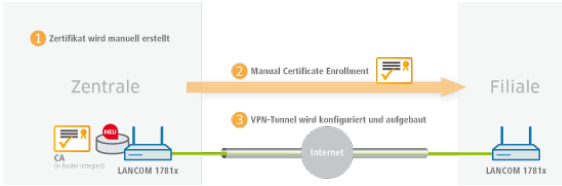
Der Aufruf der URL mit den entsprechenden Parametern sieht wie folgt aus:

```
192.168.10.74/scepwiz/a=VPN&b=iPhone&q=company
```

Tutorials

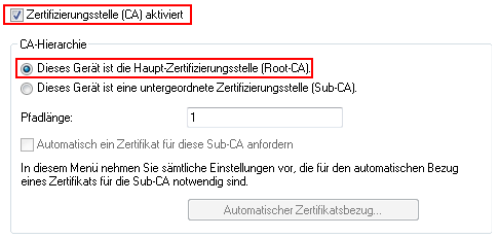
Einrichten einer CA und Erstellen und Nutzen von Zertifikaten für eine VPN-Verbindung

Dieses Tutorial beschreibt, wie Sie eine CA (Certificate-Authority) auf einem LANCOM Router aktivieren und wie die CA Sie dabei unterstützt, neue Zertifikate für eine VPN-Verbindung zwischen zwei LANCOM Routern zu erstellen und zu nutzen (Manuelle Zertifikatsverteilung).



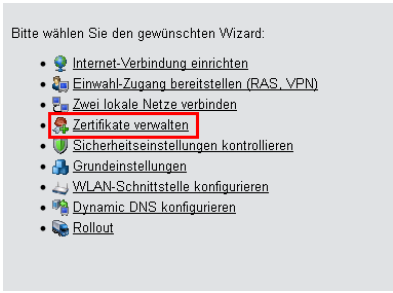
Wichtig: Auf allen Geräten müssen Datum und Uhrzeit gültig sein.

1. Aktivieren Sie die Certificate-Authority in LANconfig und definieren Sie das Gerät als Haupt-Zertifizierungsstelle (Root-CA). Diese Einstellungen finden Sie unter **Zertifikate** > **Zertifizierungsstelle (CA)**.



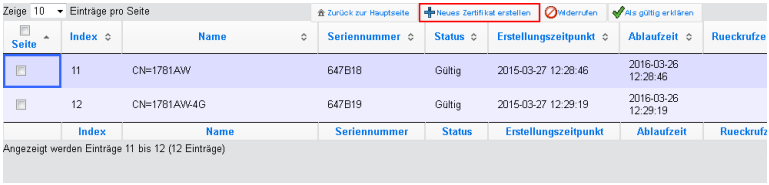
2. Sie haben nun die Möglichkeit, mit der CA Zertifikate für die VPN-Endpunkte zu erstellen, über die Verbindung später eingerichtet wird.

a) In dem Setup-Wizard **Zertifikate verwalten** erstellen Sie Zertifikate einfach und komfortabel.



b) Auf der ersten Seite des Wizards finden Sie eine Übersicht aller bisher ausgestellten Zertifikate der CA.

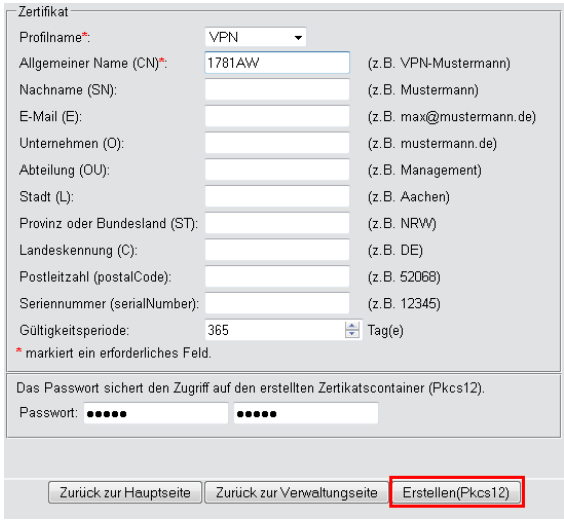
Hinweis: Das Zertifikat der CA selbst wird nicht angezeigt.



Über die Schaltfläche **Neues Zertifikat erstellen** starten Sie den Prozess zur Generierung eines neuen Zertifikates.

c) Unter dem Eintrag **Zertifikate erstellen** haben Sie die Möglichkeit, neben dem Profil und dem offiziellen Namen des Zertifikates (Commonname, kurz CN) noch weitere Zertifikats-Informationen zu konfigurieren,

die bei der Identifizierung des Zertifikates hilfreich sind. Legen Sie die Gültigkeit für das Zertifikat sowie das Passwort für die Pkcs12-Datei fest, in der das erstellte Zertifikat, der entsprechende private Schlüssel und das Zertifikat der CA zusätzlich gespeichert werden.



Haben Sie alle notwendigen und gewünschten Informationen eingetragen, erstellen Sie das Zertifikat über die Schaltfläche **Erstellen (Pkcs12)**. Das Fenster zum Speichern der Pkcs12-Datei erscheint automatisch, sobald das Zertifikat im Gerät erstellt wurde. Dieser Vorgang kann einige Sekunden in Anspruch nehmen.

d) Im Fenster **Speichern der Pkcs12-Datei** wählen Sie den Speicherort und den Namen der Pkcs12-Datei. Als Default wird der Dateiname nach folgendem Format vergeben:
`pkcs12<YYYY_MM_DD-hh_mm_ss>.p12`

YYYY: Jahr

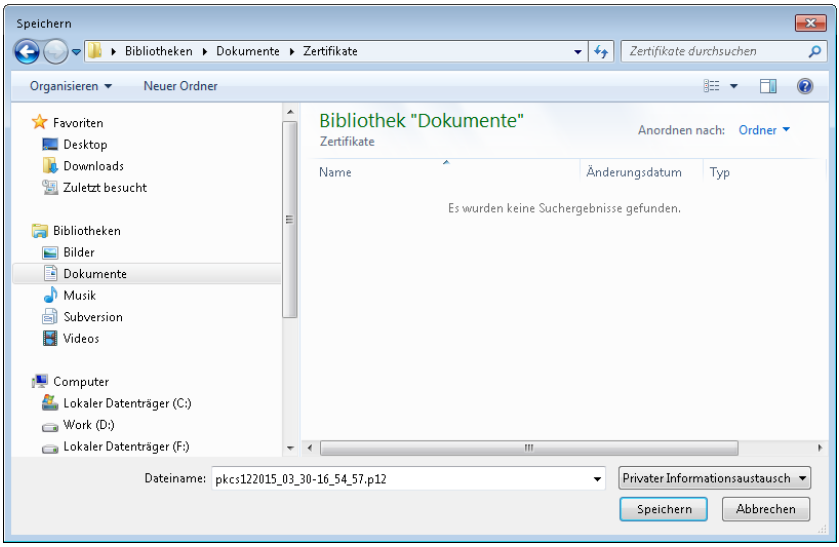
MM: Monat

DD: Tag

hh: Stunde

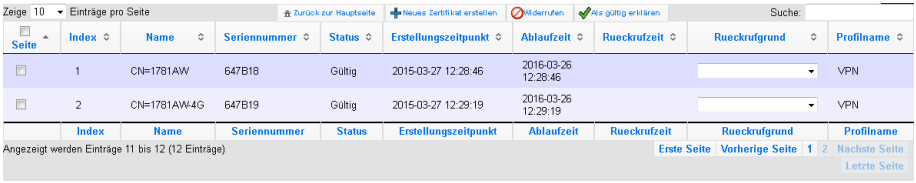
mm: Minute

ss: Sekunde



Hinweis: Der Dateiname kann wie im Beispiel beliebig abgewandelt werden.

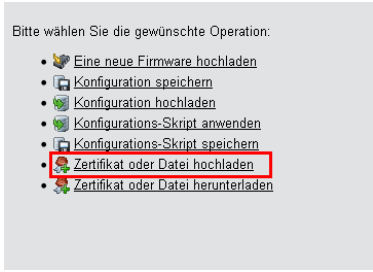
e) Weitere Zertifikate erstellen Sie nach dem gleichen Schema.



Hinweis: Übersichtsseite mit zwei erstellten Zertifikaten.

3. Damit Sie die Zertifikate für eine VPN-Verbindung nutzen können, ist es erforderlich, diese den Geräten zur Verfügung zu stellen.

a) Den Upload auf die jeweiligen VPN-Endpunkte können Sie komfortabel über WEBconfig unter **Dateimanagement** > **Zertifikat oder Datei hochladen** durchführen.



b) **Zertifikat oder Datei hochladen**

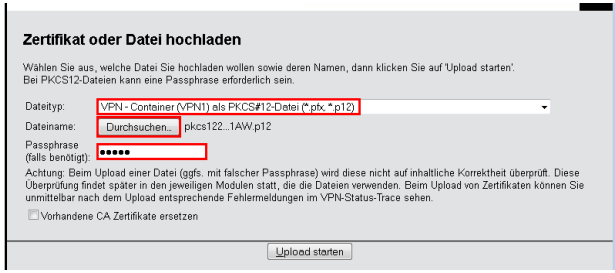
Wählen Sie zunächst den Dateityp und Speicherort. Für VPN-Verbindungen wählen Sie einen ungenutzten VPN-Container.

Hinweis: Solange noch keine Zertifikate für VPN eingerichtet wurden, sind alle VPN-Container ungenutzt.

Im nächsten Schritt wählen Sie die Pkcs12-Datei aus, welche das Zertifikat enthält, das Sie für diesen VPN-Endpunkt nutzen möchten.

Geben Sie das Passwort an, welches Sie in Schritt 2.c beim Erstellen der Datei vergeben haben.

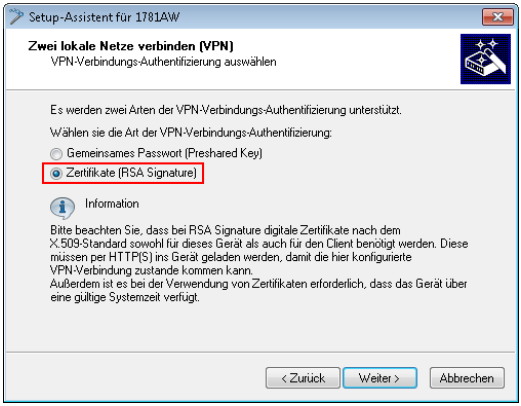
Starten Sie abschließend den Upload.



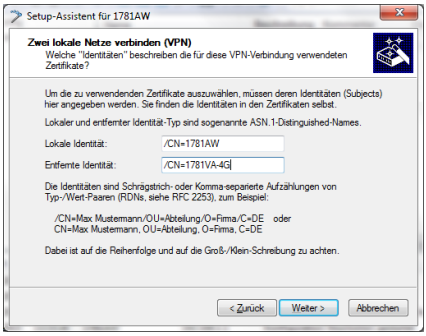
Wichtig: Dieser Vorgang ist für alle VPN-Endpunkte erforderlich. Beachten Sie, dass jeder VPN-Endpunkt ein eigenes Zertifikat braucht.

4. Stellen Sie eine VPN-Verbindung zwischen zwei VPN-Endpunkten her. Dies erfolgt über den Setup-Wizard **Zwei lokale Netze verbinden (VPN)**.

a) Wählen Sie als VPN-Verbindungs-Authentifizierung im Setup-Wizard **Zertifikate (RSA Signature)** aus.



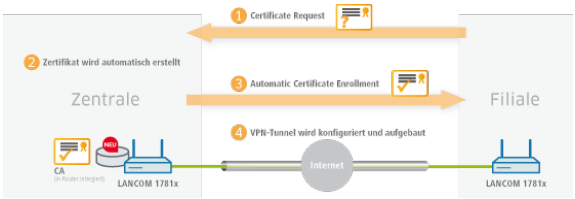
b) Im Fenster **Lokale und entfernte Identitäten** geben Sie den sogenannten "ASN.1-Distinguished-Name" an. Dies ist der offizielle Name des Zertifikates plus aller zusätzlichen Informationen, die Sie in Schritt 2.c angegeben haben. Diese zusätzlichen Informationen finden Sie in der Übersicht der Zertifikate (Schritt 2.e) in der Spalte "Name". Bei dem Punkt **Lokale Identität** geben Sie die Informationen des Zertifikates an, welches sich auf dem lokalen Gerät befindet. Der Punkt **Entfernte Identität** erhält die Zertifikat-Informationen des anderen VPN-Endpunktes.



c) Führen Sie abschließend den Wizard weiter aus. Bei dem anderen VPN-Endpunkt für diese VPN-Verbindung gehen Sie äquivalent vor.

Einrichten einer CA und Erstellen und Nutzen von Zertifikaten für eine VPN-Verbindung mit Zertifikatsrollout über SCEP

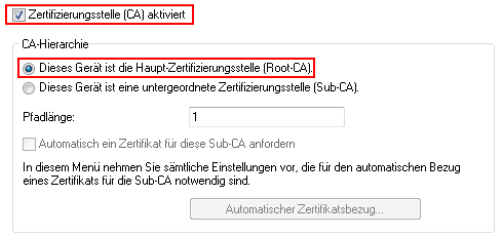
Dieses Tutorial beschreibt, wie Sie eine CA (Certificate-Authority) auf einem LANCOM Router aktivieren und wie die CA Sie dabei unterstützt, neue Zertifikate für eine VPN-Verbindung zwischen zwei LANCOM Routern zu erstellen und zu nutzen (Zertifikatsverteilung über SCEP).



Hinweis: Es werden nur Menüpunkte erläutert, die zur erfolgreichen Durchführung des Tutorials dienen.

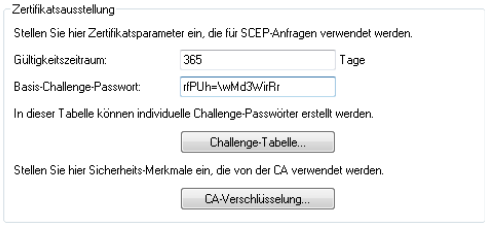
Wichtig: Auf allen Geräten müssen Datum und Uhrzeit gültig und die Certificate-Authority über "HTTPS" erreichbar sein.

1. Aktivieren Sie die Certificate-Authority in WEBconfig oder LANconfig und definieren Sie das Gerät als Hauptzertifizierungsstelle (Root-CA). Diese Einstellungen finden Sie unter **Zertifikate** > **Zertifizierungsstelle (CA)**.



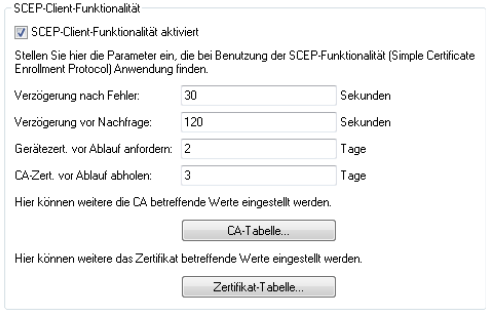
2. SCEP-Clients können Zertifikate durch SCEP (Simple Certificate Enrolement Protocol) automatisch beziehen. Dafür ist es erforderlich, dass Sie in der Haupt-Zertifizierungsstelle (Root-CA) ein Basis-Challenge-Passwort vergeben. Definieren Sie ein Kennwort unter **Zertifikate** > **Zertifikatsbehandlung**.

Hinweis: Schreiben Sie die Konfiguration nach der CA-Aktivierung zurück, generiert die CA automatisch ein Basis-Challenge-Passwort.

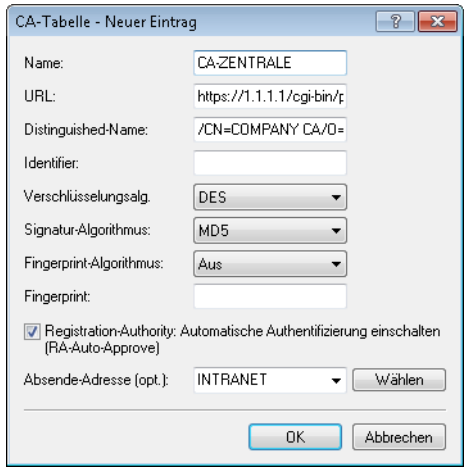


Sie haben nun die Möglichkeit, mit der CA Zertifikate für die VPN-Endpunkte zu erstellen, über die Verbindung später eingerichtet wird.

3. Damit die VPN-Endpunkte über SCEP ein Zertifikat beziehen können, ist es erforderlich, den SCEP-Client auf jedem Endpunkt zu konfigurieren. Diese Einstellung finden Sie unter **Zertifikate** > **SCEP-Client**.



a) Definieren Sie unter **Zertifikate** > **SCEP-Client** > **CA-Tabelle** weiterführende Informationen zur Certificate-Authority. Diese Tabelle enthält Informationen zur CA, von der ein Zertifikat bezogen werden soll.



Name

Der Name kann frei gewählt werden und dient zur Identifizierung auf diesem Gerät.

URL

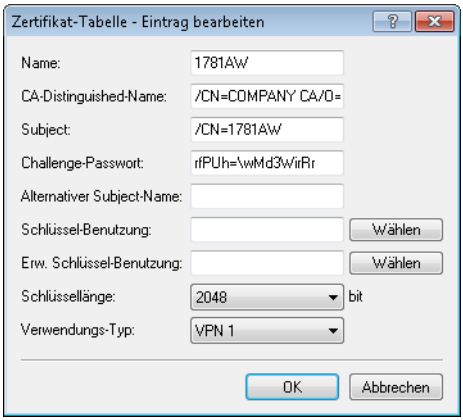
Die URL ist immer nach dem gleichen Schema aufgebaut: `https://<IP-Adresse>/cgi-bin/pkiclient.exe`. Ersetzen Sie `<IP-Adresse>` durch die IPv4-Adresse, unter der die CA aus dem WAN erreichbar ist.

Wichtig: Ist der VPN-Endpunkt gleichzeitig die CA, ist es erforderlich, an dieser Stelle die Loopback-Adresse einzutragen.

Distinguished-Name

Der Distinguished-Name der CA (siehe Screenshot in Schritt 1).

b) Definieren Sie unter **Zertifikate** > **SCEP-Client** > **Zertifikat-Tabelle** weiterführende Informationen zu dem Zertifikat, das von der CA an dieses Gerät vergeben werden soll.



Name

Der Name kann frei gewählt werden und dient zur Identifizierung auf diesem Gerät.

CA-Distinguished-Name

Der CA-Distinguished-Name (siehe Screenshot in Schritt 1).

Subject

Der gewünschte Distinguished-Name des Zertifikates. In diesem Beispiel wird nur der Common-Name gesetzt.

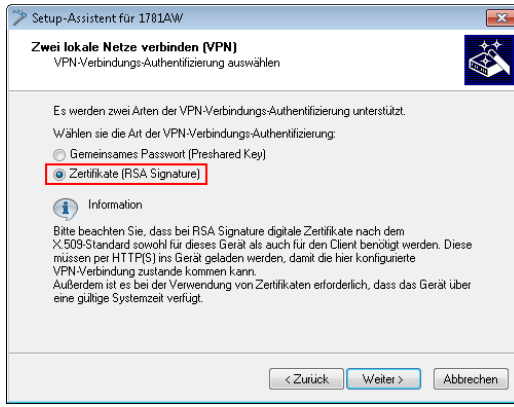
Challenge-Passwort

Das Basis-Challenge-Passwort, das auf der Certificate Authority vergeben wurde (siehe Schritt 2).

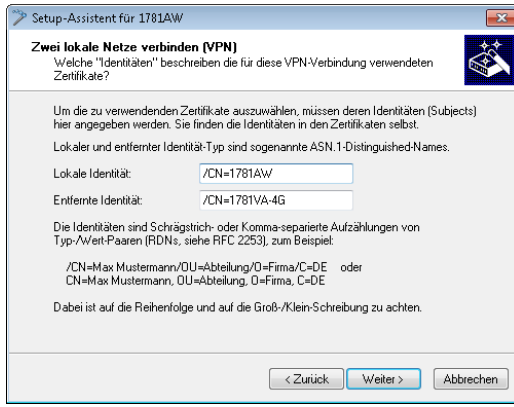
Verwendungstyp

Der Speicherplatz, in dem dieses Zertifikat abgelegt werden soll. In diesem Beispiel "VPN 1".

4. Wenn Sie den SCEP-Client auf jedem VPN-Endpunkt eingerichtet haben, stellen Sie eine VPN-Verbindung zwischen zwei VPN-Endpunkten her. Dies erfolgt über den Setup-Wizard **Zwei lokale Netze verbinden (VPN)**.
   a) Wählen Sie als VPN-Verbindungs-Authentifizierung im Setup-Wizard **Zertifikate (RSA Signature)** aus.



b) Im Fenster **Lokale und entfernte Identitäten** geben Sie den sogenannten "ASN.1-Distinguished-Name" an. Dies ist der offizielle Name des Zertifikates plus aller zusätzlichen Informationen, die Sie in Schritt 3.b unter "Subject" angegeben haben. Bei dem Punkt **Lokale Identität** geben Sie die Informationen des Zertifikates an, welches sich auf dem lokalen Gerät befindet. Der Punkt **Entfernte Identität** erhält die Zertifikat-Informationen des anderen VPN-Endpunktes.



c) Führen Sie abschließend den Wizard weiter aus. Bei dem anderen VPN-Endpunkt für diese VPN-Verbindung gehen Sie äquivalent vor.

10.9 NAT Traversal (NAT-T)

Die nicht ausreichende Anzahl von öffentlich gültigen IP-Adressen hat zur Entwicklung von Verfahren wie IP-Masquerading oder NAT (Network Address Translation) geführt, bei denen ein ganzes lokales Netzwerk hinter einer einzigen, öffentlich gültigen IP-Adresse maskiert wird. Auf diese Weise nutzen alle Clients in einem LAN die gleiche IP-Adresse beim Datenaustausch mit öffentlichen Netzwerken wie dem Internet. Die Zuordnung der ein- und ausgehenden Datenpakete zu den verschiedenen Teilnehmern im Netz wird dabei über eine Verbindung der internen IP-Adressen zu entsprechenden Port-Nummern gewährleistet.

Dieses Verfahren hat sich in den letzten Jahren sehr bewährt und ist mittlerweile Standard in nahezu allen Internet-Routern. Neue Schwierigkeiten in der Verarbeitung der maskierten Datenpakete treten jedoch bei der Verwendung von VPN auf. Da Datenverbindungen über VPN sehr stark gesichert sind, kommen Mechanismen wie Authentifizierung und Verschlüsselung hier hohe Bedeutung zu.

Die Umsetzung der internen IP-Adressen auf die zentrale, öffentlich gültige IP-Adresse des Gateways sowie die Umsetzung von Quell- und Zielports kann in manchen Anwendungen zu Problemen führen, weil dabei z. B. der üblicherweise während der IKE-Verhandlung verwendete UDP-Port 500 verändert wird und die IKE-Verhandlung somit nicht mehr erfolgreich abgeschlossen werden kann. Die Adressänderung über NAT wird also von einem VPN-Gateway als sicherheitskritische Veränderung der Datenpakete gewertet, die VPN-Verhandlung scheitert, es kommt keine Verbindung zustande.

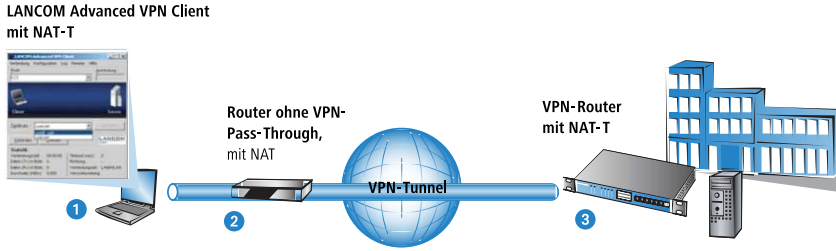
Um auch in diesen Fällen eine VPN-Verbindung erfolgreich aufbauen zu können, steht mit NAT-T (NAT Traversal) ein Verfahren bereit, die beschriebenen Probleme bei der Behandlung von Datenpaketen mit geänderten Adressen zu überwinden.

Hinweis: NAT-T kann nur bei VPN-Verbindungen eingesetzt werden, die zur Authentifizierung ESP (Encapsulating Security Payload) verwenden. ESP berücksichtigt im Gegensatz zu AH (Authentication Header) bei der Ermittlung des Hashwertes zur Authentifizierung nicht den IP-Header der Datenpakete. Der vom Empfänger berechnete Hashwert entspricht daher dem in den Paketen eingetragenen Hashwert.

Setzt die VPN-Verbindung zur Authentifizierung AH ein, kann grundsätzlich keine Verbindung über Strecken mit Network Address Translation aufgebaut werden, da sich die AH-Hashwerte bei der Änderung der IP-Adressen ebenfalls ändern und der Empfänger die Datenpakete als nicht vertrauenswürdig einstufen würde.

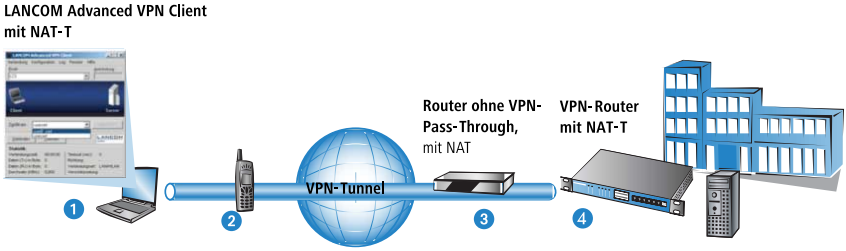
Das Verfahren von NAT Traversal überwindet die Probleme beim VPN-Verbindungsaufbau an den Endpunkten der VPN-Tunnel. Folgende Szenarien lassen sich daher unterscheiden:

- Ein Aussendienstmitarbeiter wählt sich mit einem VPN-Client über einen Router **ohne** „VPN-Pass-Through"-Unterstützung (d.h. IPSec Maskierung), aber **mit** Network Address Translation in den VPN-Router seiner Firma ein.



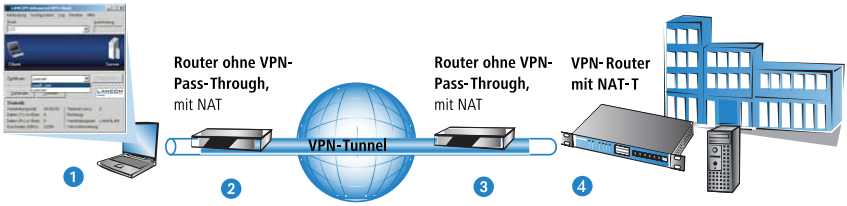
  - Die beiden Tunnelendpunkte VPN-Client **1** und VPN-Router **3** unterstützen das NAT-T-Verfahren und können so auch über den zwischengeschalteten Router eine VPN-Verbindung aufbauen.
  - Der Router **2** macht als NAT-Gerät zwischen den VPN-Endpunkten eine reine Adress-Umsetzung. In diesem Router wird kein NAT-T benötigt, hier müssen jedoch die Ports 500 und 4500 in der Firewall freigeschaltet sein, um die NAT-T-Kommunikation der beiden Tunnelendpunkte zu ermöglichen.

- Im zweiten Anwendungsbeispiel wählt sich der Außendienstmitarbeiter von unterwegs über sein Notebook **1** und ein Mobiltelefon oder Modem **2** in das Netzwerk der Zentrale ein.



- Dabei steht in der Zentrale der VPN-Router **4** hinter einem Abschlussrouter **3**, der nur den Internetzugang mit der Adressumsetzung bereitstellt.
- Die beiden Tunnelendpunkte VPN-Client **1** und VPN-Router **4** können über das NAT-T-Verfahren wie im ersten Beispiel eine VPN-Verbindung aufbauen.
- Im Abschlussrouter **2** müssen jedoch die Ports 500 und 4500 in der Firewall freigeschaltet sein, zusätzlich muss das Port-Forwarding in diesem Router aktiviert werden.

▶ In der Kombination der beiden vorhergehenden Fälle stehen auf beiden Seiten der Verbindung reine NAT-Router **2** und **3**. Die VPN-Strecke wird zwischen dem VPN-Client **1** und VPN-Router **4** aufgebaut.



Die beiden Router **2** und **3** müssen über die Firewallfreischaltung der Ports 500 und 4500 die NAT-T-Verbindung zwischen den Tunnelendpunkten zulassen, im Abschlussrouter der Zentrale muss zusätzlich das Port-Forwarding aktiviert werden.

Um dieses Verfahren zu ermöglichen, müssen beide Seiten der VPN-Verbindung NAT-T beherrschen. Der Ablauf der VPN-Verbindungsaufbaus sieht (reduziert auf die NAT-T-relevanten Vorgänge) so aus:

1. In einer frühen Phase der IKE-Verhandlung wird daher überprüft, ob die beiden Seiten der VPN-Verbindung NAT-T-fähig sind.

2. Im zweiten Schritt wird dann geprüft, ob auf der Strecke zwischen den beiden Tunnelendpunkten eine Adressumsetzung nach NAT stattfindet und an welcher Stelle der Verbindung sich die NAT-Geräte befinden.
3. Um die Probleme mit den möglicherweise veränderten Ports zu umgehen, werden anschließend alle Verhandlungs- und Datenpakete nur noch über den UDP-Port 4500 verschickt, sofern ein NAT-Gerät gefunden wurde.

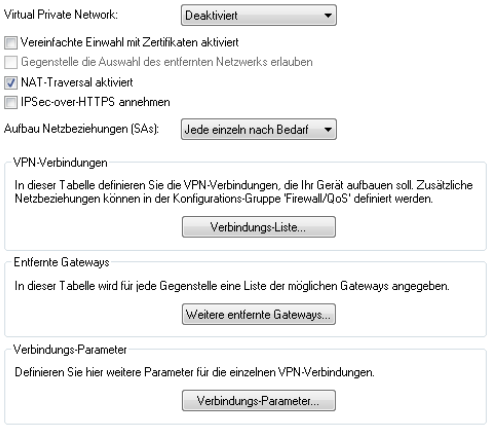
   Hinweis: Achten Sie darauf, dass neben dem UDP-Port 500 auch der UDP-Port 4500 bei Verwendung von NAT-T in der Firewall freigeschaltet ist, wenn das Gerät als NAT-Router zwischen den VPN-Endpunkten fungiert! Bei Verwendung des Firewall-Assistenten in LANconfig wird dieser Port automatisch freigeschaltet.

   Sofern die VPN-Verbindungen erstmals auf Geräten mit einer Firmware-Version 5.20 oder neuer mit dem VPN-Assistenten und anschließend dem Firewall-Assistenten von LANconfig angelegt werden, sind für die NAT-Router keine zusätzlichen Einstellungen an der Firewall erforderlich.

4. Im folgenden werden die Datenpakete noch einmal in UDP-Pakete verpackt (UDP-Encapsulation) und ebenfalls über den Port 4500 versendet. Durch diese zusätzliche Kapselung ist die Veränderung der IP-Adressen für die VPN-Verhandlung nicht mehr relevant, der VPN-Tunnel kann ohne Probleme aufgebaut werden. Auf der Gegenseite der Verbindung werden die IP-Daten wieder vom zusätzlichen UDP-Header befreit und können ohne weiteres vom Router verarbeitet werden.

Zur Verwendung dieses Verfahrens müssen beide Seiten der VPN-Verbindung NAT-T verwenden.

Den Schalter zur Aktivierung von NAT-T finden Sie in LANconfig im Konfigurationsbereich 'VPN' auf der Registerkarte 'Allgemein'.



Unter WEBconfig, Telnet oder SSH-Client finden Sie die Aktivierung von NAT-T auf folgenden Pfaden:

Konfigurationstool	*Menü/Tabelle*
WEBconfig	HiLCOS-Menübaum / Setup / VPN / NAT-T-Operating
Terminal/Telnet	`Setup/VPN/NAT-T-Operating`

10.10 Extended Authentication Protocol (XAUTH)

10.10.1 Einleitung

Bei der Einwahl von Gegenstellen über WAN-Verbindungen (z. B. über PPP) werden oft RADIUS-Server eingesetzt, um die Benutzer zu authentifizieren. Die üblichen WAN-Verbindungen wurden im Laufe der Zeit dann immer mehr von sichereren (verschlüsselten) und kostengünstigeren VPN-Verbindungen verdrängt. Der Aufbau von VPN-Verbindungen über IPSec mit IKE erlaubt jedoch keine unidirektionale Authentifizierung von Benutzern über RADIUS o. ä. .

Das Extended Authentication Protocol (XAUTH) bietet eine Möglichkeit, die Authentifizierung bei der Verhandlung von IPSec-Verbindungen um eine zusätzliche Stufe zu erweitern, in der die Benutzerdaten authentifiziert werden

können. Dazu wird zwischen der ersten und der zweiten IKE-Verhandlungsphase eine zusätzliche Authentifizierung mit XAUTH-Benutzernamen und XAUTH-Kennwort durchgeführt, welche durch die zuvor ausgehandelte Verschlüsselung geschützt ist. Diese Authentifizierung kann über einen RADIUS-Server erfolgen und so die Weiterverwendung der vorhandenen RADIUS-Datenbanken bei der Migration auf VPN-Verbindungen für die Einwahl-Clients ermöglichen. Alternativ kann die Authentifizierung eine interne Benutzertabelle des Gerätes verwenden.

Hinweis: Um die Verwendung von XAUTH besonders sicher zu gestalten, sollten Sie nach Möglichkeit anstelle des Preshared-Key-Verfahrens (PSK) die Einwahl über RSA-SIG (Zertifikate) verwenden. Stellen Sie dabei sicher, dass das VPN-Gateway nur das Zertifikat der jeweils richtigen Gegenstelle akzeptiert (und nicht alle von der gleichen CA ausgestellten Zertifikate).

10.10.2 XAUTH in der Firmware

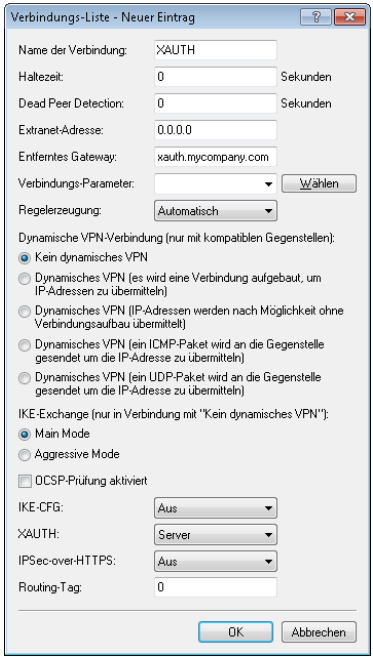
Im Gerät nutzt das XAUTH-Protokoll die Einträge in der PPP-Tabelle zur Authentifizierung der Gegenstelle. Die Verwendung der Einträge in der PPP-Tabelle ist dabei von der Richtung des Verbindungsaufbaus abhängig, also von der XAUTH-Betriebsart:

XAUTH-Betriebsart	*Server*	*Client*
XAUTH-Benutzername	Gegenstelle aus der PPP-Tabelle.	Benutzername aus der PPP-Tabelle.
	Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle dem übermittelten XAUTH-Benutzernamen entspricht. Die PPP-Gegenstelle muss dabei auch der verwendeten VPN-Gegenstelle entsprechen.	Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle der verwendeten VPN-Gegenstelle entspricht.
XAUTH-Kennwort	Kennwort aus der PPP-Tabelle.	Kennwort aus der PPP-Tabelle.

10.10.3 Konfiguration von XAUTH

Die Verwendung des XAUTH-Protokolls wird für jede VPN-Gegenstelle separat vorgenommen. Dabei wird lediglich der XAUTH-Betriebsmodus festgelegt.

LANconfig: VPN / Allgemein / Verbindungs-Liste



WEBconfig: Setup / VPN / VPN-Gegenstellen

- XAUTH

  Aktiviert die Verwendung von XAUTH für die gewählte VPN-Gegenstelle.

  Mögliche Werte:

  – Client: In der Betriebsart als XAUTH-Client startet das Gerät die erste Phase der IKE-Verhandlung (Main Mode oder Aggressive Mode) und wartet dann auf den Authentifizierungs-Request vom XAUTH-Server. Auf diesen Request antwortet der XAUTH-Client mit dem Benutzernamen und dem Kennwort aus dem Eintrag der PPP-Tabelle, in dem die PPP-Gegenstelle der hier definierten VPN-Gegenstelle entspricht. Zu

der VPN-Gegenstelle muss es also eine gleichnamige PPP-Gegenstelle geben. Der in der PPP-Tabelle definierte Benutzername weicht üblicherweise von dem Gegenstellennamen ab.

- Server: In der Betriebsart als XAUTH-Server startet das Gerät nach erfolgreicher Verhandlung der ersten IKE-Verhandlung die Authentifizierung mit einem Request an den XAUTH-Client, der daraufhin mit seinem Benutzernamen und Kennwort antwortet. Der XAUTH-Server sucht den übermittelten Benutzernamen in den Gegenstellennamen der PPP-Tabelle und prüft bei Übereinstimmung das Kennwort. Der Benutzername für diesen Eintrag in der PPP-Tabelle wird nicht verwendet.
- Aus: Bei der Verbindung zu dieser Gegenstelle wird keine XAUTH-Authentifizierung durchgeführt.

Default:

- Aus

Hinweis: Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

10.10.4 XAUTH mit externem RADIUS-Server

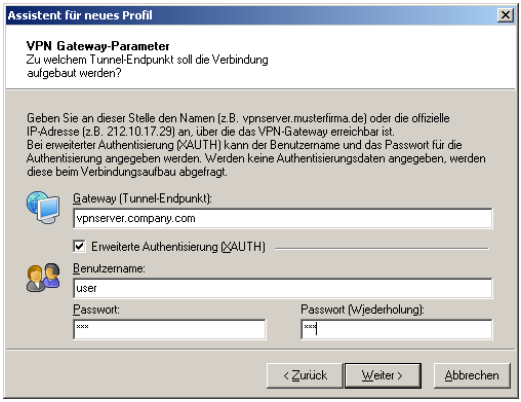
Seit der Firmware-Version 7.60 kann ein Router die Gegenstelle auch über das Extended Authentication Protocol (XAUTH) identifizieren und authentifizieren. Zur Authentifizierung wurden dabei die Benutzerdaten aus der PPP-Liste herangezogen.

Ab der Firmware-Version 7.80 kann die XAUTH-Authentifizierung auch an einen (externen) RADIUS-Server weitergereicht werden. So können z. B. die auf dem RADIUS-Server schon vorhandenen RAS-Benutzerdaten komfortabel weiter genutzt werden, wenn die RADIUS-authentifizierte Einwahl über PPP auf VPN mit XAUTH umgestellt wird.

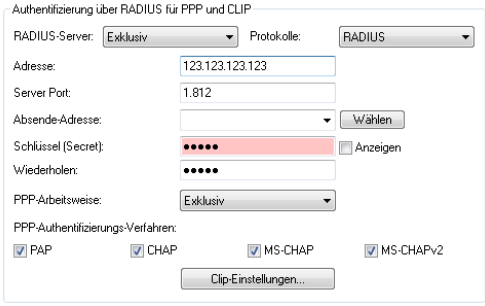
Um einen Einwahlzugang über VPN zusätzlich mit XAUTH zu authentifizieren, gehen Sie folgendermaßen vor:

1. Richten Sie einen VPN-Einwahlzugang ein, z. B. mit dem Setup-Assistenten von LANconfig.

2. Aktivieren Sie im VPN-Client der einwählenden Station die Verwendung von XAUTH. Tragen Sie als Benutzernamen und Kennwort die Werte ein, die auch im RADIUS-Server hinterlegt sind.



3. Aktivieren Sie die Authentifizierung der Einwahlgegenstellen über das XAUTH-Protokoll an einem externen RADIUS-Server. Aktivieren Sie unter LANconfig im Konfigurationsbereich **Kommunikation** auf der Registerkarte **RADIUS** für den RADIUS-Server die Betriebsart “Exklusiv”. In dieser Einstellung werden die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert.



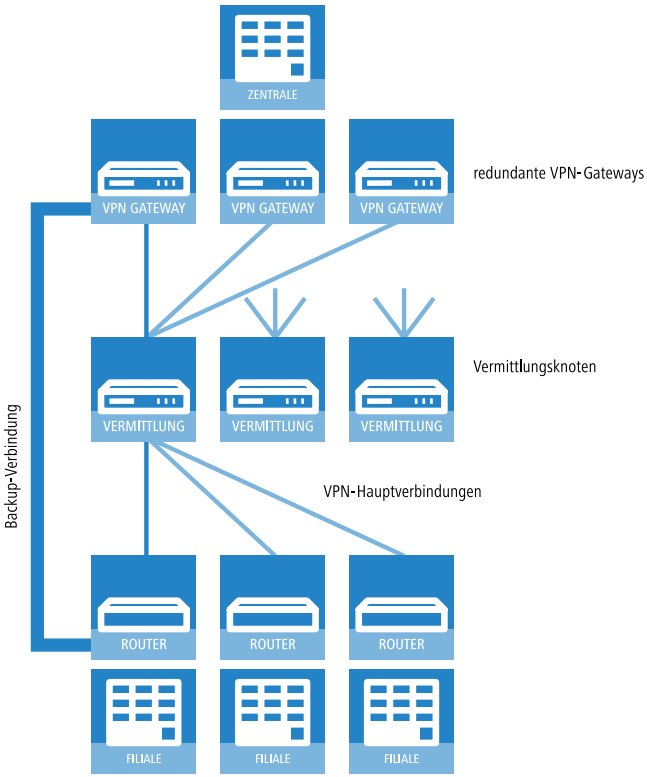
4. Geben Sie außerdem für den externen RADIUS-Server die IP-Adresse, den Port, das Protokoll und den Schlüssel an.
5. Stellen Sie auch die PPP-Arbeitsweise auf “Exklusiv” ein, damit die eingehenden XAUTH-Anfragen ausschließlich über den RADIUS-Server authentifiziert werden.

10.11 Backup über alternative VPN-Verbindung

10.11.1 Einleitung

Das Thema der Backup-Verbindungen ist gerade in verteilten Standorten mit mehreren Filialen, die über VPN an die Zentrale angebunden sind, ein zentrales Thema für die Verfügbarkeit von unternehmenskritischen Anwendungen. Bei einer direkten Beziehung von Routern in den Filialen zu redundanten Routern in der Zentrale ist das Backup einfach zu lösen: Ist ein Router in der Zentrale nicht über Internet erreichbar, kann sich die Filiale in einen anderen Router der Zentrale einwählen. Die Kommunikation der Geräte über die verfügbaren Routen läuft dabei über RIP.

In sehr großen Netzstrukturen sind die Filialen jedoch oft nicht direkt mit der Zentrale verbunden – mehrere Standorte laufen zunächst in einem Vermittlungsknoten zusammen, die Vermittlungsknoten sind dann an die Zentrale angebunden. Ist der Vermittlungsknoten für die Filiale vorübergehend nicht erreichbar, könnte die Filiale eine Backup-Verbindung direkt in die Zentrale aufbauen.



Das gelingt allerdings nur über eine ISDN-Verbindung, die aus Kostengründen und wegen der geringen Bandbreite oft nicht erwünscht ist. Eine parallele Backup-Verbindung direkt über VPN führt aus folgenden Gründen nicht zum Ziel:

- In der Zentrale sind nur die Vermittlungsknoten als VPN-Gegenstellen definiert, alle Routen zu den Filialen laufen über diese Vermittlungsknoten. Versucht eine Filiale eine direkte Verbindung zur Zentrale aufzubauen, so wird dieser Aufbau abgelehnt. Und selbst wenn diese Verbindung zustande kommen würde, bleiben in der Zentrale die Routen zu den Filialen über die Vermittlungsknoten bestehen, denn der Vermittlungsknoten ist ja aus Sicht der Zentrale noch erreichbar.

- Der Vermittlungsknoten erfährt nichts über eine evtl. vorhandene Direktverbindung der Filiale an die Zentrale, er kann also die Ziele im Netz der Filiale nicht über den Umweg der Zentrale erreichen.
- Von der Zentrale aus ist über die reguläre VPN-Verbindung, sowohl das Netz des Vermittlungsknotens, als auch das Netz der Filiale erreichbar. Über eine direkte VPN-Verbindung der Filiale in die Zentrale ist aber nur das Filialnetz erreichbar. Der Router in der Zentrale kann aufgrund dieser unterschiedlichen Eigenschaften die direkte Verbindung nicht als Backup für die reguläre Verbindung akzeptieren.
- Die Filiale kann die reguläre Verbindung zum Vermittlungsknoten nicht mehr aufbauen, weil der Eindeutigkeitsgrundsatz der IPsec-Regeln keine zweite Verbindung mit gleichem Regelsatz zulässt. Die IPSec-Regeln enthalten neben den Angaben zur Verschlüsselung auch die sogenannten Netzbeziehungen, also die IP-Adressen der Netzwerke auf beiden Seiten der Verbindung. Diese Netzbeziehungen dürfen nur einmal im VPN-Regelsatz vorkommen. Im Backupfall müssten aber zwei Regeln für dieselbe Netzbeziehung existieren – einmal für die Backup-Verbindung und einmal für die neu aufzubauende Hauptverbindung.

10.11.2 Backup-fähige Netzstruktur

Um auch für diese Anwendungen ein funktionsfähiges Backup aufbauen zu können, müssen die in den folgenden Abschnitten beschriebenen Aspekte erfüllt sein.

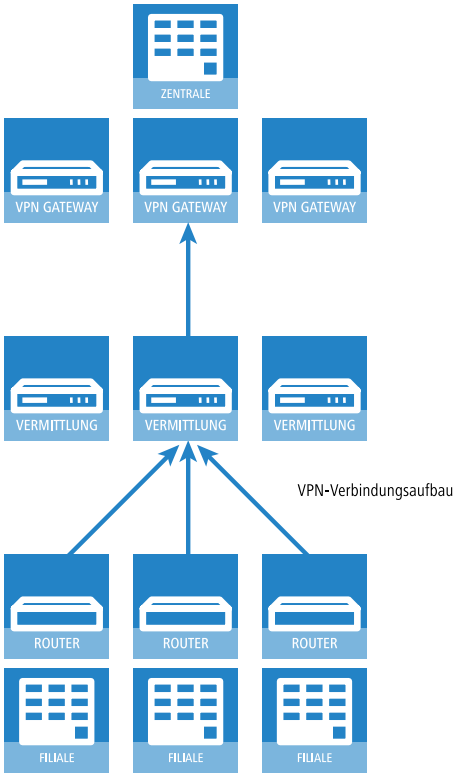
Grundvorraussetzungen

Grundvoraussetzung für die hier beschriebene Backup-Funktion ist die Einrichtung einer “Dynamic VPN”-Verbindung zwischen Filialen und Vermittlungsknoten sowie die Aktivierung der Funktionen “vereinfachten Einwahl mit Zertifikaten“ und “Gegenstelle die Auswahl des entfernten Netzes erlauben“ in den VPN-Gateways der Zentrale.

Hierarchie beim VPN-Verbindungsaufbau

Damit die Filialen im Backup-Fall eine Verbindung zum Netz der Zentrale aufbauen können, muss eine definierte Hierarchie für den Verbindungsaufbau eingehalten werden. Dabei werden die Verbindungen immer nur von den

„unteren“ zu den „oberen“ Netzen hergestellt, also von der Filiale zum Vermittlungsknoten, vom Vermittlungsknoten zur Zentrale.



In der Zentrale müssen alle Verbindungen also nur passiv angenommen werden. Die Vermittlungsknoten nehmen ebenfalls die Verbindungen der Filialen passiv an, bauen aber die Verbindungen zur Zentrale aktiv auf. Diese Hierarchie ist Voraussetzung für die spätere Definition der VPN-Regeln.

Netzwerkdefinitionen

Die Filialen bauen Netzbeziehungen zu den Vermittlungsknoten und zur Zentrale auf, was durch die entsprechenden Regeln abgedeckt sein muss. Dazu müssen entweder alle denkbaren Netzbeziehungen einzeln hinterlegt

werden oder aber die Netzwerke werden so definiert, dass mit einer Regel alle erforderlichen Netzbeziehungen erlaubt werden können. Das gelingt, wenn die Netzwerke z. B. die folgende Struktur von IP-Adressen verwenden:

- Zentralnetz 10.1.1.0/255.255.255.0
- Vermittlungsknoten 10.x.1.0/255.255.255.0
- Filialen 10.x.y.0/255.255.255.0

Mit der folgenden VPN-Regel in den VPN-Gateways der Zentrale können alle erforderlichen Netzbeziehungen zugelassen werden, d. h. alle Gegenstellen aus dem gesamten 10er-Adressraum können Verbindungen zu allen Gateways aufbauen:

- Quelle 10.0.0.0/255.0.0.0
- Ziel 10.0.0.0/255.0.0.0

Da die Filialen über die Zwischenstufe der Vermittlungsknoten mit der Zentrale kommunizieren, müssen auch in den Vermittlungsknoten entsprechende VPN-Regeln angelegt werden. Wenn dabei auch eine Kommunikation mit anderen Unterknoten und Filialen möglich sein soll, werden mit der folgenden VPN-Regel in den Vermittlungsknoten alle erforderlichen Netzbeziehungen zugelassen:

- Quelle 10.x.0.0/255.255.0.0
- Ziel 10.0.0.0/255.0.0.0

Routing-Informationen

Die Routen aus der Zentrale zu den einzelnen Filialen laufen im Normalbetrieb über die Vermittlungsknoten. Im Backup-Fall müssen diese Routen angepasst werden. Damit diese Anpassung automatisch vorgenommen werden kann, wird in den VPN-Gateways der Zentrale die “vereinfachten Einwahl mit Zertifikaten“ aktiviert. Damit kann für alle ankommenden Verbindungen eine gemeinsame Konfiguration vorgenommen werden (über die Default-Einstellungen), wenn die Zertifikate der Gegenstellen mit dem Root-Zertifikat der VPN-Gateways in der Zentrale signiert wurden. Zusätzlich wird dabei den Gegenstellen die Auswahl des entfernten Netzwerks ermöglicht. So können die Router der Filialen während der IKE-Verhandlung in Phase 2 selbst ein Netzwerk vorschlagen, das für die Anbindung verwendet werden soll.

Hinweis: Die Aktivierung der beiden Funktionen “vereinfachten Einwahl mit Zertifikaten“ und “Gegenstelle die Auswahl des entfernten Netzes erlauben“ ist eine notwendige Voraussetzung für die hier beschriebene Backup-Funktion.

Auch für die Vermittlungsknoten müssen die Routing-Informationen im Backup-Fall angepasst werden. Normalerweise werden die Vermittlungsknoten von den Filialen aus direkt erreicht. Im Backup-Fall müssen die Vermittlungsknoten die Daten aus den Filialen über den Umweg der Zentrale empfangen können. Das wird ermöglicht durch eine Route, die das gesamte zusammengefasste Netz (im Beispiel also 10.x.0.0/255.255.0.0 oder, wenn auch eine Kommunikation mit anderen Unterknoten möglich sein soll: 10.0.0.0/255.0.0.0) zur Zentrale überträgt.

Damit die Routen automatisch umgeschaltet werden können, muss auch in den Vermittlungsknoten die Auswahl des entfernten Netzes durch die Gegenstelle erlaubt werden.

Daraus ergibt sich folgender Ablauf beim Aufbau der VPN-Verbindungen:

- Der Vermittlungsknoten baut die Verbindung zur Zentrale auf und fordert alle Netzbeziehungen zu den Filialen an (d. h. er fordert das 10.x.0.0/255.255.0.0 Netz an).
- Die Filale baut die Verbindung zum Vermittlungsknoten auf und fordert ihr Netz (10.x.y.0/255.255.255.0) an.

  Damit können nun Daten von der Filiale über den Vermittlungsknoten zur Zentrale übertragen werden.

Wenn nun die VPN-Verbindung zwischen Filiale und Zentrale abbricht, passiert Folgendes:

- Der Vermittlungsknoten bemerkt den Abbruch aufgrund eines konfigurierten Pollings (DPD) und entfernt die Route zur Filiale.
- Die Filiale baut irgendwann die Backupverbindung zur Zentrale auf und fordert ihr Netz (10.x.y.0/255.255.255.0) an.

  Damit können nun Daten von der Filiale zur Zentrale übertragen werden.

  Wenn die Netze zusammengefasst wurden und die Vermittlungsknoten immer das zusammengefasste Netz (hier im Beispiel also das Netz 10.x.0.0/255.255.0.0 bzw. 10.0.0.0/255.0.0.0) zur Zentrale routen, dann

ist sogar eine Datenübertragung von der Filiale zum Vermittlungsknoten über die Zentrale möglich.

Wenn der Backup-Fall beendet wird, baut die Filiale die Haupverbindung zum Vermittlungsknoten wieder auf:

- Die Filiale baut die Backup-Verbindung wieder ab, wodurch die Zentrale die Route zur Filiale wieder löscht.
- Die Filiale fordert ihr Netz (10.x.y.0/255.255.255.0) wieder beim Vermittlungsknoten an.

  Nun ist wieder problemlos die Kommunikation zwischen Filiale und Vermittlungsknoten möglich.

  Da das Filialnetz ein Subnetz des Netzes im Vermittlungsknoten ist, ist auch sofort wieder die Kommunikation zwischen Filiale und Zentrale über den Vermittlungsknoten möglich. Die Zentrale hat keine eigene Route mehr zur Filiale und überträgt die Daten für die Filiale daher wieder zum Vermittlungsknoten.

  Hinweis: Wenn die Struktur der Netzwerkadressen nicht wie oben beschrieben gestaltet werden kann, muss in der Zentrale die Route zur Filiale statisch konfiguriert werden und auf den Vermittlungsknoten verweisen. Wenn dann die Filiale die Backup-Verbindung aufbaut, dann wird die statische durch die dynamisch angemeldete Route überschrieben. Wird die Backup-Verbindung wieder abgebaut, dann wird die dynamische Route gelöscht und die statische Route erneut aktiv. Soll in diesem Fall die Kommunikation zwischen Filialen und Vermittlungsknoten auch im Backup-Fall gewährleistet werden, müssen auch in den Vermittlungsknoten die Routen zu den Filialen statisch konfiguriert werden.

Aufbau der Backupverbindung

Um dem Grundsatz der eindeutigen IPSec-Regeln zu entsprechen, werden im Backup-Fall zunächst die VPN-Regeln für die Hauptverbindung gelöscht und dann neue Regeln für die Backup-Verbindung angelegt.

Wenn der Aufbau der Backupverbindung scheitert, wählt das Backup-Modul die nächste Backupverbindung aus, wenn mehrere konfiguriert wurden. Wenn

die nächste Backupverbindung eine ISDN-Verbindung ist, dann wird sie ganz normal aufgebaut, d. h. es müssen keine IPSec-Regeln umkonfiguriert werden.

Bei einem ISDN-Backup in der Zentrale muss eine Kopplung der Backup-Verbindung und den normalen VPN-Verbindungen zu den anderen Filialen verhindert werden, da über die VPN-Hauptverbindungen ja nicht nur der Datenverkehr zur Filiale im Backup-Fall läuft, sondern auch der zu den Vermittlungsknoten und allen anderen Filialen. Um diese Kopplung zu verhindern, stehen zwei Möglichkeiten zur Auswahl:

- In die ISDN-Backupverbindung wird eine sehr hohe Distanz für das Netz der Filiale eingetragen. So kann diese Route von den über VPN automatisch übermittelten Routen überschrieben werden.
- Alternativ können die Routen über WAN-RIP gesteuert werden. Dazu wird für jeden B-Kanal eine ISDN-Verbindung mit WAN-RIP-Unterstützung eingerichtet.

Wiederaufbau der Hauptverbindung

Während die Backup-Verbindung aufgebaut wurde, versucht das Gerät die Hauptverbindung wieder herzustellen. Bei diesem Aufbauversuch darf der VPN-Regelsatz zunächst nicht wieder neu erstellt werden, da sonst der Aufbau der Backup-Verbindung scheitert bzw. eine bestehende VPN-Verbindung einfach abreißen würde.

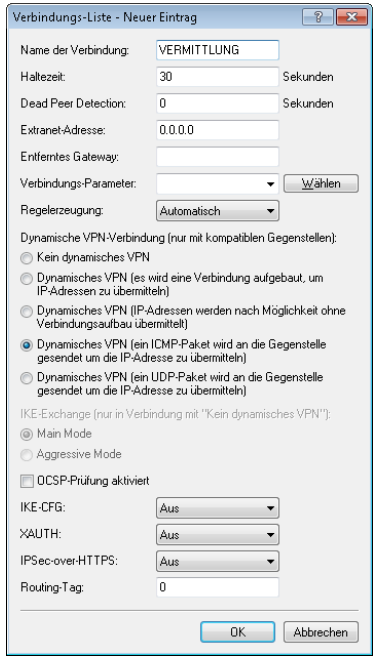
Um das zu verhindern, wird zunächst eine “Dynamic VPN”-Verhandlung mit der Gegenstelle der Hauptverbindung durchgeführt. Verläuft diese Verhandlung erfolgreich, kann die Hauptverbindung wieder aufgebaut werden. Dazu wird zunächst die Backup-Verbindung getrennt und zusätzlich der Backup-Status zurückgesetzt. So wird verhindert, dass die Backup-Verbindung sofort wieder aufgebaut wird. Erst danach wird die Hauptverbindung mit den ursprünglichen VPN-Regeln wieder etabliert.

Hinweis: Die Nutzung der “Dynamic VPN”-Verbindung zwischen Filiale und Vermittlungsknoten ist eine notwendige Voraussetzung für die hier beschriebene Backup-Funktion.

10.11.3 Konfiguration des VPN-Backups

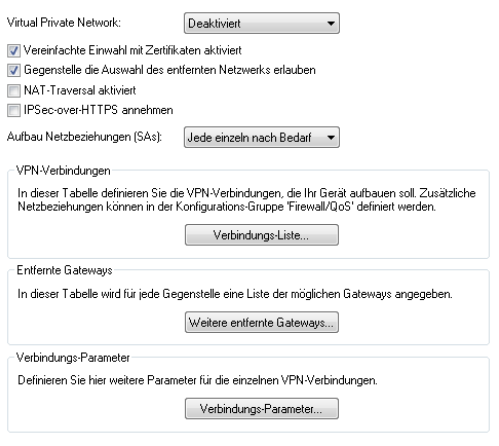
Bei der Konfiguration des VPN-Backups müssen die Filial-, Zentral- und Vermittlungsknoten-Geräte separat betrachtet werden.

- Filiale
  - Für die Hauptverbindung muss “Dynamic VPN” über ICMP/UDP konfiguriert werden.



  - Für die Backupverbindung bestehen keine Anforderungen bezüglich “Dynamic VPN”.
  - Das Backup wird wie beim ISDN-Backup in der Backup-Tabelle konfiguriert.
  - In der Filiale muss die Zentrale als Backupgegenstelle konfiguriert sein.
- Zentrale
  - Die vereinfachte Einwahl mit Zertifikaten muss eingeschaltet sein.
  - Die Auswahl der entfernten Netzwerke durch die Gegenstelle muss aktiviert werden.

– Eine Konfiguration in der Backup-Tabelle ist hier nicht notwendig.



▶ Vermittlungsknoten

– Die VPN-Verbindung zur Zentrale muss vollständig konfiguriert werden.
– Die vereinfachte Einwahl mit Zertifikaten muss eingeschaltet sein.
– Die Auswahl der entfernten Netzwerke durch die Gegenstelle muss aktiviert werden.

Hinweis: Wenn nicht mit "zusammengefassten Netzen" (d. h. das Filialnetz ist ein Subnetz des Vermittlungsknotens und das Vermittlungsknoten-Netz ist ein Subnetz des Zentralnetzes) gearbeitet wird, dann muss im Vermittlungsknoten die Route zur Filiale auf die Zentrale zeigen, damit die Filiale den Vermittlungsknoten auch im Backupfall erreichen kann. Im Normalbetrieb wird diese Route durch die von der Filiale im VPN übermittelte Route überschrieben (weil die Gegenstellen Netzbeziehungen vorgeben dürfen) und kommt somit nur zum Einsatz, wenn die direkte Verbindung abreißt und die Filiale die Backupverbindung aufbaut.

10.12 MPPE für PPTP-Tunnel

Das Verschlüsselungsprotokoll MPPE (Microsoft Point-To-Point Encryption) sichert die Datenübertragung über PPP- und VPN-Verbindungen mit Schlüssellängen von bis zu 128 Bit.

MPPE benutzt zur Verschlüsselung den sogenannten "Stateless Mode", um die Synchronisierung beider Kommunikationspartner sicherzustellen. In diesem Modus ändert sich der Sitzungs-Schlüssel mit jedem übertragenden Datenpaket. Außerdem synchronisieren beide Stationen jedesmal ihre Verschlüsselungs-Tabellen, in denen die Schlüssel zur Datenverschlüsselung gespeichert sind.

VPN-fähige Geräte nutzen MPPE als Möglichkeit zur Verschlüsselung der Datenübertragung über PPTP-Tunnel.

In LANconfig finden Sie diese Einstellung unter **Kommunikation** > **Protokolle** > **PPTP-Liste**

Haben Sie das Verschlüsselungsprotokoll MPPE aktiviert, kommen Verbindungen von Clients ausschließlich unter folgenden Voraussetzungen zustande:

- Der Client baut eine MPPE-gesicherte Verbindung auf. Bei anderen Protokollen lehnt der Router eine Verbindung ab.
- Der Client verwendet mindestens die im Router vorgegebene Schlüssellänge. Bei geringerer Schlüssellänge lehnt der Router eine Verbindung ab, bei stärkerer Verschlüsselung schaltet der Router auf die entsprechende Schlüssellänge um.

10.13 L2TPv2 (Layer 2 Tunneling Protocol Version 2)

Bei L2TP tunnelt ein sogenannter L2TP Access Concentrator (LAC) die PPP-Anfrage eines Clients über eine öffentliche Verbindung (z. B Internet, ATM, Frame Relay) zu einem L2TP Network Server (LNS). Der LNS dient als Gateway zum entfernten Netzwerk. Bei Bedarf authentifiziert dort zunächst ein angeschlossener RADIUS-Server den Client. Anschließend sendet der

LNS die zu verwendende IP-Adresse an den LAC und startet den L2TP-Tunnel. Der LAC gibt die IP-Adresse an den Client weiter. Ab diesem Zeitpunkt ist der Client über eine L2TP-Verbindung Teil des entfernten Netzwerkes.

Innerhalb der Firmware sind der LAC und der PPP-Client in einer Rolle zusammengefasst. Ein Gerät als LAC startet also sowohl den Kontrollkanal als auch die PPP-Sitzung. Im Rahmen der Netzwerkvirtualisierung werden mehrere PPP-Sitzungen in einem L2TP-Tunnel unterstützt. Ein L2TP-fähiges Gerät ist sowohl als LAC als auch als LNS einsetzbar.

Datentypen

L2TP verwendet zwei Typen von Daten:

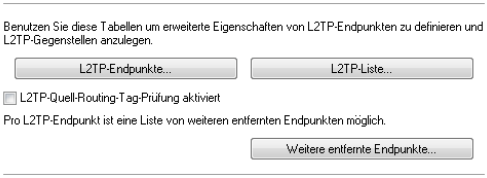
Steuerdaten
: Die Steuerdaten dienen dem Aufbau, der Aufrechterhaltung und dem Abbau von Tunnel-Verbindungen. Die Steuerdaten enthalten eine Datenfluss-Kontrolle, um sicherzustellen, dass Sender und Empfänger die Steuerdaten korrekt austauschen.

Nutzdaten
: Die Nutzdaten kapseln die PPP-Frames, die der LAC und der LNS über den Tunnel austauschen. Im Gegensatz zu den Steuerdaten enthalten die Nutzdaten keine Datenfluss-Kontrolle. Es ist also nicht sichergestellt, dass Sender und Empfänger die Daten fehlerfrei austauschen.

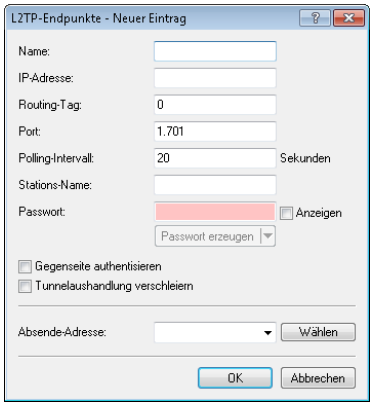
Im Gegensatz zu PPTP, welches Steuer- und Nutzdaten mit unterschiedlichen Protokollen (TCP und GRE) überträgt, nutzt L2TP für beide Datentypen ausschließlich UDP. Sie haben hierbei die Möglichkeit, mehrere logische Nutzdaten-Kanäle je Steuerdaten-Kanal zu betreiben.

10.13.1 Konfiguration der L2TP-Tunnel

Mit LANconfig konfigurieren Sie L2TP unter **Kommunikation** > **Gegenstellen**.



Die Tunnel-Konfiguration für der Steuerdaten eines L2TP-Tunnels zu einem Tunnelendpunkt erfolgt unter **L2TP-Endpunkte**.



Name

Namen des Tunnelendpunktes

IP-Adresse

IP-Adresse des Tunnelendpunktes (IPv4, IPv6, FQDN).

Routing-Tag

Routing-Tag der Route zum Tunnelendpunkt.

Hinweis: Wenn für die Absende-Adresse eine Loopback-Adresse eingetragen ist und das Routing-Tag den Wert "0" besitzt, verwendet das Gerät das Routing-Tag der Loopback-Adresse.

Port

UDP-Port

Polling-Intervall

Poll-Intervall in Sekunden

Stations-Name

Name, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

Passwort

Passwort, mit dem sich das Gerät am Tunnelendpunkt authentifiziert

Gegenseite authentisieren

Wenn zwei Tunnelendpunkte (LAC und LNS) sich gegenseitig authentifizieren sollen, um einen Tunnel aufzubauen, ist diese Option aktiv. In diesem Fall sind im Tunnelendpunkt Stations-Name und Passwort dieses Gerätes als Tunnelendpunkt konfiguriert und ebenfalls die Option **Gegenseite authentisieren** aktiv.

Tunnelaushandlung verschleiern

Wenn bereits die Aushandlung eines Tunnels zwischen LAC und LNS verschlüsselt erfolgen soll, ist diese Option aktiv. Hierbei ver- und entschlüsseln beide L2TP-Partner mit Hilfe eines gemeinsamen "preshared Secrets" bestimmte AVPs (Attribute Value Pair) der L2TP-Nachrichten.

Absende-Adresse

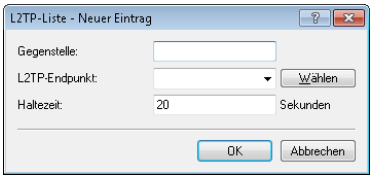
Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Hinweis: Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

Wichtig: Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

Unter **L2TP-Liste** verknüpfen Sie die L2TP-Gegenstellen mit einem zuvor konfigurierten Tunnelendpunkt.



Ein Eintrag in dieser Tabelle ist nur für die folgenden Bedingungen notwendig:

- abgehende Verbindungen,
- ankommende Verbindungen mit einem Idle-Timeout ungleich "20" oder
- wenn ankommende Verbindungen nur einen bestimmten Tunnel nutzen sollen.

Gegenstelle

Name der L2TP-Gegenstelle

L2TP-Endpunkt

Name des Tunnelendpunktes, den diese Gegenstelle verwendet.

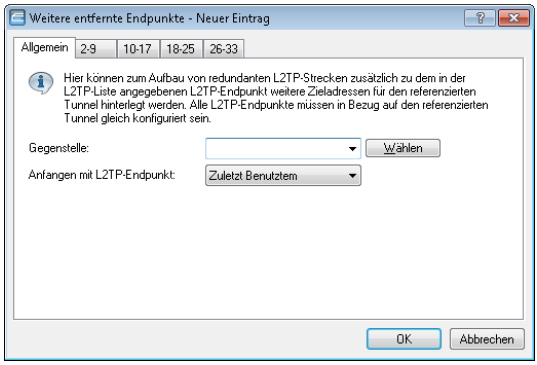
Haltezeit

Bestimmt, wie lange der L2TP-Tunnelendpunkt den Tunnel bei Inaktivität offen hält.

Bei ankommenden Tunnel-Anfragen erfolgt eine Prüfung entweder über RADIUS oder über einen Eintrag des anfragenden Hostes in der L2TP-Endpunkte-Tabelle. Existiert ein Tabellen-Eintrag mit identischer IP-Adresse (oder ist für diesen Eintrag keine IP-Adresse definiert), lässt das Gerät diesen Host für einen Tunnelaufbau zu.

Als zusätzliche Sicherung, um z. B. eine Verschlüsselung der L2TP-Sessions über IPSec zu ermöglichen, kann das Gerät darüber hinaus auch das Routing-Tag der Gegenstelle prüfen, über die es die Daten empfangen hat. Diese Option aktivieren Sie unter **L2TP-Quell-Routing-Tag-Prüfung aktiviert**.

Um bis zu 32 zusätzliche Gateways je Tunnelendpunkt zu konfigurieren, klicken Sie auf **Weitere entfernte Endpunkte**.



Wichtig: Achten Sie darauf, dass alle zusätzlich angegebenen L2TP-Endpunkte identisch zum referenzierten Tunnel-Endpunkt konfiguriert sind.

Gegenstelle

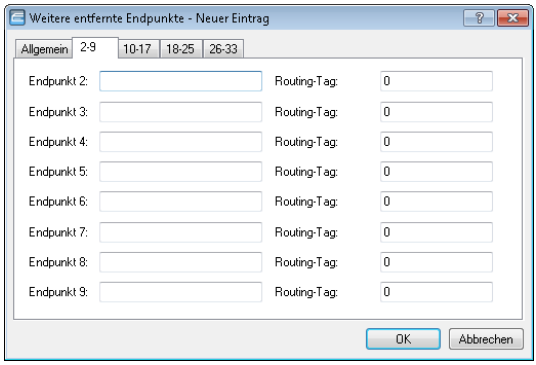
Name des Tunnelendpunktes, wie er in der Tabelle **L2TP-Endpunkte** konfiguriert ist.

Anfangen mit L2TP-Endpunkt

Option zur Auswahl des nächsten Gateways. Folgende Auswahl ist möglich:

- **Zuletzt Benutztem**: Auswahl der zuletzt erfolgreichen Adresse
- **Erstem**: Auswahl des ersten Gateways in der Liste
- **Zufall**: Zufällige Auswahl eines Gateways aus der Liste

Auf den folgenden Reitern konfigurieren Sie die Namen sowie die jeweiligen Routing-Tags der alternativen Gateways.



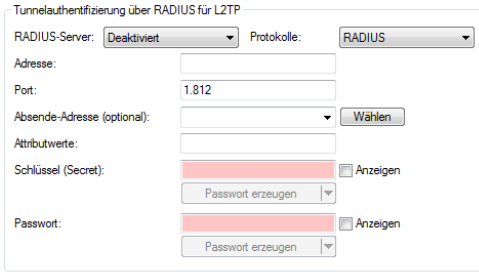
10.13.2 Authentifizierung über RADIUS

Eine RADIUS-Authentifizierung ist bei L2TP in zwei Anwendungsfällen möglich:

- Tunnel-Authentifizierung: Der RADIUS-Server prüft, ob ein LAC eine L2TP-Verbindung aufbauen darf.
- PPP-Session: Der RADIUS-Server prüft die Benutzerdaten der jeweiligen PPP-Session.

Deshalb erfolgt die Konfiguration des RADIUS-Servers für die Authentifizierung des L2TP-Tunnels und der PPP-Benutzerdaten unabhängig voneinander.

Bei einer Tunnel-Authentifizierung über RADIUS konfigurieren Sie die Einstellungen im LANconfig unter **Kommunikation** > **RADIUS** im Abschnitt **Tunnel-Authentifizierung über RADIUS für L2TP**.



RADIUS-Server

Aktiviert bzw. deaktiviert den RADIUS-Server für die Authentifizierung des Tunnelendpunktes, unabhängig von einer Authentifizierung einer PPP-Session. Die folgende Auswahl ist möglich:

- **Deaktiviert**: Der RADIUS-Server ist nicht aktiv für die Authentifizierung eines Tunnelendpunktes.
- **Aktiviert**: Der RADIUS-Server übernimmt die Authentifizierung eines Tunnelendpunktes.
- **Exklusiv**: Aktiviert die Nutzung des externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

Protokolle

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Tunnelendpunkt.

Adresse

IP-Adresse oder DNS-Name des RADIUS-Servers.

Port

Port des RADIUS-Servers

Absende-Adresse

Optionale Absende-Adresse des Gerätes. Falls Sie z. B. Loopback-Adressen konfiguriert haben, ist deren Eingabe hier ebenfalls möglich. Folgende Eingabeformate sind erlaubt:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse stattdessen zu verwenden ist
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Secret)

Shared-Secret zwischen dem RADIUS-Server und dem Gerät

Passwort

Dummy-Passwort für die Tunnel-Authentifizierung

Trifft von einem entfernten Host eine L2TP-Tunnelanfrage ein (Start Control Connection Request), schickt das Gerät eine Anfrage an den für L2TP aktivierten RADIUS-Server. Diese Anfrage enthält u. a. den Namen des Hostes, das Dummy-Passwort, die IP-Adresse des Gerätes sowie den Service-Typ "Outbound-User". Der RADIUS-Server authentifiziert den Host und schickt ein "RADIUS-Accept" an das Gerät zusammen mit dem zu verwendenden Tunnel-Passwort, dem Tunnel-Typ "L2TP" mit dem Tag "0" sowie der Tunnel-Client-Auth-ID, die dem zuvor vom Gerät übermittelten Stationsnamen entsprechen muss. Das Gerät prüft diese Daten und übernimmt bei positivem Ergebnis das Tunnel-Passwort, um den einwählenden Client zu authentifizieren und ggf. die L2TP-Tunnelaushandlung zu verschleiern.

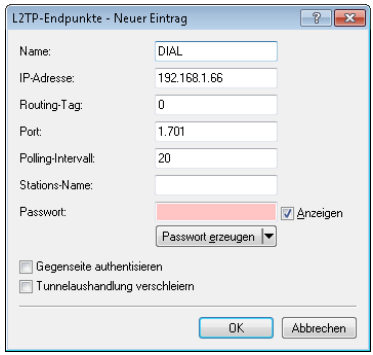
Hinweis: Die Konfiguration des RADIUS-Servers zur Authentifizierung von PPP-Sessions erfolgt, wie es im Abschnitt **Weitere Dienste** > **RADIUS** > **Konfiguration von RADIUS als Authenticator bzw. NAS** > **Einwahl über PPP und RADIUS** beschrieben ist.

10.13.3 Betrieb als L2TP Access Concentrator (LAC)

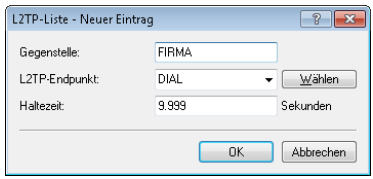
Im folgenden Beispiel baut das Gerät als L2TP Access Concentrator (LAC) einen L2TP-Tunnel zu einem L2TP Network Server (LNS) mit der IP-Adresse 192.168.1.66 auf.

Um das Gerät als LAC zu konfigurieren, gehen Sie wie folgt vor:

1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** einen Eintrag für einen LNS als entferntes L2TP-Gateway.

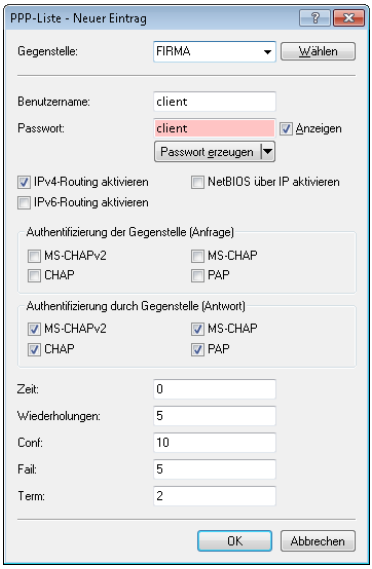


2. Vergeben Sie unter **Kommunikation** > **Protokolle** in der Tabelle **L2TP-Liste** einen Namen für diese Gegenstelle und verbinden Sie sie mit dem zuvor angelegten L2TP-Endpunkt.

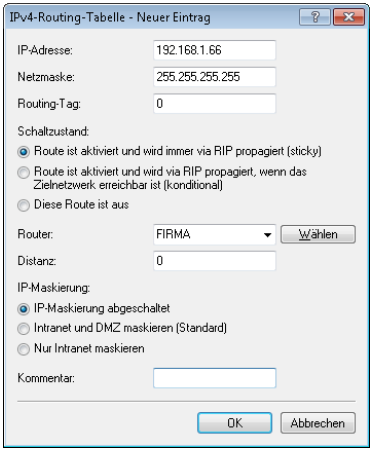


Es ist möglich, mehrere Gegenstellen mit einem L2TP-Tunnel zu verbinden. Dadurch lassen sich mehrere PPP-Sessions durch einen L2TP-Tunnel transportieren. Konfigurieren Sie hierfür in dieser Tabelle mehrere Gegenstellen mit dem gleichen L2TP-Endpunkt.

3. Erstellen Sie unter **Kommunikation** > **Protokolle** in der Tabelle **PPP-Liste** einen Eintrag für den L2TP-Tunnel.



4. Legen Sie unter **Konfiguration** > **IP-Router** > **Routing** in der entsprechenden IPv4- oder IPv6-Routing-Tabelle einen Eintrag für diese Gegenstelle an.

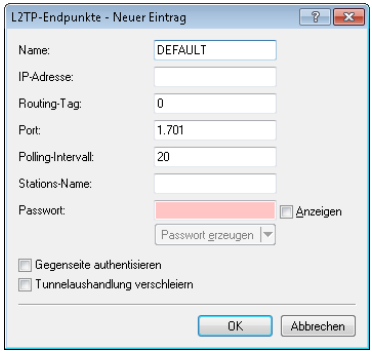


10.13.4 Betrieb als L2TP Network Server (LNS) mit Authentifizierung über RADIUS

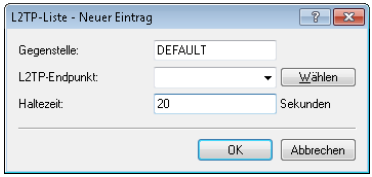
Im folgenden Beispiel arbeitet das Gerät als L2TP Network Server (LNS). Die Authentifizierung der eingehenden L2TP-Tunnel sowie der PPP-Sessions erfolgt über RADIUS.

Um das Gerät als LNS zu konfigurieren, gehen Sie wie folgt vor:

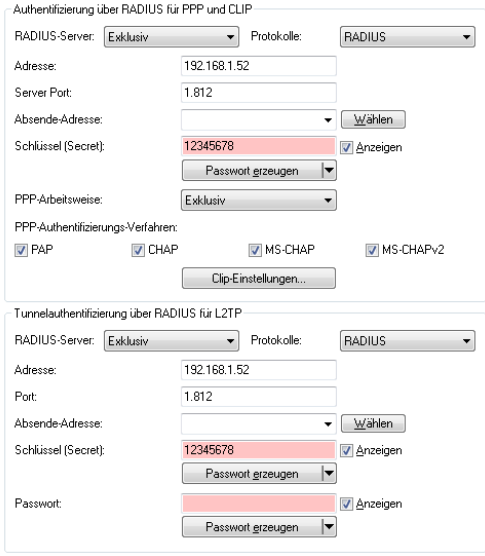
1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** einen Eintrag "DEFAULT".



2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Liste** einen Eintrag "DEFAULT".



3. Konfigurieren Sie unter **Kommunikation** > **RADIUS** den RADIUS-Server.



Hinweis: Den unteren Abschnitt **RADIUS-Server-Einstellungen für L2TP** konfigurieren Sie nur, wenn eine L2TP-Tunnel-Authentifizierung über den RADIUS-Server erfolgen soll.

4. Konfigurieren Sie den RADIUS-Server entsprechend, damit er die Authentifizierung des L2TP-Tunnels und der PPP-Sessions durchführen kann.

Möchte sich ein LAC mit dem Stationsnamen "router1" und dem Passwort "abcde" für den L2TP-Tunnel authentifizieren lassen, konfigurieren Sie den entsprechenden Eintrag im RADIUS-Server (z. B. FreeRADIUS) wie folgt:

```
router1 Cleartext-Password := "password"
        Service-Type = Outbound-User,
        Tunnel-Type  = L2TP,
        Tunnel-Password = "abcde",
        Tunnel-Client-Auth-ID = "router1"
```

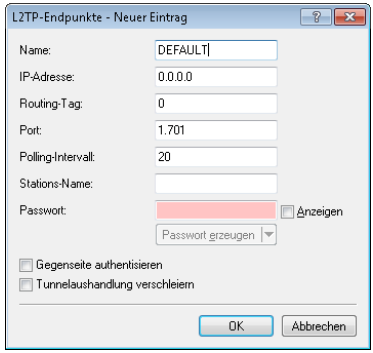
Für die Authentifizierung der PPP-Session eines Benutzers mit dem Benutzernamen "test" und dem Passwort "test" lautet der entsprechende Eintrag im RADIUS-Server wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type = Framed-User,
     Framed-Protocol = PPP
```

10.13.5 Betrieb als L2TP Network Server (LNS) für RAS-Clients

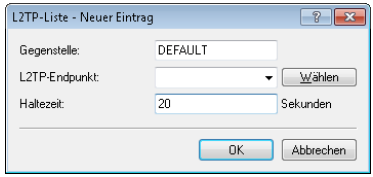
Um das Gerät als L2TP Network Server (LNS) für die Anmeldung von RAS-Clients zu konfigurieren, ohne einen RADIUS-Server im Gerät zu konfigurieren, haben Sie zwei Möglichkeiten:

1. Erstellen Sie unter **Kommunikation** > **Gegenstelle** in der Tabelle **L2TP-Endpunkte** einen Eintrag "DEFAULT".



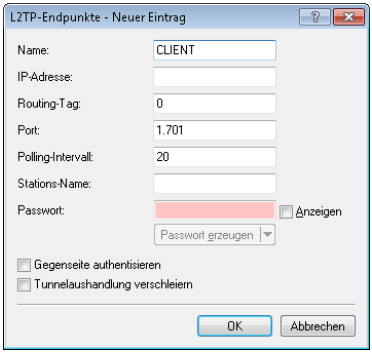
   Der Eintrag für die IP-Adresse lautet "0.0.0.0", da die IP-Adresse des L2TP-LACs dem Gerät unbekannt ist.

2. Konfigurieren Sie anschließend unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Liste** einen Eintrag "DEFAULT".

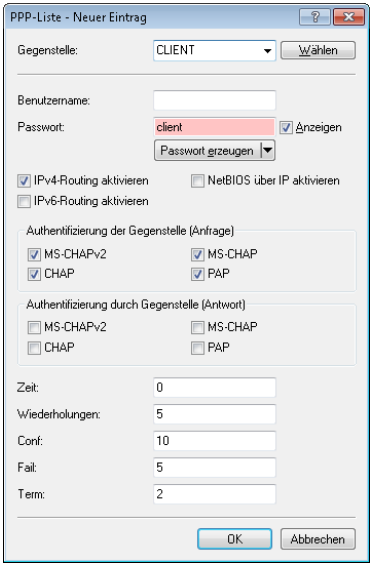


Soll der L2TP-Tunnel dauerhaft verbunden sein, setzen Sie die Haltezeit auf "9999".

3. Alternativ legen Sie unter **Kommunikation** > **Gegenstellen** in der Tabelle **L2TP-Endpunkte** für den RAS-Client einen separaten Eintrag (z. B. "CLIENT") an.



4. Anschließend konfigurieren Sie unter **Kommunikation** > **Protokolle** in der **PPP-Liste** für den Client einen neuen Eintrag.



10.14 Konkrete Verbindungsbeispiele

In diesem Kapitel werden die vier möglichen VPN-Verbindungstypen an Hand konkreter Beispiele veranschaulicht. Die vier Verbindungsarten werden nach der IP-Adressart der beiden VPN-Gateways kategorisiert:

- statisch/statisch
- dynamisch/statisch (die dynamische Seite initiiert die Verbindung)
- statisch/dynamisch (die statische Seite initiiert die Verbindung)
- dynamisch/dynamisch

Zu jeder dieser vier VPN-Verbindungsarten gibt es einen eigenen Abschnitt mit einer Aufführung aller notwendigen Konfigurationsangaben in Form der bereits bekannten Tabelle.

10.14.1 Statisch/statisch

Zwischen den beiden Geräten **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Gateways verfügen über statische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

Angabe	*Zentrale*		*Filiale*
Typ der eigenen IP-Adresse	statisch	→	statisch
Typ IP-Adresse der Gegenstelle	statisch	←	statisch
Name des eigenen Gerätes	Zentrale	→	Filiale
Name der Gegenstelle	Filiale	←	Zentrale
Shared Secret für Verschlüsselung	geheim	↔	geheim
IP-Adresse der Gegenseite	193.10.10.2		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

10.14.2 Dynamisch/statisch

Das VPN-Gateway **Filiale** baut eine VPN-Verbindung zum Gateway **Zentrale** auf. **Filiale** verfügt über eine dynamische IP-Adresse (die ihm bei der Internet-Einwahl von seinem Internet-Anbieter zugewiesen wurde), **Zentrale** hingegen über eine statische. Während des Verbindungsaufbaus überträgt **Filiale** seine

aktuelle IP-Adresse an **Zentrale** (standardmäßig über ICMP, alternativ auch über UDP Port 87).

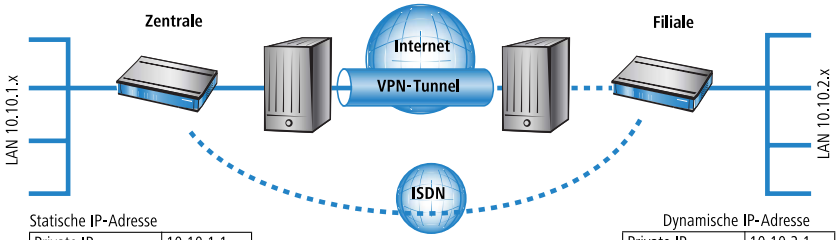
Angabe	*Zentrale*		*Filiale*
Typ der eigenen IP-Adresse	statisch		dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		statisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	⟷	vertraulich
Shared Secret für Verschlüsselung	geheim	⟷	geheim
IP-Adresse der Gegenseite	–		193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Hinweis: Für diesen Verbindungsaufbau ist kein ISDN-Anschluss erforderlich. Die dynamische Seite übermittelt ihre IP-Adresse verschlüsselt über das Internet-Protokoll ICMP (alternativ auch über UDP).

10.14.3 Statisch/dynamisch (mit Dynamic VPN)

In diesem Fall initiiert (im Gegensatz zur dynamisch/statischen Verbindung) die statische Seite den Aufbau der VPN-Verbindung.

.



Das VPN-Gateway **Zentrale** baut eine VPN-Verbindung zu **Filiale** auf. **Zentrale** verfügt über eine statische IP-Adresse, **Filiale** über eine dynamische.

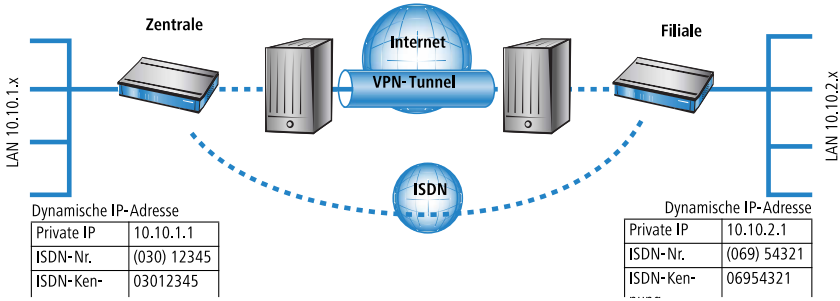
Hinweis: Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Hinweis: Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird als Pendant zur statischen IP-Adresse in der Zentrale auf der Seite der Filiale ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dynamischen IP-Adresse erlaubt.

Angabe	*Zentrale*		*Filiale*
Typ der eigenen IP-Adresse	statisch		dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		statisch
Name des eigenen Gerätes	Zentrale		Filiale
Name der Gegenstelle	Filiale		Zentrale
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich		vertraulich
Shared Secret für Verschlüsselung	geheim		geheim
IP-Adresse der Gegenseite			193.10.10.1
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Hinweis: Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus, über den im Normalfall jedoch keine gebührenpflichtigen Verbindungen aufgebaut werden.

10.14.4 Dynamisch/dynamisch (mit Dynamic VPN)



Zwischen den beiden Geräten **Zentrale** und **Filiale** wird eine VPN-Verbindung aufgebaut. Beide Seiten haben dynamische IP-Adressen. Beide Seiten können den Verbindungsaufbau initiieren.

Hinweis: Die Angaben zur ISDN-Verbindung werden für die Übertragung der IP-Adresse verwendet und nicht für den eigentlichen Verbindungsaufbau ins Internet. Die Internetverbindung wird mit dem Internet-Zugangs-Assistenten konfiguriert.

Hinweis: Alternativ kann diese Anwendung mit Hilfe von Dynamic-DNS gelöst werden. Dabei wird an Stelle einer statischen IP-Adresse ein dynamischer DNS-Name verwendet, der die Zuordnung zur gerade aktuellen dynamischen IP-Adresse erlaubt.

Angabe	*Zentrale*		*Filiale*
Typ der eigenen IP-Adresse	dynamisch	⤫	dynamisch
Typ IP-Adresse der Gegenstelle	dynamisch		dynamisch
Name des eigenen Gerätes	Zentrale	⤫	Filiale
Name der Gegenstelle	Filiale		Zentrale
ISDN-Rufnummer Gegenstelle	06954321		03012345
ISDN-Anruferkennung Gegenstelle	06954321		03012345
Kennwort zur sicheren Übertragung der IP-Adresse	vertraulich	⟷	vertraulich

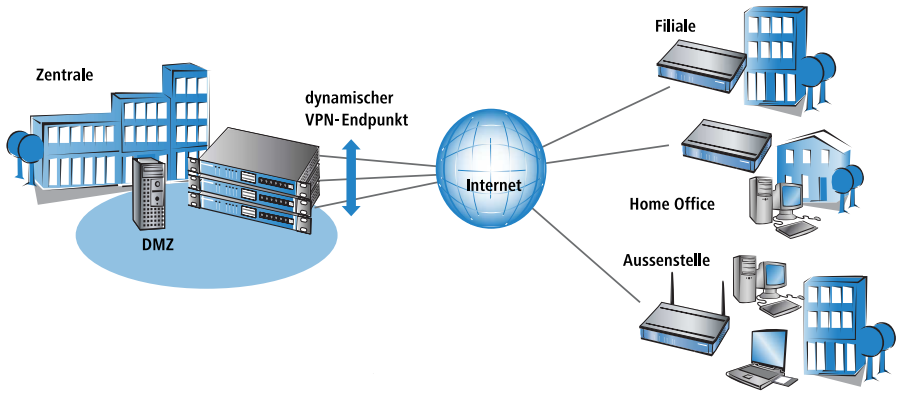
Angabe	*Zentrale*		*Filiale*
Shared Secret für Verschlüsselung	geheim	⟷	geheim
IP-Netzadresse des entfernten Netzes	10.10.2.0		10.10.1.0
Netzmaske des entfernten Netzes	255.255.255.0		255.255.255.0

Hinweis: Der beschriebene Verbindungsaufbau setzt bei beiden VPN-Gateways einen ISDN-Anschluss voraus.

10.14.5 VPN-Verbindungen: hohe Verfügbarkeit mit „Lastenausgleich“

Mehrere VPN-Gateway-Adressen

In verteilten Unternehmensstrukturen, die auf Vernetzung der Standorte über VPN setzen, kommt der Verfügbarkeit der zentralen VPN-Gateways eine besondere Bedeutung zu. Nur wenn diese zentralen Einwahlknoten einwandfrei funktionieren, kann die betriebliche Kommunikation reibungslos ablaufen.



Mit der Möglichkeit, mehrere „Remote-Gateway“-Adressen als „dynamischer VPN-Endpunkt“ für eine VPN-Verbindung zu konfigurieren, bieten VPN-Gateways eine hohe Verfügbarkeit durch den Einsatz redundanter Geräte. Dabei werden in der Zentrale mehrere Gateways mit gleicher VPN-Konfigura-

tion eingesetzt. In den Außenstellen werden alle vorhandenen Gateways als mögliche Gegenstellen für die gewünschte VPN-Verbindung eingetragen. Falls eines der Gateways nicht erreichbar ist, weicht der entfernte Router automatisch auf eine der anderen Gegenstellen aus.

Damit die Rechner im LAN der Zentrale auch wissen, welche Aussenstelle gerade über welches VPN-Gateway erreicht werden kann, werden die jeweils aktuellen Outband-Routen zu den verbundenen Gegenstellen über RIPv2 im Netzwerk der Zentrale propagiert.

Hinweis: Wenn die Außenstellen so konfiguriert werden, dass sie beim Aufbau der VPN-Verbindung die Gegenstelle zufällig auswählen, wird mit diesem Mechanismus die Hochverfügbarkeit mit gleichmäßiger Lastverteilung zwischen den VPN-Gateways in der Zentrale realisiert („Load Balancing“).

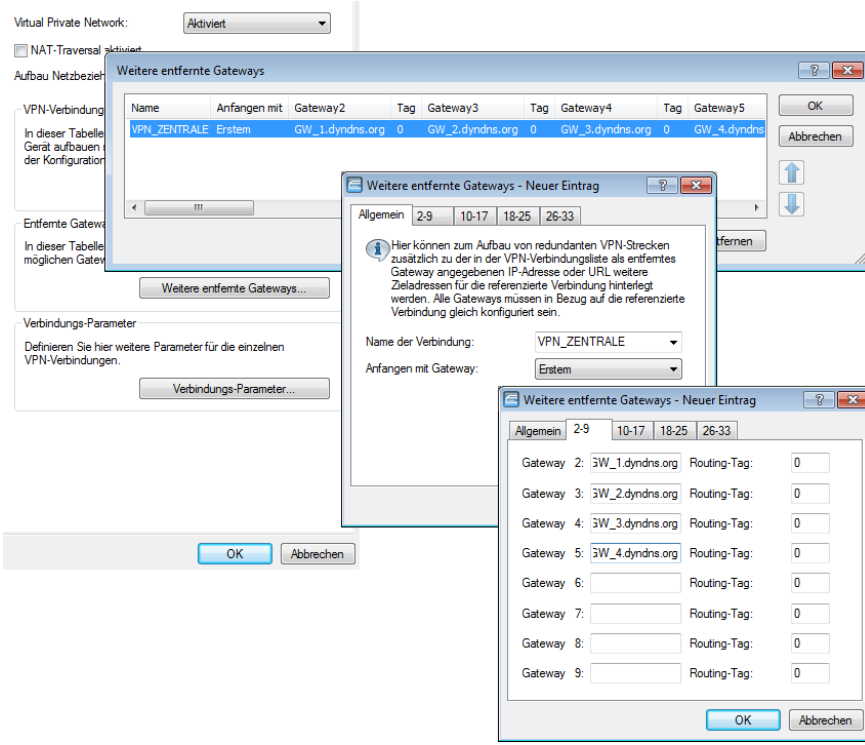
Konfiguration

Bei der Konfiguration tragen Sie in der Liste der „Remote Gateways“ zusätzliche Ziele für eine VPN-Verbindung ein. Die Liste besteht aus den folgenden Einträgen:

- Name: Name der Gegenstelle aus der VPN-Verbindungsliste, das „Ziel“ der VPN-Verbindung.
- Gateway 2 bis Gateway 9: Adresse der alternativen Gateways, als IP-Adresse oder auflösbarer DNS-Name.
- Anfang: In welcher Reihenfolge sollen die Einträge versucht werden. Zur Auswahl stehen:
  - Zuletzt benutzter: Wählt den Eintrag, zu dem zuletzt erfolgreich eine VPN-Verbindung hergestellt werden konnte.
  - Erster: Wählt den ersten Eintrag aus allen konfigurierten Gegenstellen aus.
  - Zufall: Wählt zufällig eine der konfigurierten Gegenstellen aus. Mit dieser Einstellung erreichen Sie ein effektives Load Balancing für die Gateways in der Zentrale.

  Hinweis: Der Eintrag für das Gateway in der VPN-Verbindungsliste kann frei bleiben, wenn alle möglichen Gateways in der Liste der „Remote Gateways“ eingetragen sind.

Bei der Konfiguration mit LANconfig finden Sie die Liste der Gateway-Adressen im Konfigurationsbereich 'VPN' auf die Registerkarte 'Allgemein' unter der Schaltfläche **Entferntes Gateway**.



Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Einstellungen für die Remote-Gateway-Adressen auf folgenden Pfaden:

Konfigurationstool	*Menü/Tabelle*
WEBconfig	HiLCOS-Menübaum / Setup / Config / Remote-Gateway-Liste
Terminal/Telnet	`Setup/VPN/Remote-Gateway-Liste`

Zur Definition der Strategie, nach der die konfigurierten Remote-Gateway-Adressen verwendet werden, stehen folgende Möglichkeiten zur Verfügung:

- `zuletzt-verwendetem`
- `erstem`

- `zufaelligem`

Beispiel:

Mit dem folgenden Befehl legen Sie drei Gateways als Ziel in der Zentrale fest, die zufällig ausgewählt werden:

```
set VPN_ZENTRALE 213.217.69.75 213.217.69.76 213.217.69.77
* * * * * zufaelligem
```

10.15 Wie funktioniert VPN?

Ein VPN muss in der Praxis einer Reihe von Ansprüchen gerecht werden:

- Unbefugte Dritte dürfen die Daten nicht lesen können (Verschlüsselung)
- Ausschluss von Datenmanipulationen (Datenintegrität)
- Zweifelsfreie Feststellung des Absenders der Daten (Authentizität)
- Einfache Handhabung der Schlüssel
- Kompatibilität mit VPN-Geräten verschiedener Hersteller

Diese fünf wichtigen Ziele erreicht VPN durch die Verwendung des weitverbreiteten IPSec-Standards.

10.15.1 IPSec – Die Basis für VPN

Das ursprüngliche IP-Protokoll enthält keinerlei Sicherheitsvorkehrungen. Erschwerend kommt hinzu, dass Pakete unter IP nicht gezielt an den Empfänger gesendet werden, sondern über das gesamte Netzwerksegment an alle angeschlossenen Rechner gestreut werden. Wer auch immer möchte, bedient sich und liest die Pakete mit. Datenmissbrauch ist so möglich.

Deshalb wurde IP weiterentwickelt und es gibt IP inzwischen auch in einer sicheren Variante: IPSec. VPN basiert auf IPSec.

IPSec steht für „**IPSec**urity Protocol“ und ist ursprünglich der Name einer Arbeitsgruppe innerhalb des Interessenverbandes IETF, der **I**nternet **E**ngineering **T**ask **F**orce. Diese Arbeitsgruppe hat über die Jahre ein Rahmenwerk für ein gesichertes IP-Protokoll entwickelt, das heute allgemein als IPSec bezeichnet wird.

Wichtig ist, dass IPSec selber kein Protokoll ist, sondern nur der Standard für ein Protokoll-Rahmenwerk. IPSec besteht in der Tat aus verschiedensten Protokollen und Algorithmen für die Verschlüsselung, die Authentifizierung und das Schlüssel-Management. Diese Standards werden in den folgenden Abschnitten vorgestellt.

Sicherheit im IP-Gewand

IPSec ist (nahezu) vollständig innerhalb in Ebene 3 des OSI-Modells implementiert, also in der Vermittlungsebene (dem Network Layer). Auf Ebene 3 wird in IP-Netzwerken der Verkehr der Datenpakete auf Basis des IP-Protokolls abgewickelt.

Damit ersetzt IPSec das IP-Protokoll. Die Pakete werden unter IPSec intern anders aufgebaut als IP-Pakete. Ihr äußerer Aufbau bleibt dabei aber vollständig kompatibel zu IP. IPSec-Pakete werden deshalb weitgehend problemlos innerhalb bestehender IP-Netze transportiert. Die für den Transport der Pakete zuständigen Geräte im Netzwerk können IPSec-Pakete mit Blick aufs Äußere nicht von IP-Paketen unterscheiden.

Ausnahmen sind bestimmte Firewalls und Proxy-Server, die auch auf den Inhalt der Pakete zugreifen. Die Probleme resultieren dabei aus (teilweise funktionsbedingten) Inkompatibilitäten dieser Geräte mit dem geltenden IP-Standard. Diese Geräte müssen entsprechend an IPSec angepasst werden.

In der nächsten Generation des IP-Standards (IPv6) wird IPSec fest implementiert werden. Man kann deshalb davon ausgehen, dass IPSec auch in Zukunft der wichtigste Standard für virtuelle private Netzwerke sein wird.

10.15.2 Alternativen zu IPSec

IPSec ist ein offener Standard. Er ist unabhängig von einzelnen Herstellern und wird innerhalb der IETF unter Einbezug der interessierten Öffentlichkeit entwickelt. Die IETF steht jedermann offen und verfolgt keine wirtschaftlichen Interessen. Aus dieser offenen Gestaltung zur Zusammenführung verschiedener technischer Ansätze resultiert die breite Anerkennung von IPSec.

Dennoch gab und gibt es andere Ansätze zur Verwirklichung von VPNs. Nur die beiden wichtigsten seien hier erwähnt. Sie setzen nicht auf der Netzwerkebene wie IPSec an, sondern auf Verbindungs- und auf Anwendungsebene.

Sicherheit auf Verbindungsebene – PPTP, L2F, L2TP

Bereits auf der Verbindungsebene (Level 2 des OSI-Modells) können Tunnel gebildet werden. Microsoft und Ascend entwickelten frühzeitig das **P**oint-to-**P**oint **T**unneling **P**rotocol (PPTP). Cisco stellte ein ähnliches Protokoll mit **L**ayer **2F**orwarding (L2F) vor. Beide Hersteller einigten sich auf ein gemeinsames Vorgehen und in der IETF wurde daraus das **L**ayer **2T**unnel **P**rotocol (L2TP).

Der Vorteil dieser Protokolle gegenüber IPSec liegt vor allem darin, dass beliebige Netzwerk-Protokolle auf eine solche sichere Netzwerkverbindung aufgesetzt werden können, insbesondere NetBEUI und IPX.

Ein wesentlicher Nachteil der beschriebenen Protokolle ist die fehlende Sicherheit auf Paketebene. Außerdem wurden die Protokolle speziell für Einwahlverbindungen entwickelt.

Sicherheit auf höherer Ebene – SSL, S/MIME, PGP

Auch auf höheren Ebenen des OSI-Modells lässt sich die Kommunikation durch Verschlüsselung absichern. Bekannte Beispiele für Protokolle dieser Art sind SSL (**S**ecure **S**ocket **L**ayer) vornehmlich für Webbrowser-Verbindungen, S/MIME (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtensions) für E-Mails und PGP (**P**retty **G**ood **P**rivacy) für E-Mails und Dateien.

Bei allen obengenannten Protokollen übernimmt eine Anwendung die Verschlüsselung der übertragenen Daten, beispielsweise der Webbrowser auf der einen Seite und der HTTP-Server auf der anderen Seite.

Ein Nachteil dieser Protokolle ist die Beschränkung auf bestimmte Anwendungen. Für verschiedene Anwendungen werden zudem in aller Regel verschiedene Schlüssel benötigt. Die Verwaltung der Konfiguration wird auf jedem einzelnen Rechner vorgenommen und kann nicht komfortabel nur auf den Gateways erfolgen, wie das bei IPSec möglich ist. Zwar sind Sicherungsprotokolle auf Anwendungsebene intelligenter, schließlich kennen sie die Bedeutung der übertragenen Daten. Zumeist sind sie aber auch deutlich komplexer.

Alle diese Layer-2-Protokolle erlauben nur Ende-Ende-Verbindungen, sind also (ohne Ergänzungen) ungeeignet für die Kopplung ganzer Netzwerke.

Andererseits benötigen diese Mechanismen nicht die geringsten Änderungen der Netzwerkgeräte oder der Zugangssoftware. Zudem können sie im Unterschied zu Protokollen in unteren Netzwerkebenen auch dann noch wirken, wenn die Dateninhalte schon in den Rechner gelangt sind.

Die Kombination ist möglich

Alle genannten Alternativen sind verträglich zu IPSec und daher auch parallel anzuwenden. Auf diese Weise kann das Sicherheitsniveau erhöht werden. Es ist beispielsweise möglich, sich mit einer L2TP-Verbindung ins Internet einzuwählen, einen IPSec-Tunnel zu einem Web-Server aufzubauen und dabei die HTTP-Daten zwischen Webserver und Browser im gesicherten SSL-Modus auszutauschen.

Allerdings beeinträchtigt jede zusätzlich eingesetzte Verschlüsselung den Datendurchsatz. Der Anwender wird im Einzelfall entscheiden, ob ihm die Sicherheit alleine über IPSec ausreicht oder nicht. Nur in seltenen Fällen wird eine höhere Sicherheit tatsächlich notwendig sein. Zumal sich der verwendete Grad an Sicherheit auch innerhalb von IPSec noch einstellen lässt.

10.16 Die Standards hinter IPSec

IPSec basiert auf verschiedenen Protokollen für die verschiedenen Teilfunktionen. Die Protokolle bauen aufeinander auf und ergänzen sich. Die durch dieses Konzept erreichte Modularität ist ein wichtiger Vorteil von IPSec gegenüber anderen Standards. IPSec ist nicht auf bestimmte Protokolle beschränkt, sondern kann jederzeit um zukünftige Entwicklungen ergänzt werden. Die bisher integrierten Protokolle bieten außerdem schon jetzt ein so hohes Maß an Flexibilität, dass IPSec perfekt an nahezu jedes Bedürfnis angepasst werden kann.

10.16.1 Module von IPSec und ihre Aufgaben

IPSec hat eine Reihe von Aufgaben zu erfüllen. Für jede dieser Aufgaben wurde eines oder mehrere Protokolle definiert.

- Sicherung der Authentizität der Pakete
- Verschlüsselung der Pakete

- Übermittlung und Management der Schlüssel

10.16.2 Security Associations – nummerierte Tunnel

Eine logische Verbindung (Tunnel) zwischen zwei IPSec-Geräten wird als SA (**S**ecurity **A**ssociation) bezeichnet. SAs werden selbstständig vom IPSec-Gerät verwaltet. Eine SA besteht aus drei Werten:

- Security Parameter Index (SPI)

  Kennziffer zur Unterscheidung mehrerer logischer Verbindungen zum selben Zielgerät mit denselben Protokollen

- **IP-Ziel-Adresse**
- **Verwendetes Sicherheitsprotokoll**

  Kennzeichnet das bei der Verbindung eingesetzte Sicherheitsprotokoll: AH oder ESP (zu diesen Protokollen in den folgenden Abschnitten mehr).

Eine SA gilt dabei nur für eine Kommunikationsrichtung der Verbindung (simplex). Für eine vollwertige Sende- und Empfangsverbindung werden zwei SAs benötigt. Außerdem gilt eine SA nur für ein eingesetztes Protokoll. Werden AH und ESP verwendet, so sind ebenfalls zwei separate SAs notwendig, also jeweils zwei für jede Kommunikationsrichtung.

Die SAs werden im IPSec-Gerät in einer internen Datenbank verwaltet, in der auch die erweiterten Verbindungsparameter abgelegt werden. Zu diesen Parametern gehören beispielsweise die verwendeten Algorithmen und Schlüssel.

10.16.3 Verschlüsselung der Pakete – das ESP-Protokoll

Das ESP-Protokoll (**E**ncapsulating **S**ecurity **P**ayload) verschlüsselt die Pakete zum Schutz vor unbefugtem Zugriff. Diese ehemals einzige Funktion von ESP wurde in der weiteren Entwicklung des Protokolls um Möglichkeiten zum Schutz der Integrität und zur Feststellung der Authentizität erweitert. Zudem verfügt auch ESP inzwischen über einen wirksamen Schutz gegen Wiedereinspielung von Paketen. ESP bietet damit alle Funktionen von AH an.

Arbeitsweise von ESP

Der Aufbau von ESP ist komplizierter als der von AH. Auch ESP fügt einen Header hinter den IP-Header ein, zusätzlich allerdings auch noch einen eigenen Trailer und einen Block mit ESP-Authentifizierungsdaten.

Transport- und Tunnel-Modus

ESP kann (wie AH auch) in zwei Modi verwendet werden: Im Transport-Modus und im Tunnel-Modus.

Im Transport-Modus wird der IP-Header des ursprünglichen Paketes unverändert gelassen und es werden ESP-Header, die verschlüsselten Daten und die beiden Trailer eingefügt.

Der IP-Header enthält die unveränderte IP-Adresse. Der Transport-Modus kann daher nur zwischen zwei Endpunkten verwendet werden, beispielsweise zur Fernkonfiguration eines Routers. Zur Kopplung von Netzen über das Internet kann der Transport-Modus nicht eingesetzt werden – hier wird ein neuer IP-Header mit der öffentlichen IP-Adresse des Gegenübers benötigt. In diesen Fällen kommt ESP im Tunnel-Modus zum Einsatz.

Im Tunnel-Modus wird das gesamte Paket inkl. dem ursprünglichen IP-Header am Tunnel-Eingang verschlüsselt und authentifiziert und mit ESP-Header und -Trailern versehen. Diesem neuen Paket wird ein neuer IP-Header vorangesetzt, diesmal mit der öffentlichen IP-Adresse des Empfängers am Tunnel-Ende.

Verschlüsselungs-Algorithmen

IPSec setzt als übergeordnetes Protokoll keine bestimmten Verschlüsselungs-Algorithmen voraus. In der Wahl der angewandten Verfahren sind die Hersteller von IPSec-Produkten daher frei. Üblich sind folgende Standards:

- AES – Advanced Encryption Standard

AES ist der offizielle Verschlüsselungsstandard für die Verwendung in US-amerikanischer Regierungsbehörden und damit die wichtigste Verschlüsselungstechnik weltweit. Im Jahr 2000 entschied sich das **N**ational **I**nstitute of **S**tandards and **T**echnology (NIST) nach einem weltweiten Wettbewerb zwischen zahlreichen Verschlüsselungsalgorithmen für den Rijndael-Algorithmus (gesprochen: „Reindoll“) und erklärte ihn 2001 zum AES.

Beim Rijndael-Algorithmus handelt es sich um ein symmetrisches Verschlüsselungsverfahren, das mit variablen Block- und Schlüssellängen arbeitet. Es wurde von den beiden belgischen Kryptografen Joan Daemen und Vincent Rijmen entwickelt und zeichnet sich durch hohe Sicherheit, hohe Flexibilität und hervorragende Effizienz aus.

- DES – Data Encryption Standard

  DES wurde Anfang der 70er Jahre von IBM für die NSA (National Security Agency) entwickelt und war jahrelang weltweiter Verschlüsselungsstandard. Die Schlüssellänge dieses symmetrischen Verfahrens beträgt 56 Bits. Es gilt heute aufgrund der geringen Schlüssellänge als unsicher und wurde vom NIST im Jahr 2000 durch den AES (Rijndael-Algorithmus) ersetzt. Er sollte nicht mehr verwendet werden.

- Triple-DES (auch 3-DES)

  Ist eine Weiterentwicklung des DES. Der herkömmliche DES-Algorithmus wird dreimal hintereinander angewendet. Dabei werden zwei verschiedene Schlüssel mit jeweils 56 Bits Länge eingesetzt, wobei der Schlüssel des ersten Durchlaufs beim dritten Durchlauf wiederverwendet wird. Es ergibt sich eine nominale Schlüssellänge von 168 Bit bzw. eine effektive Schlüssellänge von 112 Bit.

  Triple-DES kombiniert die ausgeklügelte Technik des DES mit einem ausreichend langen Schlüssel und gilt daher als sehr sicher. Triple-DES arbeitet allerdings langsamer als andere Verfahren.

- Blowfish

  Die Entwicklung des prominenten Kryptografen Bruce Schneier verschlüsselt symmetrisch. Blowfish erreicht einen hervorragenden Datendurchsatz und gilt als sehr sicher.

- CAST (nach den Autoren **C**arlisle **A**dams und **S**tafford **T**avares)

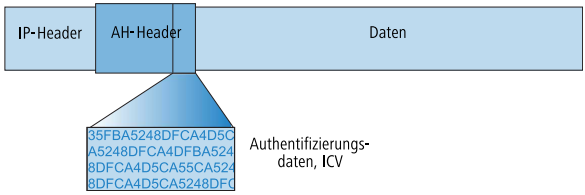
Ist ein symmetrisches Verfahren mit einer Schlüssellänge von 128 Bits. CAST ermöglicht eine variable Änderung von Teilen des Algorithmus' zur Laufzeit.

Hinweis: Die Verschlüsselung kann unter LANconfig in der Expertenkonfiguration angepasst werden. Eingriffe dieser Art sind in der Regel nur dann erforderlich, wenn VPN-Verbindungen zwischen Geräten unterschiedlicher Hersteller aufgebaut werden sollen.

10.16.4 Die Authentifizierung – das AH-Protokoll

Das AH-Protokoll (**A**uthentification **H**eader) gewährleistet die Integrität und Authentizität der Daten. Häufig wird die Integrität als Bestandteil der Authentizität betrachtet. Wir betrachten im Folgenden die Integrität als separates Problem, das von AH gelöst wird. Neben Integrität und Authentizität bietet AH auch einen wirksamen Schutz gegen Wiedereinspielen empfangener Pakete (Replay Protection).

IP-Paketen fügt AH einen eigenen Header direkt hinter dem ursprünglichen IP-Header hinzu. Wichtigster Bestandteil dieses AH-Headers ist ein Feld mit Authentifizierungsdaten (Authentication Data), häufig auch als **I**ntegrity **C**heck **V**alue (ICV) bezeichnet.

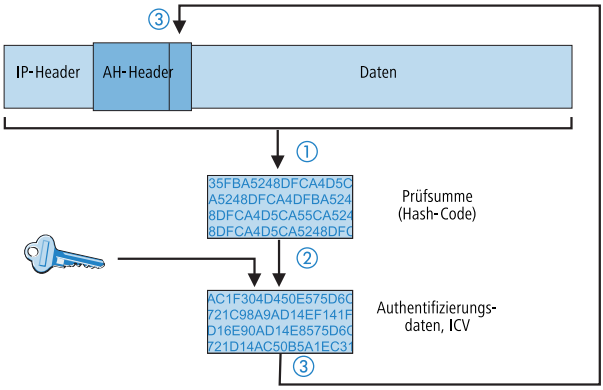


Der Ablauf von AH im Sender

Im Sender der Pakete läuft die Erstellung der Authentication Data in 3 Schritten ab.

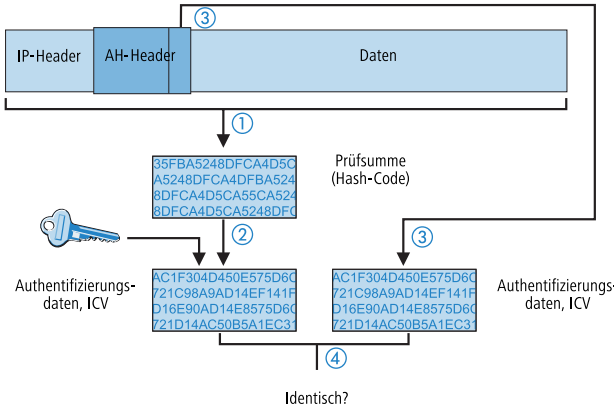
1. Aus dem Gesamtpaket wird eine Prüfsumme mittels Hash-Algorithmen errechnet.

2. Diese Prüfsumme wird zusammen mit einem dem Sender und Empfänger bekannten Schlüssel erneut durch einen Hash-Algorithmus geschickt.
3. Es ergeben sich die gesuchten Authentifizierungsdaten, die im AH-Header abgelegt werden.



Prüfung von Integrität und Authentizität im Empfänger

Beim Empfänger läuft das AH-Protokoll sehr ähnlich ab. Auch der Empfänger berechnet zunächst mit seinem Schlüssel die Authentifizierungsdaten für das empfangene Paket. Beim Vergleich mit dem übermittelten ICV des Paketes stellt sich heraus, ob Integrität und Authentizität des Paketes gegeben sind oder nicht.



Bildung der Prüfsumme für den Integritäts-Check

Um die Integrität, also die Korrektheit der transferierten Pakete zu gewährleisten, versieht AH beim Versand jedes Paket mit einer Prüfsumme. Beim Empfänger prüft AH, ob die Prüfsumme zum Inhalt des Paketes passt. Ist das nicht der Fall, dann wurde es entweder falsch übertragen oder bewusst verändert. Solche Pakete werden sofort verworfen und gelangen nicht mehr auf höhere Protokollebenen.

Zur Errechnung der Prüfsumme stehen verschiedene sogenannte Hash-Algorithmen zur Verfügung. Hash-Algorithmen zeichnen sich dadurch aus, dass das Ergebnis (der Hash-Code) charakteristisch für die Eingangsdaten ist („Fingerabdruck“), ohne dass umgekehrt vom Hash-Code auf die Eingangsdaten geschlossen werden könnte. Außerdem haben bei einem hochwertigen Hash-Algorithmus kleinste Änderungen des Eingangswertes einen völlig unterschiedlichen Hash-Code zur Folge. So werden systematische Analysen mehrerer Hash-Codes erschwert.

Die beiden gängigsten Hash-Algorithmen sind MD5 und SHA-1. Beide Methoden arbeiten ohne Schlüssel, d.h. alleine auf der Basis fester Algorithmen. Schlüssel kommen erst in einem späteren Schritt von AH ins Spiel: bei der endgültigen Berechnung der Authentification Data. Die Integritäts-Prüfsumme ist nur ein notwendiges Zwischenergebnis auf dem Weg dorthin. Das VPN-Modul im LCOS unterstützt MD5 und SHA-1.

Berechnung der Authentifizierungsdaten

Im zweiten Schritt bildet AH einen neuen Hash-Code aus der Prüfsumme und einem Schlüssel, die endgültigen Authentifizierungsdaten. Auch für diesen Prozess gibt es unter IPSec verschiedene Standards zur Auswahl. Einer lautet HMAC (**H**ash-based **M**essage **A**uthentication **C**ode). Als Hash-Algorithmen stehen die Hash-Funktionen MD5 und SHA-1 zur Verfügung. Die HMAC-Versionen heißen entsprechend HMAC-MD5-96 und HMAC-SHA-1-96.

Jetzt wird deutlich, dass AH das Paket selber unverschlüsselt lässt. Lediglich die Prüfsumme des Paketes und der eigene Schlüssel werden gemeinsam zum ICV, den Authentifizierungsdaten, chiffriert und dem Paket als Prüfkriterium beigelegt.

Das VPN-Modul im LCOS unterstützt HMAC.

Replay Protection – Schutz vor wiederholten Paketen

AH kennzeichnet zusätzlich zur Beschriftung mit dem ICV jedes Paket auch mit einer eindeutigen, fortlaufenden Nummer (Sequence Number). Dadurch kann der Empfänger solche Pakete erkennen, die von einem Dritten aufgenommen wurden und nun wiederholt gesendet werden. Diese Art von Angriffen wird als „Packet Replay“ bezeichnet.

Hinweis: Mit AH ist keine Maskierung von IPSec-Tunneln möglich, sofern nicht zusätzliche Maßnahmen wie NAT-Traversal oder ein äußeres Layer-2-Tunneling (z. B. PPPT/L2TP) nochmals einen „veränderbaren“ äußeren IP-Header bereitstellen.

10.16.5 Management der Schlüssel – IKE & IKEv2

Das **I**nternet **K**ey **E**xchange Protocol (IKE) ist ein Protokoll, das Unterprotokolle zum Aufbau der SAs (Security Associations) und für das Schlüsselmanagement beinhalten kann.

Innerhalb von IKE werden zwei Unterprotokolle verwendet: Oakley für die Authentifizierung der Partner und den Schlüsselaustausch sowie ISAKMP für die Verwaltung der SAs.

Aufbau der SA mit ISAKMP/Oakley

Jeder Aufbau einer SA erfolgt in mehreren Schritten (bei dynamischen Internet-Verbindungen erfolgen diese Schritte, nachdem die öffentliche IP-Adresse übertragen wurde):

1. Per ISAKMP sendet der Initiator an die Gegenstelle eine Meldung im Klartext mit der Aufforderung zum Aufbau einer SA und Vorschlägen (Proposals) für die Sicherheitsparameter dieser SA.
2. Die Gegenstelle antwortet mit der Annahme eines Vorschlags.
3. Beide Geräte erzeugen nun Zahlenpaare (bestehend aus öffentlichem und privatem Zahlenwert) für das Diffie-Hellman-Verfahren.
4. In zwei weiteren Mitteilungen tauschen beide Geräte ihre öffentlichen Zahlenwerte für Diffie-Hellman aus.
5. Beide Seiten erzeugen aus übertragenem Zahlenmaterial (nach dem Diffie-Hellman-Verfahren) und Shared Secret einen gemeinsamen geheimen Schlüssel, mit dem die weitere Kommunikation verschlüsselt wird. Außerdem authentifizieren sich beide Seiten gegenseitig anhand von Hash-Codes ihres gemeinsamen Shared Secrets. Die sogenannte Phase 1 des SA-Aufbaus ist damit beendet.
6. Phase 2 basiert auf der verschlüsselten und authentifizierten Verbindung, die in Phase 1 aufgebaut wurde. In Phase 2 werden die Sitzungsschlüssel für die Authentifizierung und die symmetrische Verschlüsselung des eigentlichen Datentransfers erzeugt und übertragen.

Hinweis: Für die Verschlüsselung des eigentlichen Datentransfers werden symmetrische Verfahren eingesetzt. Asymmetrische Verfahren (auch bekannt als Public-Key-Verschlüsselung) sind zwar sicherer, da keine geheimen Schlüssel übertragen werden müssen. Zugleich erfordern sie aber aufwändige Berechnungen und sind daher deutlich langsamer als symmetrische Verfahren. In der Praxis wird Public-Key-Verschlüsselung meist nur für den Austausch von Schlüsselmaterial eingesetzt. Die eigentliche Datenverschlüsselung erfolgt anschließend mit schnellen symmetrischen Verfahren.

Der regelmäßige Austausch neuer Schlüssel

ISAKMP sorgt während des Bestehens der SA dafür, dass regelmäßig neues Schlüsselmaterial zwischen den beiden Geräten ausgetauscht wird. Dieser Vorgang geschieht automatisch und kann über die Einstellung der 'Lifetime' in der erweiterten Konfiguration von LANconfig kontrolliert werden.

10.16.6 IKEv2

Der VPN-Aufbau ist mit OpenBAT-Geräten sowohl über IKEv1 als auch über IKEv2 möglich.

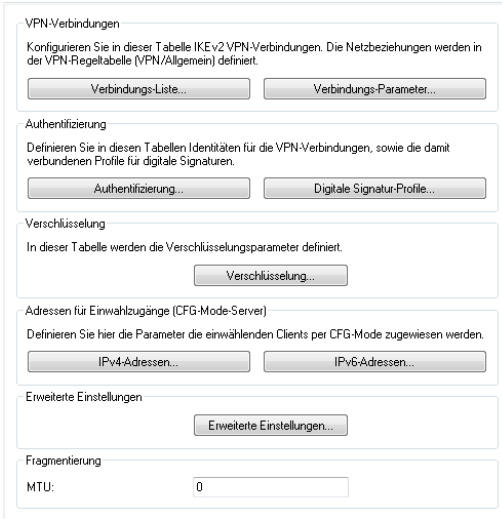
IKEv2 ermöglicht einen schnelleren und sichereren Verbindungsaufbau von VPN-Tunneln. Erstmals ist zudem die VPN-verschlüsselte Vernetzung von IPv6-basierten Standorten auch im Mischbetrieb mit IPv4 möglich.

Die Einrichtung einer VPN-Verbindung über IKEv1 ist bei manueller Konfiguration komplex und fehleranfällig, so dass viele Implementationen von IPSec inkompatibel zueinander konfiguriert sein können und damit eine VPN-Verbindung zwischen den Geräten durch fehlerhafte Konfigurationsvorgänge scheitern kann. Die IKEv2-Konfiguration im HiLCOS ermöglicht es dem Administrator, zuverlässig eine Übereinstimmung der Konfiguration mit der Gegenstelle einzurichten. Der Administrator hat z. B. die Möglichkeit, mehrere Diffie-Hellman-Gruppen anzuwählen. Damit erhält das Gerät über die überarbeitete Benutzeroberfläche an vielen Konfigurationsparametern empfohlene Default-Werte. Dieser vereinfachte Konfigurationsablauf mit IKEv2 beseitigt folglich Fehlerquellen, was wiederum zu einem geringeren Administrationsaufwand führt. Zusätzlich ist der VPN-Verbindungsaufbau bei IKEv2 performanter, denn IKEv2 nutzt für den Informationsaustausch bei der Aushandlung eines VPN-Tunnels nur 4 Pakete (je VPN-Partner ein REQUEST und ein REPLY), anstatt wie bei IKEv1 zwischen 6 (im “aggressive/quick mode”) und 12 (im “main mode”) Paketen. Der Sicherheitsstandard ist bei IKEv2 genauso hoch wie bei IKEv1.

Bei der Verwendung von IKEv2 werden *RFC 7296*, *RFC 7427* und im IKEv2-Client-Betrieb *RFC 5685* unterstützt.

IKEv2 mit LANconfig konfigurieren

IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec**.



VPN-Verbindungen

In diesem Abschnitt konfigurieren Sie die IKEv2-VPN-Verbindungen und Verbindungsparameter.

Authentifizierung

Definieren Sie in dieser Tabelle die Identitäten für die VPN-Verbindungen.

Digitale Signatur-Profile

Definieren Sie in dieser Tabelle die Authentifizierungs-Methode für die VPN-Verbindungen.

Verschlüsselung

Definieren Sie in dieser Tabelle die Verschlüsselungsparameter.

Adressen für Einwahlzugänge (CFG-Mode-Server)

Definieren Sie in dieser Tabelle die Parameter, die das Gerät den einwählenden Clients per CFG-Mode zuweist.

Erweiterte Einstellungen

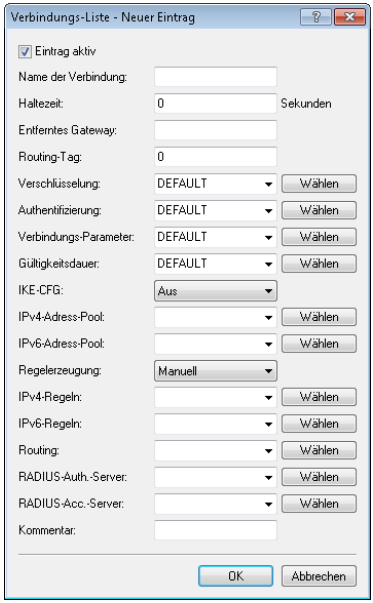
Konfigurieren Sie in diesem Abschnitt die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter und die Präfixe für das IKEv2-Routing.

Um eine IKEv2-Verbindung zu konfigurieren, ist zunächst ein Eintrag in der **Verbindungs-Liste** erforderlich. Um den Konfigurationsaufwand gering zu halten, enthält HiLCOS Default-Einträge, die die meisten Parameter mit den gängigen Einstellungen für starke Verschlüsselungsalgorithmen, Dead-Peer-Detection oder Gültigkeitszeiträume vorbelegen. Lediglich die Angabe der VPN-Gegenstellen-Adresse, der Authentifizierungs-Parameter (unter **Authentifizierung**) sowie der VPN-Regeln (unter **VPN** > **Allgemein** > **Netzwerk-Regeln**) ist erforderlich.

Hinweis: Der Konsolenbefehl `show vpn` zeigt, ob die so eingerichtete VPN-Verbindung erfolgreich ist.

Verbindungs-Liste

In dieser Tabelle konfigurieren Sie die IKEv2-Verbindungen zu VPN-Partnern.



Eintrag aktiv

Aktiviert oder deaktiviert die Verbindung zu dieser VPN-Gegenstelle.

Name der Verbindung

Enthält den Namen der Verbindung zur Gegenstelle.

Haltezeit

Gibt die Haltezeit in Sekunden an, die das Gerät eine Verbindung ohne Datenfluss aufrecht erhält.

Entferntes Gateway

Enthält die Adresse (IPv4- oder IPv6-Adresse, FQDN) des VPN-Partners.

Routing-Tag

Enthält das Routing-Tag für diese VPN-Verbindung.

Verschlüsselung

Bestimmt die Verschlüsselung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verschlüsselung**.

Authentifizierung

Bestimmt die Authentifizierung der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Authentifizierung**.

Verbindungs-Parameter

Bestimmt die allgemeinen Parameter der VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Verbindungs-Parameter**.

Gültigkeitsdauer

Bestimmt die Lebensdauer der Schlüssel einer VPN-Verbindung. Der entsprechende Eintrag steht in der Tabelle **Erweiterte Einstellungen** > **Gültigkeitsdauer**.

IKE-CFG

Bestimmt den IKEv2-Config-Modus dieser Verbindung für RAS-Einwahlen.

Mögliche Werte sind:

- Aus: IKEv2-Config-Modus deaktiviert
- Server: Der Router verteilt Konfigurationsparameter (z. B. Adressen oder DNS-Server) an VPN-Clients Die zu vergebenden Parameter werden im IPv4- bzw. IPv6-Adresspool konfiguriert.
- Client: Der Router fragt beim Server Konfigurationsparameter (z. B. Adressen oder DNS-Server an).

IPv4-Adress-Pool

IPv4-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

IPv6-Adress-Pool

IPv6-Adressen und DNS-Server für Einwahlzugänge im IKE-CFG-Modus Server.

Regelerzeugung

Bestimmt, wie VPN-Regeln erstellt werden.

Mögliche Werte:

Automatisch

Als Quellnetz wird das lokale Intranet eingesetzt (privater IP-Adressbereich, zu dem das lokale VPN-Gateway selbst gehört). Als Zielnetze dienen für die automatisch erstellten VPN-Regeln die Netzbereiche aus der IP-Routing-Tabelle, für die als Router ein entferntes VPN-Gateway eingetragen ist.

Werden zwei einfache lokale Netzwerke gekoppelt, ist es der VPN-Automatik möglich, aus dem IP-Adressbereich des eigenen LANs und dem Eintrag des entfernten LAN in der IP-Routing-Tabelle die erforderliche Netzbeziehung ableiten.

Manuell

Die Regelerstellung für die Netzbeziehungen erfolgt wie die manuelle Regel-Definition für IPv4 oder IPv6.

IPv4-Regeln

Gibt an, welche IPv4-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv4-Regeln stehen in der Tabelle **VPN** > **Netzwerk-Regeln**.

IPv6-Regeln

Gibt an, welche IPv6-Regeln für diese VPN-Verbindung gelten sollen.

Die IPv6-Regeln stehen in der Tabelle **VPN** > **Netzwerk-Regeln**.

Routing

Gibt die Routen an, die der Gegenseite dynamisch per IKE-CFG Mode übermittelt werden sollen. Diese Funktion ist nur im IKEv2-CFG Mode für Client und Server möglich.

Die Routen für IPv4- und IPv6-Verbindungen stehen in den Tabellen **Erweiterte Einstellungen** > **IPv4-Routing/IPv6-Routing**.

RADIUS-Auth.-Server

Bestimmt den RADIUS-Server für die Autorisierung des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

RADIUS-Auth.-Server

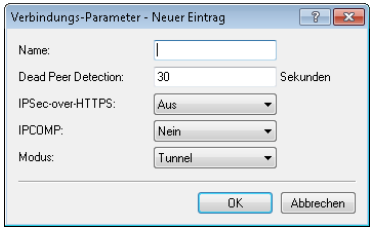
Bestimmt den RADIUS-Server für das Accounting des VPN-Peers. Den RADIUS-Server für IKEv2 konfigurieren Sie unter **VPN** > **IKEv2/IPSec** unter **Erweiterte Einstellungen**.

Kommentar

Vergeben Sie diesem Eintrag einen aussagekräftigen Kommentar.

Verbindungs-Parameter

In dieser Tabelle definieren Sie die Parameter von IKEv2-VPN-Verbindungen, die nicht Bestandteil der SA-Verhandlung sind. Es existiert ein Standardeintrag “DEFAULT” mit gängigen Einstellungen.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld “Verbindungs-Parameter” zu.

Dead Peer Detection

Enthält die Zeit in Sekunden, nach der das Gerät die Verbindung beendet, wenn es in der Zwischenzeit den entfernten Peer nicht mehr erreicht.

IPSec-over-HTTPS

Gibt an, ob die Verbindung IKEv2 über HTTPS verwendet.

IPCOMP

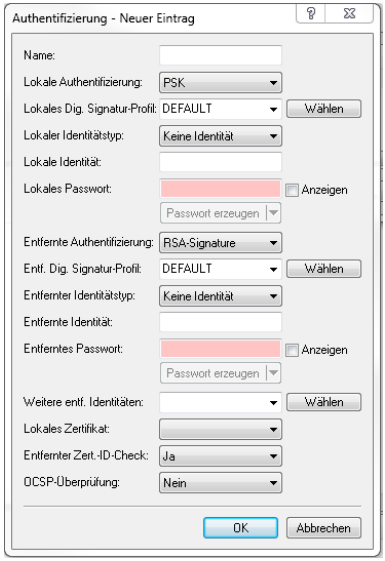
Gibt an, ob die Geräte die IKEv2-Datenpakete komprimiert übertragen.

Modus

Bestimmt den Übertragungsmodus.

Authentifizierung

In dieser Tabelle konfigurieren Sie die Parameter für die IKEv2-Authentifizierung der lokalen und mindestens einer entfernten Identität.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld “Authentifizierung” zu.

Lokale Authentifizierung

Legt die Authentifizierungsmethode für die lokale Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema
- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Lokales Digitales Signatur-Profil

Profilname des verwendeten lokalen Digital-Signatur-Profils.

Lokaler Identitätstyp

Zeigt den ID-Typ der lokalen Identität an. Entsprechend interpretiert das Gerät die Eingabe unter “Lokale Identität”. Mögliche Angaben sind:

- Keine Identität: Es wird keine Identität übertragen.
- IPv4-Adresse: Das Gerät verwendet eine IPv4-Adresse als lokale ID.
- IPv6-Adresse: Das Gerät verwendet eine IPv6-Adresse als lokale ID.
- Domänen-Name (FQDN): Das Gerät verwendet einen Domänen-Namen als lokale ID.
- E-Mail-Adresse (FQUN): Das Gerät verwendet eine E-Mail-Adresse als lokale ID.
- ASN.1-Distinguished-Name: Das Gerät verwendet einen Distinguished Name als lokale ID (z. B. “CN=client01.example.com,O=test,C=DE”
- Key-ID (Gruppenname): Das Gerät verwendet den Gruppennamen als lokale ID. Den Gruppennamen können sie beliebig definieren.

Lokale Identität

Enthält die lokale Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter “Lokaler Identitätstyp”.

Lokales Passwort

Enthält das Passwort der lokalen Identität. Mit diesem Passwort authentifiziert sich das Gerät bei der Gegenseite. Das lokale und entfernte Passwort kann identisch oder unterschiedlich sein.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest. Mögliche Werte sind:

- PSK: Pre-Shared Key
- RSA-Signature: Verwendung von digitalen Zertifikaten mit privatem RSA-Schlüssel und RSA-Signaturschema
- Digitale-Signatur: Verwendung von konfigurierbaren Authentifizierungsmethoden mit digitalen Zertifikaten nach *RFC 7427*. Dieses Verfahren ist ein erweiterbares und flexibles Authentifizierungsverfahren, bei dem z. B. Padding- und Hash-Verfahren frei konfiguriert werden können.

Das Gerät verwendet die konfigurierte Authentifizierungsmethode beim Verbindungsaufbau mit der Gegenstelle. Die Methode muss mit der entsprechenden Konfiguration auf der Gegenseite übereinstimmen.

Dabei es möglich, unterschiedliche Authentifizierungsverfahren für die lokale und entfernte Authentifizierung zu verwenden. Beispielsweise kann sich die Zentrale per RSA-Signature ausweisen, während Filialen oder Clients PSK zur Authentifizierung verwenden.

Entferntes Digitales Signatur-Profil

Profilname des entfernten Digital-Signatur-Profils.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter “Entfernte Identität”. Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld “Entfernte Identität” ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.

- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID (z. B. “CN=client01.example.com,O=test,C=DE”).
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter “Entfernter Identitätstyp”.

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

Weitere entf. Identitäten

Für redundante VPN-Szenarien ist die Angabe von alternativen entfernten Identitäten möglich.

Konfigurieren Sie hier weitere entfernte Identitäten aus der Tabelle **Erweiterte Einstellungen** > **Identitäten-Liste**.

Lokales Zertifikat

Zeigt das lokale Zertifikat an.

Entfernte Zertifikatsprüfung

Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

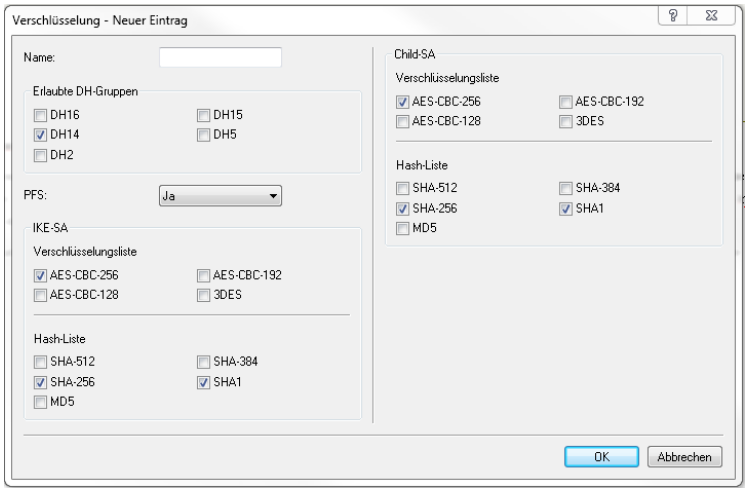
Verschlüsselung

In dieser Tabelle konfigurieren Sie die Verschlüsselungsparameter. Es existiert ein Standardeintrag “DEFAULT” mit gängigen Einstellungen.

Eine Mehrfachauswahl der Parameter ist möglich. Diese Parameterlisten propagiert das Gerät im IKE-Protokoll und in CHILD-SAs. Beide VPN-Partner verständigen sich anschließend auf einen Algorithmus der propagierten Listen. Beim Aufbau der ersten IKE-SA einigen sich die VPN-Partner auf die höchste der gegenseitig propagierten DH-Gruppen. Diese DH-Gruppe nutzen die VPN-

Partner, wenn sie die IKE-SAs erneuern oder wenn sie CHILD-SAs erzeugen oder erneuern (bei aktiviertem PFS).

Die Verbindung zwischen den VPN-Partnern kommt zustande, wenn es in der Menge der konfigurierten Verschlüsselungsparameter Gemeinsamkeiten gibt. Stimmen die Parameter in keinem Fall überein, findet keine Verbindung statt.



Name

Enthält den eindeutigen Namen dieses Eintrages. Diesen Namen ordnen Sie den Verbindungen in der **Verbindungs-Liste** im Feld “Verschlüsselung” zu.

Erlaubte DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen, auf deren Basis die VPN-Partner einen Schlüssel für den Datenaustausch erstellen. Je höher die gewählte DH-Gruppe, desto komplexer ist der erzeugte Schlüssel. Aktuell werden folgende Gruppen unterstützt:

- DH-2 (1024-Bit Modulus)
- DH-5 (1536-Bit Modulus)
- DH-14 (2048-Bit Modulus)
- DH-15 (3072-Bit Modulus)
- DH-16 (4096-Bit Modulus)

PFS

Gibt an, ob Perfect Forward Secrecy (PFS) aktiviert ist.

Verschlüsselungsliste

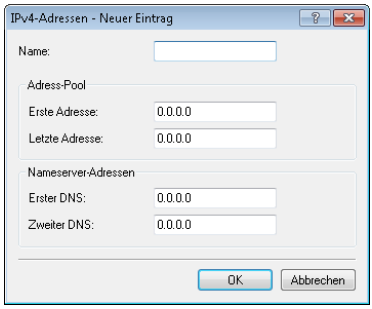
Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind.

Hash-Liste

Gibt an, welche Hash-Algorithmen aktiviert sind.

IPv4-Adressen

In dieser Tabelle konfigurieren Sie die IPv4-Parameter, die das Gerät den einwählenden VPN-Clients per CFG-Mode zuweist.



Name

Enthält den Namen der Schnittstelle für den Einwahlzugang.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv4-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Nameserver-Adressen

Erster DNS

Enthält die erste DNS-Adresse.

Zweiter DNS

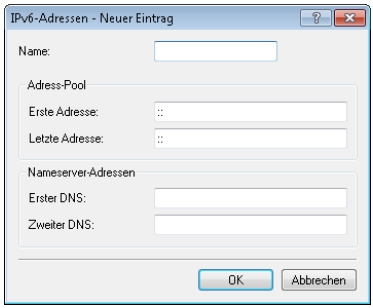
Enthält die zweite DNS-Adresse.

IPv6-Adressen

Wenn das Gerät als “CFG-Mode-Server” arbeitet, vergibt der Server per IKEv2-Configuration-Payload eine Adresse aus einem lokalen Adress-Pool an Clients. Außerdem kann er dem Client bis zu zwei DNS-Server zuweisen.

Serverseitig aktivieren Sie dazu in der VPN-Verbindungsliste den CFG-Mode “Server” und auf der Client-Seite den CFG-Mode “Client”.

In dieser Tabelle konfigurieren Sie die IPv6-Parameter, die das Gerät den einwählenden VPN-Clients im CFG-Mode “Server” zuweist.



Name

Enthält den Namen der Schnittstelle für den Einwahlzugang.

Adress-Pool

Erste Adresse

Geben Sie hier die erste IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Letzte Adresse

Geben Sie hier die letzte IPv6-Adresse des Adressbereiches ein, den Sie den VPN-Clients zur Verfügung stellen wollen.

Nameserver-Adressen

Erster DNS

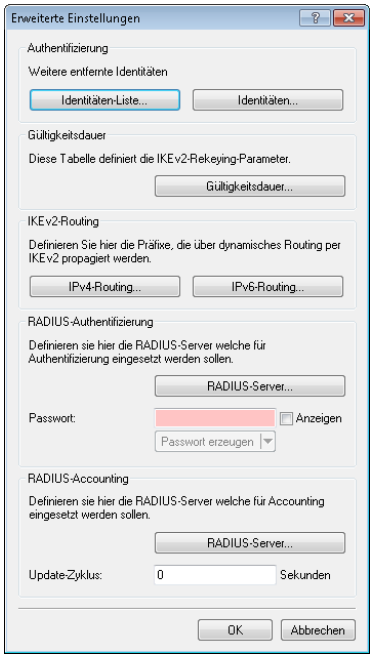
Enthält die erste DNS-Adresse.

Zweiter DNS

Enthält die zweite DNS-Adresse.

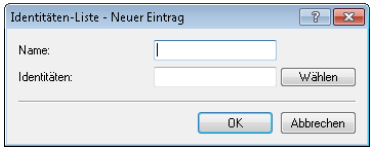
Erweiterte Einstellungen

In diesem Dialog konfigurieren Sie die Einstellungen zur Authentifizierung weiterer entfernter Identitäten, die IKEv2-Rekeying-Parameter, die Präfixe für da IKEv2-Routing sowie die RADIUS-Server für IKEv2.



Identitäten-Liste

In dieser Tabelle fassen Sie weitere entfernte Identitäten in einer Gruppe zusammen.



Name

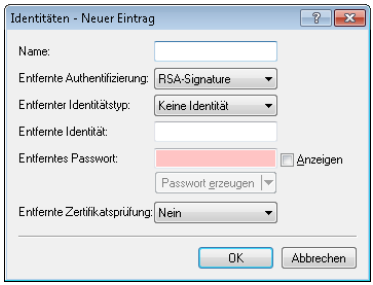
Enthält den eindeutigen Namen dieses Eintrages.

Identität

Listet die weiteren entfernten Identitäten auf, die in dieser Gruppe zusammengefasst sind. Diese Identitäten konfigurieren Sie unter **Identitäten**.

Identitäten

In dieser Tabelle konfigurieren Sie weitere entfernte Identitäten. Diesen Namen wählen Sie bei der Gruppierung von entfernten Identitäten unter **Identitäten-Liste** aus.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Entfernte Authentifizierung

Legt die Authentifizierungsmethode für die entfernte Identität fest.

Entfernter Identitätstyp

Zeigt den ID-Typ an, den das Gerät von der entfernten Identität erwartet. Entsprechend interpretiert das Gerät die Eingabe unter “Entfernte Identität”. Mögliche Angaben sind:

- Keine Identität: Das Gerät akzeptiert jede ID des entfernten Gerätes. Eine Angabe im Feld “Entfernte Identität” ignoriert das Gerät.
- IPv4-Adresse: Das Gerät erwartet eine IPv4-Adresse als entfernte ID.
- IPv6-Adresse: Das Gerät erwartet eine IPv6-Adresse als entfernte ID.

- Domänen-Name (FQDN): Das Gerät erwartet einen Domänen-Namen als entfernte ID.
- E-Mail-Adresse (FQUN): Das Gerät erwartet eine E-Mail-Adresse als entfernte ID.
- ASN.1-Distinguished-Name: Das Gerät erwartet einen Distinguished Name als entfernte ID.
- Key-ID (Gruppenname): Das Gerät erwartet den Gruppennamen als entfernte ID.

Entfernte Identität

Enthält die entfernte Identität. Die Bedeutung dieser Eingabe ist abhängig von der Einstellung unter “Entfernter Identitätstyp”.

Entferntes Passwort

Enthält das Passwort der entfernten Identität.

Entfernte Zertifikatsprüfung

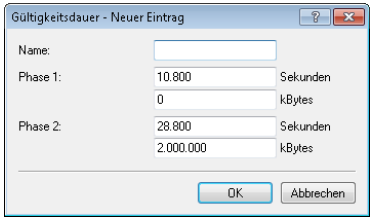
Diese Option bestimmt, ob das Gerät prüft, ob die angegebene entfernte Identität im empfangenen Zertifikat enthalten ist.

Gültigkeitsdauer

In dieser Tabelle definieren Sie die IKEv2-Rekeying-Parameter. Es existiert ein Standardeintrag “DEFAULT” mit gängigen Einstellungen.

Je Phase unterscheidet das Gerät nach Zeit oder zu übertragender Datenmenge. Der Parameter, der als erstes seinen festgelegten Grenzwert erreicht, startet die Erneuerung des entsprechenden IKEv2-Schlüssels.

Hinweis: Der Wert “0” bedeutet, dass das Gerät keinen Grenzwert für den entsprechenden Schlüssel festlegt.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Phase 1

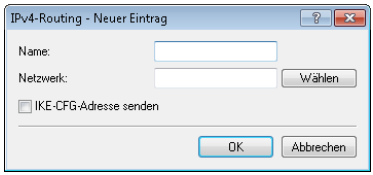
Enthält die Zeit in Sekunden oder die Datenmenge in Kilobyte bis zur Erneuerung des IKE-SA-Schlüssels.

Phase 2

Enthält die Zeit in Sekunden oder die Datenmenge in Kilobyte bis zur Erneuerung des CHILD-SA-Schlüssels.

IPv4-Routing

In dieser Tabelle konfigurieren Sie die IPv4-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IP-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IP-Adresse
- IP-Adresse/IP-Maske
- IP-Adresse/Präfixlänge
- IP-Schnittstellen-Name

Die Konfiguration der IP-Subnetze erfolgt unter **IPv4** > **Allgemein** im Abschnitt **Eigene Adressen**.

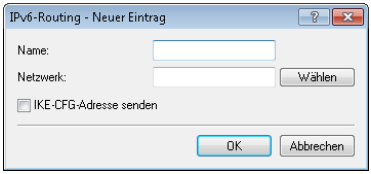
IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Hinweis: Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

IPv6-Routing

In dieser Tabelle konfigurieren Sie die IPv6-Netze, die das Gerät über dynamisches Routing per IKEv2 propagiert.



Name

Enthält den eindeutigen Namen dieses Eintrages.

Netzwerk

Enthält die kommaseparierte Liste von IPv6-Subnetzen.

Die Angabe der Netze ist in den folgenden Formaten möglich:

- IPv6-Adresse
- IPv6-Adresse/Präfixlänge
- IPv6-Schnittstellen-Name

Die Konfiguration der IP-Subnetze erfolgt unter **IPv6** > **Allgemein** im Abschnitt **IPv6-Netzwerke**.

IKE-CFG-Adresse senden

Als Client sendet das Gerät die erhaltene CFG-Mode-Adresse an den VPN-Peer (Server).

Hinweis: Diese Option ist nur dann erforderlich, falls die Gegenseite keinen automatischen Routing-Eintrag für zugewiesene IP-Adressen erzeugt. LANCOM Router erzeugen die notwendigen Routen automatisch.

RADIUS-Authentifizierung

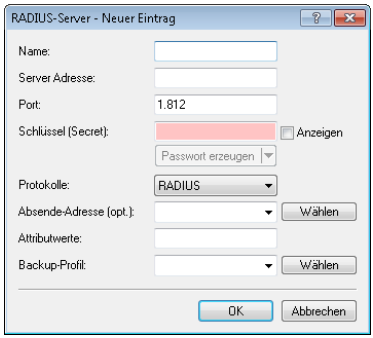
Im Abschnitt **RADIUS-Authentifizierung** konfigurieren Sie die Einstellungen der RADIUS-Server zur Autorisierung von VPN-Clients.

Bestimmen Sie im Feld **Passwort** das Passwort, das der RADIUS-Server im Access-Request-Attribut als Benutzer-Passwort erhält.

Der RADIUS-Server ordnet dieses Passwort normalerweise direkt einem VPN-Peer zu, um diesen für den Netzwerkzugang zu autorisieren. Bei IKEv2 autorisiert jedoch nicht der RADIUS-Server den anfragenden VPN-Peer, sondern das OpenBAT-Gateway, nachdem es die entsprechende Autorisierung in der `Access-Accept`-Nachricht des RADIUS-Servers erhalten hat.

Entsprechend geben Sie an dieser Stelle ein Dummy-Passwort ein.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert “1812” ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des OpenBAT-Gateways am RADIUS-Server.

Hinweis: Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Auth.-Server**.

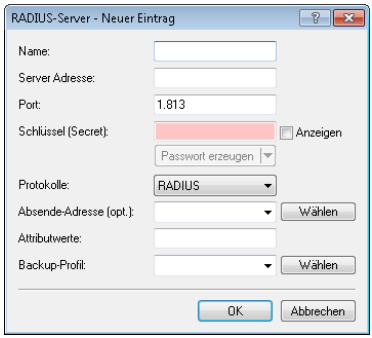
RADIUS-Accounting

Im Abschnitt **RADIUS-Accounting** konfigurieren Sie die Einstellungen der RADIUS-Server zum Accounting von VPN-Clients.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.

Bestimmen Sie im Feld **Update-Zyklus** die Zeit in Sekunden zwischen zwei aufeinanderfolgenden Interim-Update-Nachrichten. Das Gerät fügt zufällig eine Toleranz von ±10% ein, um die Update-Nachrichten paralleler Accounting Sessions zeitlich voneinander abzutrennen.

Mit einem Klick auf **RADIUS-Server** öffnet sich der Dialog zur Konfiguration des RADIUS-Servers.



Name

Geben Sie eine Bezeichnung für diesen Eintrag ein.

Server-Adresse

Geben Sie den Hostnamen für den RADIUS-Server an (IPv4-, IPv6- oder DNS-Adresse).

Port

Geben Sie den UDP-Port des RADIUS-Servers an. Der Wert “1813” ist als Standardwert voreingestellt.

Schlüssel (Secret)

Dieser Eintrag enthält den Schlüssel (Shared Secret) zur Autorisierung des OpenBAT-Gateways am RADIUS-Server.

Hinweis: Bestätigen Sie den angegebenen Schlüssel durch eine erneute Eingabe im darauf folgenden Feld.

Protokolle

Wählen Sie aus dem Drop-Down-Menü zwischen dem normalen RADIUS-Protokoll und dem sicheren RADSEC-Protokoll für die RADIUS-Anfrage.

Absende-Adresse (opt.)

Geben Sie hier ggf. die Loopback-Adresse des Gerätes an.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}`

setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Profil

Wählen Sie aus der Liste der RADIUS-Server-Profile ein Profil als Backup-Server.

Die Auswahl der hier konfigurierten RADIUS-Server erfolgt in der Verbindungsliste unter **VPN** > **IKEv2/IPSec** > **Verbindungs-Liste** im Feld **RADIUS-Acc.-Server**.

IKEv2-Fragmentierung

Die Fragmentierung von Datenpaketen richtet sich nach der Maximum Transmission Unit (MTU). Die MTU bezeichnet die maximale Größe, die ein Paket haben darf, um als Payload über einen Kanal versendet werden zu können. Diese wird zu Beginn einer Übertragung von beiden Kommunikationspartnern ausgehandelt, um die optimale Datenübertragung ohne eine zusätzliche Fragmentierung von Datenpaketen gewährleisten zu können.

In HiLCOS ist die IKEv2-Fragmentierung automatisch aktiviert. Sie können davon abweichend manuell eine maximale MTU definieren.

Wechseln Sie dazu in LANconfig in die Ansicht **VPN** > **IKEv2/IPSec**.

Geben Sie im Abschnitt **Fragmentierung** im Feld **MTU** die maximale IP-Paketlänge/-größe in Byte an. Je kleiner Sie den Wert wählen, je stärker ist die Fragmentierung der Nutzdaten.

RADIUS-Unterstützung für IKEv2

HiLCOS ermöglicht es, die IKEv2-Konfiguration für Autorisierung und Accounting von VPN-Peers durch einen externen RADIUS-Server durchführen zu lassen.

In mittleren bis großen VPN-Szenarien sind die Tabellen für VPN-Konfigurationen in der Regel sehr umfangreich und komplex. Wenn mehrere VPN-

Gateways aus Redundanzgründen zum Einsatz kommen, muss sichergestellt werden, dass die Konfiguration auf allen VPN-Gateways identisch ist.

Der Einsatz eines zentralen RADIUS-Servers ermöglicht die fast vollständige Auslagerung der Konfiguration der VPN-Parameter vom VPN-Gateway auf einen oder mehrere RADIUS-Server. Sobald eine VPN-Gegenstelle eine VPN-Verbindung zum Gerät aufbauen will, versucht das Gerät, die ankommende Verbindung per RADIUS zu authentifizieren und weitere notwendige Verbindungsparameter wie z. B. VPN-Netzbeziehungen, CFG-Mode-Adresse oder DNS-Server vom RADIUS-Server abzurufen.

Dabei kann die VPN-Konfiguration entweder vollständig oder nur teilweise vom RADIUS-Server abgerufen mit lokal vorhandenen Parametern kombiniert werden. Dieser Mechanismus funktioniert nur für ankommende Verbindungen.

Durch das optionale RADIUS-Accounting können Informationen über VPN-Verbindungen zentral auf einem RADIUS-Server gesammelt werden. Diese Informationen können z. B. aus Verbindungsdauer des Clients, Aufbauzeitpunkt oder das übertragene Datenvolumen bestehen.

Die Konfiguration der RADIUS-Server erfolgt in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen**.

RADIUS-Autorisierung

Das OpenBAT-Gateway überträgt bei der Anmeldung eines VPN-Peers die folgenden RADIUS-Attribute im `Access-Request` an den RADIUS-Server:

ID	*Bezeichnung*	*Bedeutung*
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der AUTH-Verhandlung mit dem OpenBAT-Gateway überträgt.
2	User-Passwort	Das Dummy-Passwort, wie es in LANconfig unter **VPN** > **IKEv2/IPSec** > **Erweiterte Einstellungen** > **Passwort** konfiguriert ist.
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut “95” (siehe unten).
6	Servcie-Type	Der Service-Type ist immer “Outbound (5)” bzw. “Dialout-Framed-User”.

ID	*Bezeichnung*	*Bedeutung*
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv4-Verbindung, überträgt das Gateway stattdessen das Attribut “4” (siehe oben).

Von den in der `Access-Accept`-Antwort des RADIUS-Servers enthaltenen Attributen wertet das OpenBAT-Gateway daraufhin die folgenden, teils vendorspezifischen Attribute aus:

ID	*Bezeichnung*	*Bedeutung*
8	Framed-IP-Address	IPv4-Adresse für den Client (im IKE-CFG-Mode “Server”).
22	Framed-Route	IPv4-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen.
39	Tunnel-Password	Setzt bei Verwendung von synchronen PSKs die Passwörter der lokalen und der entfernten Identität auf den selben Wert.
88	Framed-Pool	Name des IPv4-Adressen-Pools, aus dem der Client die IP-Adresse und den DNS-Server bezieht. **Hinweis:** Die Werte in “Framed-IP-Address” und “LCS-DNS-Server-IPv4-Address” haben gegenüber diesem Attribut Vorrang.
99	Framed-IPv6-Route	IPv6-Routen, die in Richtung des Clients (Next-Hop-Client) auf dem VPN-Gateway in der Routing-Tabelle eingetragen werden sollen.
168	Framed-IPv6-Address	IPv6-Adresse für den Client (im IKE-CFG-Mode “Server”).
169	DNS-Server-IPv6-Address	IPv6-DNS-Server für den Client (im IKE-CFG-Mode “Server”).
172	Stateful-IPv6-Address-Pool	Name des IPv6-Adressen-Pools (im IKE-CFG-Mode “Server”).

ID	*Bezeichnung*	*Bedeutung*
Lancom 19	LCS-IKEv2-Local-Password	Lokaler IKEv2-PSK
Lancom 20	LCS-IKEv2-Remote-Password	Entfernter IKEv2-PSK
Lancom 21	LCS-DNS-Server-IPv4-Address	IPv4-DNS-Server für den Client (im IKE-CFG-Mode “Server”)
Lancom 22	LCS-VPN-IPv4-Rule	Beinhaltet die IPv4-Netzwerkregeln (Beispiele: siehe unten)
Lancom 23	LCS-VPN-IPv6-Rule	Beinhaltet die IPv6-Netzwerkregeln (Beispiele: siehe unten)
Lancom 24	LCS-Routing-Tag	Routing-Tag, das für den Client konfiguriert werden soll (IPv4/IPv6).
Lancom 25	LCS-IKEv2-IPv4-Route	Routen in Präfix-Schreibweise (z. B. “192.168.1.0/24”), die das OpenBAT-Gateway per `INTERNAL_IP4_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.
Lancom 26	LCS-IKEv2-IPv6-Route	Routen in Präfix-Schreibweise (z. B. “2001:db8::/64”), die das OpenBAT-Gateway per `INTERNAL_IP6_SUBNET` an den Client übertragen soll. Die Auswertung von mehreren Attributen ist möglich.

Beipiele für Netzwerkregeln

Das Format für eine Netzwerkregel im Radius-Server gestaltet sich in der Form `<lokale Netze> * <entfernte Netze>`.

Die Einträge für `<Lokale Netze>` und `<entfernte Netze>` setzen sich dabei aus komma-separierten Listen zusammen.

Beispiel 1: `10.1.1.0/24,10.2.0.0/16 * 172.32.0.0/12`

Daraus ergeben sich die folgenden Netzwerkregeln:

- `10.2.0.0/255.255.0.0 <-> 172.16.200.0/255.255.255.255`
- `10.1.1.0/255.255.255.0 <-> 172.16.200.0/255.255.255.255`

Beispiel 2: `10.1.1.0/24 * 0.0.0.0/0`

Daraus ergibt sich die folgende Netzwerkregel:

- `10.1.1.0/255.255.255.0 <-> 0.0.0.0/0.0.0.0`

Dabei bedeutet `0.0.0.0/0` “ANY”, d. h. ein beliebiges Netz. `0.0.0.0/32` kann dazu verwendet werden, einen CFG-Mode-Client genau auf seine (noch unbekannte) Config-Mode-Adresse einzuschränken. Diese Adresse kommt z. B. aus einem Adress-Pool auf dem Gerät oder ebenfalls aus dem RADIUS-Server.

Beispiel 3: `2001:db8:1::/48 * 2001:db8:6::/48`

RADIUS-Accounting

Das OpenBAT-Gateway zählt die übertragenen Datenpakete und -Oktette und sendet diese Daten regelmäßig als `Accounting-Request`-Nachrichtenan an den Accounting-RADIUS-Server. Der RADIUS-Server beantwortet diese Meldung daraufhin jeweils mit einer `Accounting-Response`-Nachricht.

Die `Accounting-Request`-Nachrichten besitzen die folgenden Status-Typen:

Start

Sobald sich ein VPN-Peer am OpenBAT-Gateway anmeldet, startet das Gateway über IKEv2 eine Accounting-Session und sendet eine `Start`-Statusmeldung mit entsprechenden RADIUS-Attributen an den Accounting-RADIUS-Server.

Interim-Update

Während einer laufenden Accounting-Session sendet das Gateway in definierten Zeitabständen `Interim-Update`-Statusmeldungen an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

Stop

Nach dem Ende einer Sitzung sendet das OpenBAT-Gateway eine `Stop`-Statusmeldung an den Accounting-RADIUS-Server. Auch diese Meldung sendet es nur an den Accounting-RADIUS-Server, der auch die `Start`-Statusmeldung als gültig beantwortet hat. Eventuell konfigurierte Backup-Server ignoriert das Gateway.

In der `Access-Request`-Meldung überträgt das Gateway die folgenden RADIUS-Attribute an den RADIUS-Server:

ID	*Bezeichnung*	*Bedeutung*	*Status-Typ*
1	User-Name	Die Remote-ID des VPN-Peers, wie er sie in der AUTH-Verhandlung mit dem OpenBAT-Gateway überträgt.	▶ Start ▶ Interim-Update ▶ Stop
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut “95” (siehe unten).	▶ Start ▶ Interim-Update ▶ Stop
8	Framed-IP-Address	IPv4-Adresse des VPN-Clients.	▶ Start ▶ Interim-Update ▶ Stop
31	Calling-Station-Id	Gibt die ID (als IPv4- oder IPv6-Adresse) der rufenden Station an (z. B. des VPN-Clients).	▶ Start ▶ Interim-Update ▶ Stop
32	NAS-Identifier	Der Gerätename des Gateways.	▶ Start ▶ Interim-Update ▶ Stop
40	Acct-Status-Type	Beinhaltet den Status-Typ “Start” (1).	▶ Start
40	Acct-Status-Type	Beinhaltet den Status-Typ “Interim-Update” (3).	▶ Interim-Update
40	Acct-Status-Type	Beinhaltet den Status-Typ “Stop” (2).	▶ Stop
42	Acct-Input-Octets	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	▶ Interim-Update ▶ Stop
43	Acct-Output-Octets	Enthält die Anzahl der zum VPN-Peer gesendeten Oktette. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	▶ Interim-Update ▶ Stop

ID	Bezeichnung	Bedeutung	Status-Typ
44	Acct-Session-Id	Der Name des VPN-Peers und der Zeitstempel zum Session-Start bilden die eindeutige Session-ID.	▶ Start ▶ Interim-Update ▶ Stop
46	Acct-Session-Time	Enthält die verstrichene Zeit in Sekunden seit Beginn der Session.	▶ Interim-Update ▶ Stop
47	Acct-Input-Packets	Enthält die Anzahl der aktuell aus Richtung VPN-Peer empfangenen Datenpakete.	▶ Interim-Update ▶ Stop
48	Acct-Output-Packets	Enthält die Anzahl der aktuell zum VPN-Peer gesendeten Datenpakete.	▶ Interim-Update ▶ Stop
49	Acct-Terminate-Cause	Enthält die Ursache für die Beendigung der Session.	▶ Stop
52	Acct-Input-Gigawords	Enthält die Anzahl der aus Richtung VPN-Peer empfangenen Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	▶ Interim-Update ▶ Stop
53	Acct-Input-Gigawords	Enthält die Anzahl der zum VPN-Peer gesendeten Gigawords. Der Wert bezieht sich auf die entschlüsselten Daten, beginnend mit dem IP-Header.	▶ Interim-Update ▶ Stop
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gateways an, das den Zugang für einen Anwender anfragt. Erfolgt die Verbindung über eine IPv6-Verbindung, überträgt das Gateway stattdessen das Attribut “4” (siehe oben).	▶ Start ▶ Interim-Update ▶ Stop
168	Framed-IPv6-Address	IPv6-Adresse des VPN-Clients.	▶ Start ▶ Interim-Update ▶ Stop

10.16.7 Replay-Detection

Mit der Replay-Detection beinhaltet der IPsec-Standard eine Möglichkeit, sogenannte Replay-Attacken zu erkennen. Bei einer Replay-Attacke sendet eine Station die zuvor unberechtigt protokollierten Daten an eine Gegenstelle, um eine andere als die eigene Identität vorzutäuschen.

Die Idee der Replay-Detection besteht darin, eine bestimmte Anzahl von aufeinander folgenden Paketen zu definieren (ein "Fenster" mit der Länge "n"). Da der IPSec-Standard die Pakete mit einer fortlaufenden Sequenznummer versieht kann das empfangene VPN-Gerät feststellen, ob ein Paket eine Sequenznummer aus dem zulässigen Fensters trägt. Wenn z. B. die aktuell höchste empfangene Sequenznummer 10.000 lautet bei einer Fensterbreite von 100, dann liegt die Sequenznummer 9.888 außerhalb des erlaubten Fensters.

Die Replay-Detection verwirft emfpangene Pakete dann, wenn sie entweder:

- eine Sequenznummer vor dem aktuellen Fenster tragen, in diesem Fall betrachtet die Replay-Detection als zu alt, oder
- eine Sequenznummer tragen, welche das VPN-Gerät zuvor schon einmal empfangen hat, in diesem Fall wertet die Replay-Detection dieses Paket als Teil einer Replay-Attacke

Bitte beachten Sie bei der Konfiguration des Fensters für die Replay-Detection folgende Aspekte:

- wenn Sie das Fenster zu groß wählen, übersieht die Replay-Detection möglicherweise eine aktuell von einem Angreifer ausgeführte Replay-Attacke
- wenn Sie das Fenster zu klein wählen, verwirft die Replay-Detection aufgrund einer während der Datenübertragung geänderten Paketreihenfolge möglicherweise rechtmäßige Pakete und erzeugt so Störungen in der VPN-Verbindung

Hinweis: Wägen Sie den Einsatz der Replay-Detection in Ihrem speziellen Anwendungsfall ab. Aktivieren Sie die Replay-Detection nur dann, wenn Sie die Sicherheit der VPN-Verbindung höher bewerten als die störungsfreie Datenübertragung.

10.17 Anwendungskonzepte für LANconfig

In diesem Abschnitt finden Sie verschiedene Anwendungskonzepte für LANconfig.

10.17.1 1-Click-VPN für Netzwerke (Site-to-Site)

Die Einstellungen für die Kopplung von Netzwerken können sehr komfortabel über den 1-Click-VPN-Assistenten vorgenommen werden. Dabei können sogar mehrere Router gleichzeitig an einen zentrales Netzwerk gekoppelt werden.

1. Markieren Sie in LANconfig die Router, für die Sie eine VPN-Kopplung zu einem zentralen Router einrichten möchten.
2. Ziehen Sie die Geräte mit der Maus auf den Eintrag für den zentralen Router.
3. Der 1-Click-VPN Site-to-Site-Assistent startet. Geben Sie den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
4. Wählen Sie aus, ob der Verbindungsaufbau über den Namen bzw. die IP-Adresse des zentralen Routers oder über eine ISDN-Verbindung erfolgen soll. Geben Sie dazu die Adresse bzw. den Namens des zentralen Routers bzw. seine ISDN-Nummer an.
5. Im letzten Schritt legen Sie fest, wie die verbundenen Netzwerke untereinander kommunizieren können:
   - Nur das INTRANET der Zentrale wird für die Außenstellen verfügbar gemacht.
   - Alle privaten Netze der Außenstellen können ebenfalls über die Zentrale untereinander verbunden werden.

Hinweis: Alle Eingaben werden nur einmal für das Zentralgerät vorgenommen und dann in den Geräteeigenschaften hinterlegt.

10.17.2 1-Click-VPN für Advanced VPN Client

VPN-Zugänge für Mitarbeiter, die sich mit Hilfe des LANCOM Advanced VPN Clients in ein Netzwerk einwählen, lassen sich sehr einfach mit dem Setup-Assistenten erstellen und in eine Datei exportieren, die vom LANCOM Advanced VPN Client als Profil eingelesen werden kann. Dabei werden die erforderlichen Informationen der aktuellen Konfiguration des VPN-Routers entnommen und mit zufällig ermittelten Werten ergänzt (z. B. für den Preshared Key).

1. Starten Sie im LANconfig über **Gerät** > **Setup Assistent** den Setup-Assistenten **Einwahl-Zugang bereitstellen (RAS, VPN)**.
2. Wählen Sie im Folgefenster **VPN-Verbindung-über das Internet** und klicken Sie **Weiter**.
3. Wählen Sie aus der Liste den Eintrag **LANCOM Advanced VPN Client […]** und aktivieren Sie die Option **Beschleunigen Sie das Konfigurieren mit 1-Click-VPN**.
4. Geben Sie im nächsten Schritt den Namen für diesen Zugang ein und wählen Sie aus, über welche Adresse der Router aus dem Internet erreichbar ist.
5. Im letzten Schritt können Sie wählen, wie die neuen Zugangsdaten ausgegeben werden sollen:

   - Profil als Importdatei für den LANCOM Advanced VPN Client speichern
   - Profil per E-Mail versenden
   - Profil ausdrucken

Gefahr: Das Versenden der Profildatei per E-Mail stellt ein Sicherheitsrisiko dar, weil die E-Mail unterwegs ggf. abgehört werden könnte. Zum Versenden der Profildatei per E-Mail muss in der Konfiguration des Geräts ein SMTP-Konto mit den erforderlichen Zugangsdaten eingerichtet sein. Außerdem muss auf dem Konfigurationsrechner ein E-Mail-Programm als Standard-Mail-Anwendung eingerichtet sein, über die auch andere Anwendungen E-Mails versenden dürfen.

Beim Erstellen des VPN-Zugangs werden Einstellungen verwendet, die optimal auf die Verwendung im LANCOM Advanced VPN Client abgestimmt sind, darunter z. B.:

- Gateway: Sofern im VPN-Router definiert, wird hier ein DynDNS-Name verwendet, ansonsten die IP-Adresse
- FQDN: Kombination aus dem Namen der Verbindung, einer fortlaufenden Nummer und der internen Domäne im VPN-Router
- Domäne: Sofern im VPN-Router definiert, wird hier die interne Domäne verwendet, ansonsten ein DynDNS-Name oder die IP-Adresse
- VPN IP-Netze: Alle im Gerät definierten IP-Netzwerke vom Typ 'Intranet'.
- Preshared Key: Zufällig generierter Schlüssel mit einer Länge von 16 ASCII-Zeichen.
- Verbindungsmedium: Für den Verbindungsaufbau wird das LAN genutzt.
- VoIP-Priorisierung: Die VoIP-Priorisierung ist standardmäßig aktiviert.
- Exchange Mode: Als Exchange-Mode wird der 'Aggressive Mode' verwendet.
- IKE-Config-Mode: Der IKE-Config-Mode ist aktiviert, die IP-Adress-Informationen für den LANCOM Advanced VPN Client werden automatisch vom VPN-Router zugewiesen.

11 Virtuelle LANs (VLANs)

11.1 Was ist ein Virtuelles LAN?

Die steigende Verfügbarkeit von preiswerten Layer-2-Switches erlaubt den Aufbau sehr viel größerer LANs als in der Vergangenheit. Bisher wurden oft kleinere Abschnitte eines Netzwerks mit Hubs zusammengeschlossen. Diese einzelnen Segmente (Collision Domains) wurden dann über Router zu größeren Einheiten zusammengeschlossen. Da ein Router jedoch immer die Grenze zwischen zwei LANs bildet, entstehen in dieser Struktur mehrere LANs mit eigenen IP-Adresskreisen.

Mit dem Einsatz von Switches können dagegen sehr viel mehr Stationen zu einem großen LAN zusammen geschlossen werden. Durch die gezielte Steuerung des Datenflusses auf die einzelnen Ports wird die verfügbare Bandbreite besser genutzt als beim Einsatz von Hubs, die Konfiguration und Wartung von Routern im Netzverbund entfällt.

Aber auch eine auf Switches basierende Netzwerkstruktur hat ihrer Nachteile:

- Broadcasts werden wie auch bei den Hubs über das gesamte LAN gesendet, selbst wenn die entsprechenden Datenpakete nur für ein bestimmtes Segment des LANs von Bedeutung sind. Bei einer ausreichenden Anzahl von Stationen im Netz kann das schon zu einer deutlichen Einschränkung der verfügbaren Bandbreite im LAN führen.
- Der gesamte Datenverkehr auf dem physikalischen LAN ist “öffentlich”. Selbst wenn einzelne Segmente unterschiedliche IP-Adresskreise nutzen, kann jede Station im LAN theoretisch den Datenverkehr aus allen logischen Netzen auf dem Ethernetstrang abhören. Der Schutz einzelner LAN-Segmente mit Firewalls oder Router erhöht wieder die Anforderungen an die Administration des Netzwerks.

Eine Möglichkeit, diese Probleme zu überwinden, stellen die virtuellen LANs (VLAN) dar, wie sie in IEEE 802.1p/q beschrieben sind. Bei diesem Konzept werden auf einem physikalischen LAN mehrere virtuelle LANs definiert, die sich gegenseitig nicht behindern und die auch den Datenverkehr der jeweils

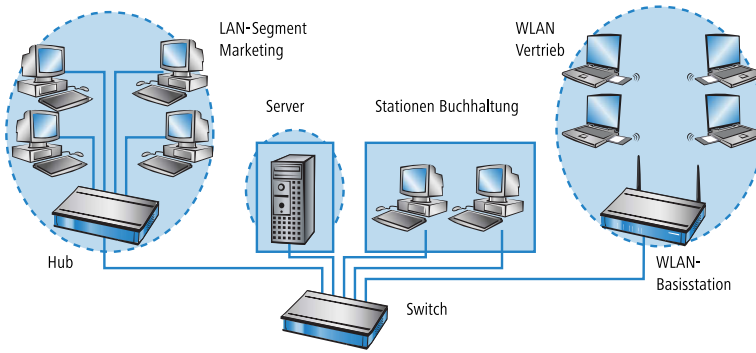
anderen VLANs auf dem physikalischen Ethernetstrang nicht empfangen oder abhören können.

11.2 So funktioniert ein VLAN

Mit der Definition von VLANs auf einem LAN sollen folgende Ziele erreichet werden:

- Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern abgeschirmt werden.
- Der Broadcast-Datenverkehr soll ebenfalls auf die logischen Einheiten reduziert werden und nicht das gesamte LAN belasten.
- Der Datenverkehr von bestimmten logischen Einheiten soll gegenüber anderen Netzteilnehmern mit einer besonderen Priorität übertragen werden.

Zur Verdeutlichung ein Beispiel: In einem LAN ist an einem Switch ein Hub angeschlossen, der vier Stationen aus dem Marketing an das Netz anbindet. Ein Server und zwei Stationen der Buchhaltung sind direkt an den Switch angeschlossen. Den letzten Abschnitt bildet die Basisstation eines Funknetzwerks, in dem sich vier WLAN-Clients aus dem Vertrieb befinden.



Die Stationen aus Marketing und Vertrieb sollen miteinander kommunizieren können. Außerdem sollen Sie auf den Server zugreifen. Die Buchhaltung benötigt ebenfalls Zugriff auf den Server, soll aber ansonsten von den anderen Stationen abgeschirmt werden.

11.2.1 Frame-Tagging

Um den Datenverkehr eines virtuellen LANs gegen die anderen Netzteilnehmer abschirmen und ggf. priorisieren zu können, müssen die Datenpakete eine entsprechende Kennzeichnung aufweisen. Dazu werden die MAC-Frames um ein zusätzliches Merkmal (ein “Tag”) erweitert. Das entsprechende Verfahren wird daher auch als “Frame-Tagging” bezeichnet.

Das Frame-Tagging muss dabei so realisiert sein, dass folgende Anforderungen erfüllt werden:

- Datenpakete mit und ohne Frame-Tagging müssen auf einem physikalischen LAN parallel nebeneinander her existieren können.
- Stationen und Switches im LAN, welche die VLAN-Technik nicht unterstützen, müssen die Datenpakete mit Frame-Tagging ignorieren bzw. wie “normale” Datenpakete behandeln.

Das Tagging wird durch ein zusätzliches Feld im MAC-Frame realisiert. In diesem Feld sind zwei für das virtuelle LAN wesentliche Informationen enthalten:

- **VLAN-ID**: Mit einer eindeutigen Nummer wird das virtuelle LAN gekennzeichnet. Diese ID bestimmt die Zugehörigkeit eines Datenpakets zu einem logischen (virtuellen) LAN. Mit diesem 12-Bit-Wert können bis zu 4094 unterschiedliche VLANs definiert werden (die VLAN-IDs “0” und “4095” sind reserviert bzw. nicht zulässig).

  Hinweis: Die VLAN-ID “1” wird von vielen Geräten als Default-VLAN-ID verwendet. Bei einem unkonfigurierten Gerät gehören alle Ports zu diesem Default-VLAN. Diese Zuweisung kann bei der Konfiguration allerdings auch wieder verändert werden.

- **Priorität**: Die Priorität eines VLAN-gekennzeichneten Datenpakets wird mit einem 3-Bit-Wert markiert. Dabei steht die “0” für die geringste, die “7” für die höchste Priorität. Datenpakete ohne VLAN-Tag werden mit der Priorität “0” behandelt.

Durch dieses zusätzliche Feld werden die MAC-Frames länger als eigentlich erlaubt. Diese “überlangen” Pakete können nur von VLAN-fähigen Stationen und Switches richtig erkannt und ausgewertet werden. Bei Netzteilnehmern ohne VLAN-Unterstützung führt das Frame-Tagging quasi nebenbei zum gewünschten Verhalten:

- Switches ohne VLAN-Unterstützung leiten diese Datenpakete einfach weiter und ignorieren die zusätzlichen Felder im MAC-Frame.
- Stationen ohne VLAN-Unterstützung können in den Paketen aufgrund des eingefügten VLAN-Tags den Protokolltyp nicht erkennen und verwerfen sie stillschweigend.

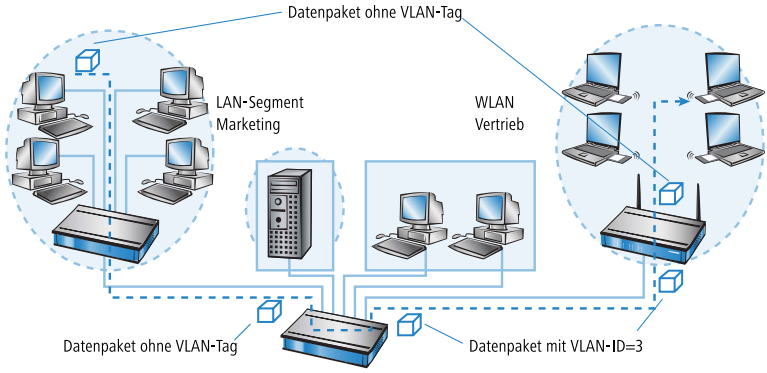
Hinweis: Ältere Switches im LAN können überlange Frames möglicherweise nicht richtig zwischen den einzelnen Ports weiterleiten und verwerfen die getaggten Pakete.

11.2.2 Umsetzung in den Schnittstellen des LANs

Mit den virtuellen LANs sollen bestimmte Stationen zu logischen Einheiten zusammengefasst werden. Die Stationen selbst können aber die notwendigen VLAN-Tags in der Regel weder erzeugen noch verarbeiten.

Der Datenverkehr zwischen den Netzteilnehmern läuft immer über die verschiedenen Schnittstellen (Interfaces) der Verteiler im LAN. Diesen Verteilern (Switches, Basisstationen) fällt damit also die Aufgabe zu, die VLAN-Tags der gewünschten Anwendung entsprechend in die Datenpakte einzubauen, sie auszuwerten und ggf. wieder zu entfernen. Da die logischen Einheiten jeweils mit den verschiedenen Interfaces der Verteiler verbunden sind, werden die Regeln über die Generierung und Verarbeitung der VLAN-Tags den einzelnen Schnittstellen zugewiesen.

Greifen wir dazu das erste Beispiel wieder auf:



Ein Rechner aus dem Marketing schickt ein Datenpaket an einen Rechner im Vertrieb. Der Hub im Marketing leitet das Paket einfach weiter an den Switch. Der Switch empfängt das Paket auf seinem Port Nr. 1 und weiß, dass dieser Port zum VLAN mit der VLAN-ID “3” gehört. Er setzt in den MAC-Frame das zusätzliche Feld mit dem richtigen VLAN-Tag ein und gibt das Paket auch nur auf den Ports (2 und 5) wieder aus, die ebenfalls zum VLAN 3 gehören. Die Basisstation im Vertrieb empfängt das Paket auf dem LAN-Interface. Anhand der Einstellungen kann die Basisstation erkennen, dass die WLAN-Schnittstelle ebenfalls zum VLAN 3 gehört. Sie entfernt das VLAN-Tag aus dem MAC-Frame und gibt das Paket auf der drahtlosen Schnittstelle wieder aus. Der Client im WLAN kann das Paket, das nun wieder die “normale” Länge hat, wie jedes andere Datenpaket ohne VLAN-Tagging verarbeiten.

11.2.3 VLAN Q-in-Q-Tagging

VLANs nach IEEE 802.1q werden üblicherweise eingesetzt, um mehrere Netzwerke auf einem gemeinsamen physikalischen Medium zu betreiben, die dennoch untereinander abgeschirmt werden sollen. In manchen Fällen werden VLANs aber auch auf öffentlichen Netzen der Provider verwendet, um die Netzwerke von verschiedenen Unternehmen zu trennen. Damit können sowohl im LAN als auch der WAN-Strecke VLAN-Tags zum Einsatz kommen – VLAN-getaggte LAN-Pakete müssen zur Übertragung im WAN daher mit einem weiteren VLAN-Tag versehen werden. Zur Steuerung des VLAN-Taggings kann das Verhalten für jeden Port separat definiert werden.

11.2.4 Anwendungsbeispiele

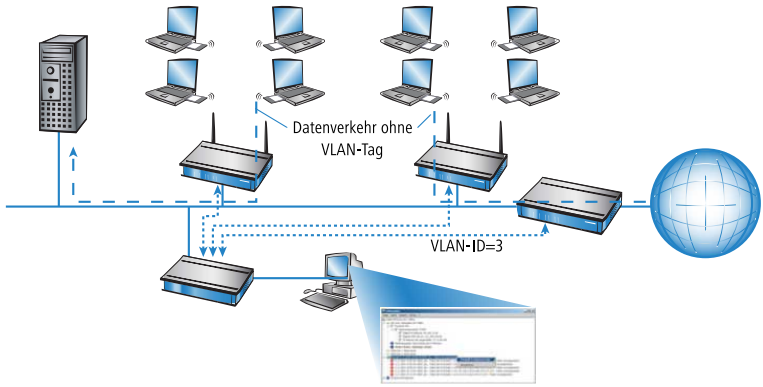
Die Hauptanwendung von virtuellen LANs ist die Aufgabe, auf einem physikalischen Ethernetstrang unterschiedliche logische Netzwerke einzurichten, deren Datenverkehr vor den anderen logischen Netzen geschützt ist.

Die folgenden Abschnitte zeigen Beispiele für den Einsatz von virtuellen LANs vor diesem Hintergrund.

Management- und User-Traffic auf einem LAN

Auf dem Campus einer Universität werden mehrere Hot-Spots aufgestellt. Damit ist den Studenten über Notebooks mit WLAN-Karten der Zugang zum

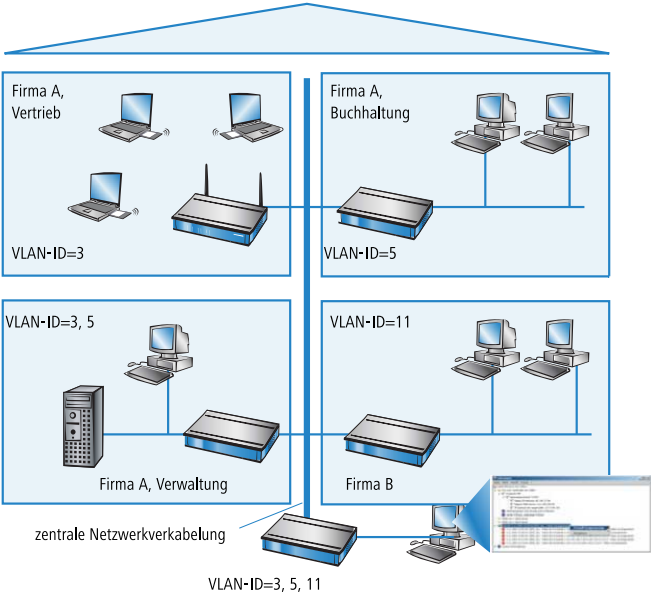
Server der Bibliothek und zum Internet möglich. Die Hot-Spots sind an das LAN der Universität angeschlossen. Über dieses LAN greifen die Administratoren auch auf die Basisstationen zu, um über SNMP verschiedene Management-Aufgaben zu erledigen.



Mit dem Einrichten eines virtuellen LANs zwischen den Basisstationen und dem Switch des Administratoren wird der Management-Datenverkehr von dem “öffentlichen” Verkehr auf dem LAN abgeschirmt.

Verschiedene Organisationen auf einem LAN

Die Flexibilität der modernen Arbeitswelt bringt für die Administratoren neue Herausforderungen an die Planung und Wartung der Netzwerkstrukturen. In öffentlichen Bürogebäuden ändert sich permanent die Belegung der Räume durch die Mieter, und auch innerhalb einer Firma werden die Teams häufig neu zusammengestellt. In beiden Fällen müssen die einzelnen Einheiten jedoch über ein unabhängiges, abgeschirmtes LAN verfügen. Diese Aufgabe lässt sich mit Änderungen an der Hardware nur sehr aufwändig oder gar nicht realisieren, weil z. B. in einem Bürogebäude nur eine zentrale Verkabelung vorhanden ist.



Mit virtuellen LANs lässt sich diese Aufgabe sehr elegant lösen. Auch bei einem späteren Wechsel von Abteilungen oder Firmen im Gebäude kann die Netzstruktur sehr einfach angepasst werden.

Alle Netzteilnehmer nutzen in diesem Beispiel das zentrale Ethernet, das mit den angeschlossenen Geräten von einem Dienstleister überwacht wird. Die Firma A hat drei Abteilungen in zwei Etagen. Der Vertrieb kann über die VLAN-ID 3 mit der Verwaltung kommunizieren, die Buchhaltung mit der Verwaltung über die VLAN-ID 5. Untereinander sehen sich die Netze von Buchhaltung und Vertrieb nicht. Die Firma B ist über die VLAN-ID 11 ebenfalls von den anderen Netzen abgeschirmt, nur der Dienstleister kann zu Wartungszwecken auf alle Geräte zugreifen.

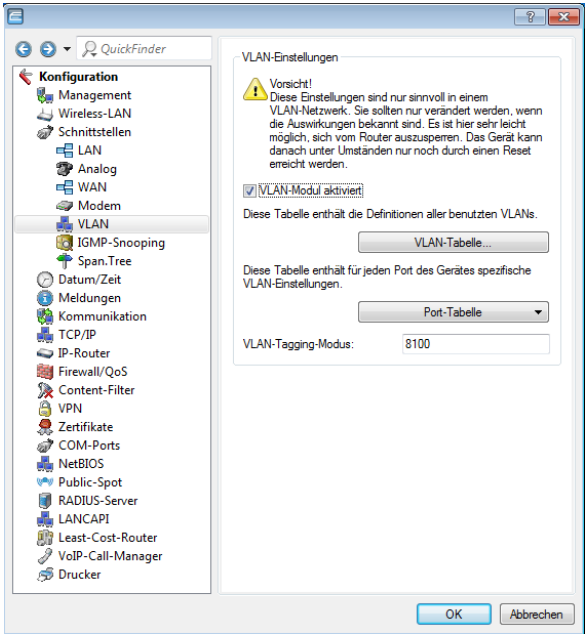
11.3 Konfiguration von VLANs

Die Konfiguration im VLAN-Bereich der Geräte hat zwei wichtige Aufgaben:

- Virtuelle LANs definieren und ihnen dabei einen Namen, eine VLAN-ID und die zugehörigen Interfaces zuordnen
- Für die Interfaces definieren, wie mit Datenpaketen mit bzw. ohne VLAN-Tags verfahren werden soll

11.3.1 Allgemeine Einstellungen

In diesem Dialog finden Sie die allgemeinen Einstellungen für das VLAN.



LANconfig: Schnittstellen / VLAN

WEBconfig: HiLCOS-Menübaum / Setup / VLAN

VLAN-Modul aktivieren

Schalten Sie das VLAN-Modul nur ein, wenn Sie mit den Auswirkungen der VLAN-Nutzung vertraut sind.

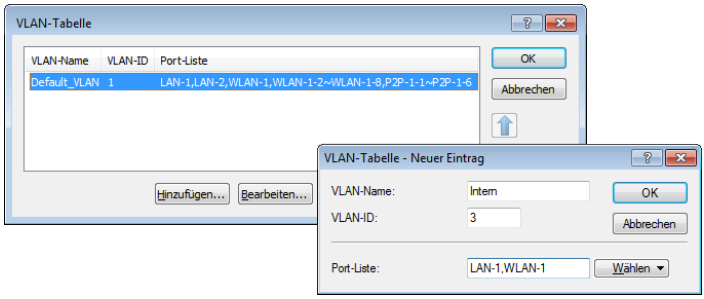
Hinweis: Mit fehlerhaften VLAN-Einstellungen können Sie den Konfigurationszugang zum Gerät verhindern.

VLAN-Tagging-Modus

Beim Übertragen von VLAN-getaggten Netzen über Netze der Provider, die ihrerseits VLAN verwenden, setzen die Provider teilweise spezielle VLAN-Tagging-IDs ein. Um die VLAN-Übertragung darauf einzustellen, kann der Ethernet2-Typ des VLAN-Tags als 'Tag-Value' als 16 Bit-Hexadezimalwert eingestellt werden. Default ist '8100' (VLAN-Tagging nach 802.1p/q), andere gängige Werte für VLAN-Tagging wären z. B. '9100' oder '9901'.

11.3.2 Die Netzwerktabelle

In der Netzwerktabelle werden die virtuellen LANs definiert, an denen das Gerät teilnehmen soll.



LANconfig: Schnittstellen / VLAN / VLAN-Tabelle

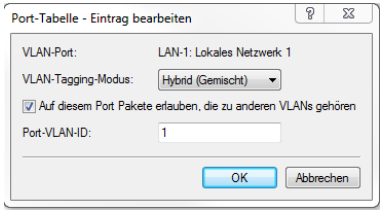
WEBconfig: HiLCOS-Menübaum / Setup / VLAN / Netzwerke

- **VLAN-Name**: Der Name des VLANs dient nur der Beschreibung bei der Konfiguration. Dieser Name wird an keiner anderen Stelle verwendet.
- **VLAN-ID**: Diese Nummer kennzeichnet das VLAN eindeutig.
- **Portliste**: In dieser Liste werden die Interfaces des Geräts eingetragen, die zu dem VLAN gehören.

  Für ein Gerät mit einem LAN-Interface und einem WLAN-Port können z. B. die Ports “LAN-1” und “WLAN-1” eingetragen werden. Bei Portbereichen werden die einzelnen Ports durch eine Tilde getrennt: “P2P-1~P2P-4”.

11.3.3 Die Porttabelle

In der Porttabelle werden die einzelnen Ports des Gerätes für die Verwendung im VLAN konfiguriert. Die Tabelle hat einen Eintrag für jeden Port des Gerätes mit folgenden Werten:



LANconfig: Schnittstellen / VLAN / Port-Tabelle

WEBconfig: HiLCOS-Menübaum / Setup / VLAN / Port-Tabelle

- **Port**: Der Name des Ports, nicht editierbar
- **Tagging-Modus**

  Steuert die Verarbeitung und Zuweisung von VLAN-Tags auf diesem Port.

  - Access (Niemals): Ausgehende Pakete erhalten auf diesem Port kein VLAN-Tag. Eingehende Pakete werden so behandelt, als hätten sie kein VLAN-Tag. Haben die eingehenden Pakete ein VLAN-Tag, so wird es ignoriert und so behandelt, als ob es zur Payload des Paketes gehört. Eingehende Pakete werden immer dem für diesen Port definierten VLAN zugewiesen.
  - Trunk (Immer): Ausgehende Pakete erhalten auf diesem Port immer ein VLAN-Tag, egal ob sie dem für diesen Port definierten VLAN angehören oder nicht. Eingehende Pakete müssen über ein VLAN-Tag verfügen, anderenfalls werden sie verworfen.
  - Hybrid (Gemischt): Erlaubt einen gemischten Betrieb von Paketen mit und ohne VLAN-Tags auf dem Port. Pakete ohne VLAN-Tag werden dem für diesen Port definierten VLAN zugeordnet. Ausgehende Pakete erhalten ein VLAN-Tag, außer sie gehören dem für diesen Port definierten VLAN an.
  - Default: Hybrid (gemischt)

- **Auf diesem Port Pakete erlauben, die zu anderen VLANs gehören**

Diese Option gibt an, ob getaggte Datenpakete mit beliebigen VLAN-IDs akzeptiert werden sollen, auch wenn der Port nicht Mitglied dieses VLANs ist.

- **Port-VLAN-ID**

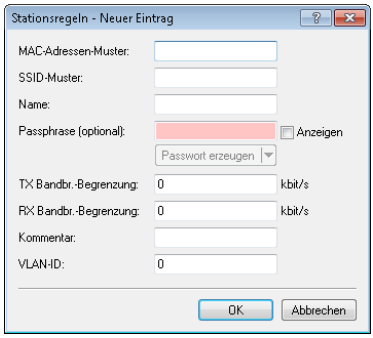
  Diese Port-ID hat zwei Funktionen:

  – Ungetaggte Pakete, die auf diesem Port im Modus "Hybrid (gemischt)" empfangen werden, werden diesem VLAN zugeordnet, ebenso sämtliche ankommenden Pakete im Modus "Access (Niemals)".
  – Im Modus "Hybrid (gemischt)" entscheidet dieser Wert darüber, ob ausgehende Pakete ein VLAN-Tag erhalten oder nicht: Pakete, die dem für diesen Port definierten VLAN zugeordnet wurden, erhalten **kein** VLAN-Tag, alle anderen erhalten ein VLAN-Tag.

11.4 Konfigurierbare VLAN-IDs

11.4.1 VLAN-IDs für WLAN-Clients

VLANs werden im Gerät üblicherweise fest mit einem LAN-Interface verbunden. Alle Pakete, die über dieses Interface geleitet werden, bekommen daher bei Aktivierung des VLAN-Moduls die gleiche VLAN-ID. In manchen Fällen ist es jedoch erwünscht, die verschiedenen Benutzer eines WLANs auch unterschiedlichen VLANs zuzuordnen.



LANconfig: Wireless-LAN / Stationen / Stationen

WEBconfig: HiLCOS-Menübaum / Setup / WLAN / Access-List

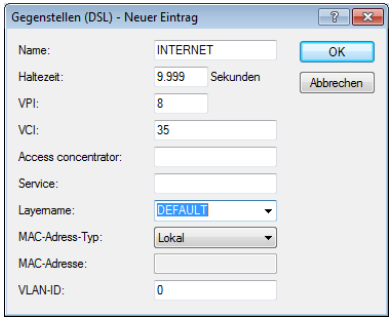
Die client-spezifische VLAN-ID kann Werte von 0 bis 4094 annehmen. der Defaultwert von '0' steht für eine nicht spezifizierte VLAN-ID. In diesem Fall wird der Client dem VLAN-Port des logischen WLAN-Netzwerks zugeordnet.

Folgende Voraussetzungen müssen erfüllt sein, damit die client-spezifische VLAN-Zuweisung gelingt:

- Der VLAN-Betrieb muss aktiviert sein.
- Die VLAN-IDs, die einzelnen Clients zugewiesen werden sollen, müssen in der VLAN-Netzwerk-Tabelle enthalten sein.
- Die LAN-Interfaces und alle WLAN-Interfaces, die von den Clients genutzt werden, müssen dem entsprechenden VLAN zugeordnet sein.

11.4.2 VLAN-IDs für DSL-Interfaces

In manchen DSL-Netzen werden VLAN-Tags verwendet, so wie sie auch in lokalen Netzen zur Unterscheidung von logischen Netzwerken auf gemeinsamen genutzten Übertragungsmedien eingesetzt werden. Um diese VLAN-Tags im Router richtig verarbeiten zu können, kann zu jeder DSL-Gegenstelle eine entsprechende VLAN-ID definiert werden.



LANconfig: Kommunikation / Gegenstellen / Gegenstellen (DSL)

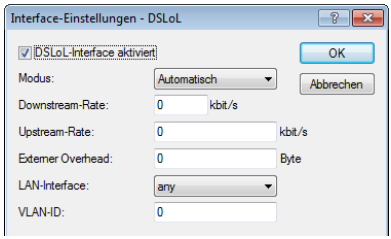
WEBconfig: HiLCOS-Menübaum / Setup / WAN / DSL-Breitband-Gegenstellen

- **VLAN-ID**

ID, mit der das VLAN auf der DSL-Verbindung eindeutig identifiziert werden kann.

11.4.3 VLAN-IDs für DSLoL-Interfaces

Um den Datenverkehr über ein DSLoL-Interface besser von restlichen Traffic separieren zu können, kann für das DSLoL-Interface unter `Setup/Interfaces/DSLoL` oder im LANconfig im Konfigurationsbereich 'Interfaces' auf der Registerkarte 'WAN' bei den Interface-Einstellungen für das DSLoL-Interface im Feld 'VLAN-ID' eingestellt werden.



11.5 VLAN-Tags auf Layer 2/3 im Ethernet

11.5.1 Einleitung

VLAN-Tags bieten auch bei solchen Switches, die keine IP-Header auswerten können, die Möglichkeit einer einfachen QoS-Steuerung. Der Standard IEEE 802.1p definiert ein Prioritäts-Tag im VLAN-Header mit einer Länge von drei Bit, das den ersten drei Bit des DSCP-Felder (Differentiated Services Code Point – DiffServ) bzw. der Precedence im TOS-Feld (Type of Service) entspricht. Bei der Verarbeitung der VLAN-getaggten Pakete müssen Empfangs- und Senderichtung getrennt betrachtet werden:

- Wird ein getaggtes Ethernet-Paket empfangen, so gibt es drei Möglichkeiten das Tag zu verarbeiten:
  - Das VLAN-Tag wird ignoriert.
  - Das VLAN-Tag wird immer in das DiffServ- bzw. TOS-Feld kopiert.

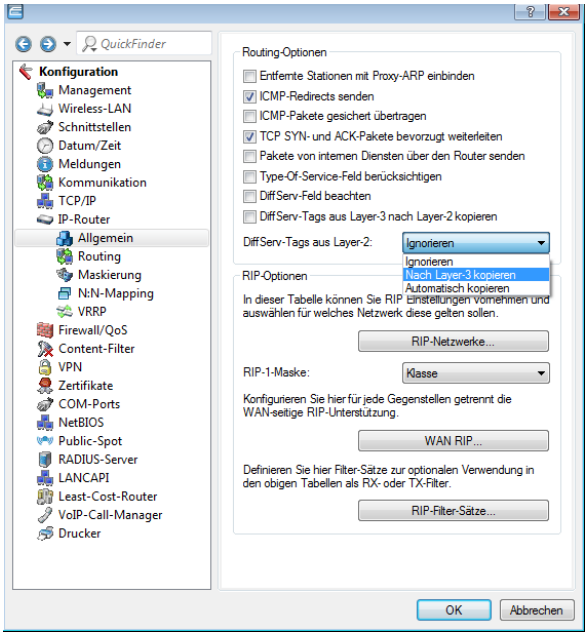
- Das VLAN-Tag wird nur dann in das DiffServ- bzw. TOS-Feld kopiert, wenn dort noch keine Kennzeichnung vorhanden ist, die Precedence also '000' ist.

- Beim Senden eines Paketes auf das Ethernet kann das VLAN-Tag in Abhängigkeit von der Precedence gesetzt werden. Dies darf aber nur dann geschehen, wenn der Empfänger diese Tags auch versteht, d.h. getaggte Pakete empfangen kann. Daher werden die Tags nur für solche Stationen gesetzt, wenn HiLCOS von der jeweiligen Adresse getaggte Pakete empfangen hat.

Hinweis: Beim Empfang eines getaggten Pakets wird das Tag im zugehörigen Eintrag der Verbindungsliste gespeichert. Wenn ein Paket mit gesetzter Precedence gesendet werden soll, dann wird die zuvor hinterlegte VLAN-ID mit der Precedence in das Paket als VLAN-Tag eingetragen. Wenn von einer Verbindung weitere Verbindungen geöffnet werden, wie z. B. bei FTP oder H.323, dann wird das Tag an die neuen Einträge vererbt.

11.5.2 Konfiguration des VLAN-Taggings auf Layer 2/3

Bei der Konfiguration des VLAN-Taggings auf Layer 2/3 wird neben den allgemeinen Routing-Einstellungen das Verhalten beim Empfangen und beim Senden getaggten Pakete definiert.



LANconfig: IP-Router / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / IP-Router / Routing-Methode

- **Type-Of-Service-Feld berücksichtigen**

  Das TOS/DiffServ-Feld wird als TOS-Feld betrachtet, es werden die Bits 'Low-Delay' und 'High-Reliability' ausgewertet.

- **DiffServ-Feld beachten**

  Das TOS/DiffServ-Feld wird als DiffServ-Feld betrachtet. Nach Auswertung der Precedence werden Pakete mit den Code Points 'AFxx' gesichert und Pakete mit den Code Points 'EF' bevorzugt übertragen. Alle anderen Pakete werden normal übertragen.

- **DiffServ-Tags aus Layer-2**

  Die Einstellung für das Layer2-Layer3-Tagging regelt das Verhalten beim Empfangen eines Datenpakets:

  - Ignorieren: VLAN-Tags werden ignoriert.

- Nach Layer-3 kopieren: Prioritäts-Bits im VLAN-Tag werden immer in die Precedence des DSCP kopiert.
- Automatisch kopieren: Prioritäts-Bits im VLAN-Tag werden nur dann in die Precedence des DSCP kopiert, wenn diese '000' ist.

▶ **DiffServ-Tags aus Layer-3 nach Layer-2 kopieren**

Die Einstellung für das Layer3-Layer2-Tagging regelt das Verhalten beim Senden eines Datenpakets. Wenn diese Option aktiuviert ist, werden VLAN-Tags mit Prioritäts-Bits erzeugt, die aus der Precedence des DSCP stammen, wenn der Empfänger mindestens ein getaggtes Paket verschickt hat.

12 Wireless LAN – WLAN

12.1 Einleitung

Hinweis: Die folgenden Abschnitte beschreiben allgemein die Funktionalität des HiLCOS-Betriebssystems im Zusammenhang mit Funknetzwerken. Welche Funktionen von Ihrem Gerät unterstützt werden, entnehmen Sie bitte dem Handbuch zum jeweiligen Gerät.

In diesem Kapitel stellen wir Ihnen kurz die Technologie von Funk-Netzwerken vor. Außerdem geben wir Ihnen einen Überblick über die vielfältigen Einsatzmöglichkeiten, Funktionen und Fähigkeiten Ihrer Hirschmann WLAN-Geräte.

Ein Funk-LAN verbindet einzelne Endgeräte (PCs und mobile Rechner) zu einem lokalen Netzwerk (auch LAN – **L**ocal **A**rea **N**etwork). Im Unterschied zu einem herkömmlichen LAN findet die Kommunikation nicht über Netzwerkkabel, sondern über Funkverbindungen statt. Aus diesem Grund nennt man ein Funk-LAN auch **W**ireless **L**ocal **A**rea **N**etwork (WLAN).

In einem Funk-LAN stehen alle Funktionen eines kabelgebundenen Netzwerks zur Verfügung: Zugriff auf Dateien, Server, Drucker etc. ist ebenso möglich wie die Einbindung der einzelnen Stationen in ein firmeninternes Mailsystem oder der Zugang zum Internet.

Die Vorteile von Funk-LANs liegen auf der Hand: Notebooks und PCs können dort aufgestellt werden, wo es sinnvoll ist – Probleme mit fehlenden Anschlüssen oder baulichen Veränderungen gehören bei der drahtlosen Vernetzung der Vergangenheit an. Funk-LANs sind außerdem einsetzbar für Verbindungen über größere Distanzen. Teure Mietleitungen und die damit verbundenen baulichen Maßnahmen können gespart werden.

- Access Points (APs) werden üblicherweise verwendet, um ein oder mehrere WLANs mit kabelgebundenen LAN zu verbinden. Sie übertragen dabei die Daten der Clients nur in der Funktion einer “Bridge”, das Routing ins Internet oder zu anderen Gegenstellen wird von anderen Netzwerkkompo-

nenten übernommen. Die APs verfügen daher in der Regel nur über eine oder mehrere Ethernetschnittstellen.

Die Geräte können entweder als autarke APs mit eigener Konfiguration betrieben werden (WLAN-Module in der Betriebsart „Access Point-Modus“) oder als Teilnehmer in einer WLAN-Infrastruktur, die von einem zentralen WLAN-Controller (WLC) gesteuert wird (Betriebsart „Managed-Modus“).

12.2 LANCOM Active Radio Control (ARC)

Mit dem intelligenten WLAN-Optimierungskonzept **LANCOM Active Radio Control (ARC)** optimieren Sie nachhaltig Ihr Funkfeld und vermeiden proaktiv Störquellen im WLAN. Active Radio Control besteht aus mehreren, sich ideal ergänzenden Funktionen im Hirschmann Betriebssystem HiLCOS, mithilfe dessen Sie die Leistungsfähigkeit Ihres WLANs deutlich verbessern. Alle Funktionen von Active Radio Control sind kostenlos enthalten im Hirschmann Betriebssystem HiLCOS und lassen sich einfach über die entsprechenden Management-Tools bedienen.

RF Optimization (Funkfeldoptimierung)

Automatische Auswahl optimaler WLAN-Kanäle: WLAN-Clients profitieren von einem verbesserten Durchsatz dank reduzierter Kanalüberlappungen. In Controller basierten WLAN-Installationen erfolgt eine automatische Auswahl optimaler Kanäle für verwaltete Access Points.

Weitere Informationen dazu finden Sie im Abschnitt *Funkfeldoptimierung* auf Seite 1384.

Band Steering

Nutzen Sie die Bandbreite Ihres WLANs optimal aus: Der automatische, wahlweise vom AP oder WLC gesteuerte Wechsel von Clients in das 5-GHz-Frequenzband verdoppelt die WLAN-Performance, weil meist nur dort genügend Kanäle für eine Kanalbündelung zur Verfügung stehen.

Weitere Informationen dazu finden Sie im Abschnitt *WLAN Band Steering* auf Seite 1199 sowie *Client Steering über den WLC* auf Seite 1388.

Adaptive Noise Immunity

Besserer WLAN-Durchsatz durch Immunität vor Störsignalen:
WLAN-Clients profitieren von deutlich mehr Datendurchsatz dank einer

ungestörten Funkabdeckung. Durch aktivierte Adaptive Noise Immunity blendet ein Access Point Störquellen im Funkfeld aus und fokussiert sich ausschließlich auf WLAN-Clients mit ausreichender Signalstärke.

Weitere Informationen dazu finden Sie im Abschnitt *Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN* auf Seite 1215.

Spectral Scan

Überprüfen Sie Ihr WLAN-Funkspektrum auf Störquellen: Mit Hirschmann Spectral Scan haben Sie ein professionelles Werkzeug für ein effizientes WLAN-Troubleshooting. Ein Scan des gesamten Funkspektrums identifiziert Störquellen außerhalb des WLANs und ermöglicht eine grafische Darstellung.

Weitere Informationen dazu finden Sie im Abschnitt *Spectral Scan* auf Seite 1207.

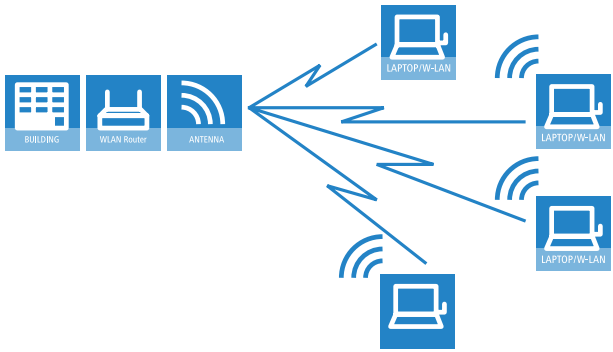
12.3 Anwendungsszenarien

WLAN-Systeme eignen sich in vielen Bereichen als Ersatz für oder Ergänzung zu verkabelten Netzwerken. In manchen Fällen bieten WLANs sogar völlig neue Anwendungsmöglichkeiten, die einen enormen Fortschritt in der Organisation der Arbeit oder deutliche Einsparpotenziale bedeuten.

- Größere Funk-LANs, evtl. Anschluss an LAN und Internet mit einem oder mehreren APs (Infrastruktur-Modus)
- Hotspot oder Gastzugang
- Verbinden zweier LANs über eine Funkstrecke (Point-to-Point-Modus)
- Relaisfunktion zur Verbindung von Netzwerken über mehrere APs
- Anbindung von Geräten mit Ethernet-Schnittstelle über einen AP (Client-Modus)
- Zentrale Verwaltung durch einen WLC (Managed-Modus)
- WDS (Wireless Distribution System)
- Datenübertragung zu bewegten Objekten im Industriebereich
- Durchleiten von VPN-verschlüsselten Verbindungen mit VPN Pass-Through
- Einfache, direkte Verbindung zwischen Endgeräten ohne AP (Ad-hoc-Modus)

12.3.1 Infrastruktur-Modus

Im Infrastruktur-Modus verbinden sich die WLAN-Clients mit einem zentralen Vermittlungspunkt, dem AP. Der AP spannt eine oder mehrere Funkzellen (WLAN-Netzwerke) auf, regelt die Zugangsrechte der WLAN-Clients zu diesen Funkzellen, die Kommunikation der Clients untereinander und den Zugang zu anderen Netzwerken. In größeren WLAN-Anwendungen (z. B. in Unternehmen, deren Geschäftsräume sich über mehrere Gebäude oder Etagen verteilen) können auch mehrere verbundene APs einen gemeinsamen Zugang für WLAN-Clients anbieten. Je nach Bedarf können die Clients zwischen den verschiedenen APs wechseln (Roaming). Da diese Lösung in vielen Hochschulen und Universitäten eingesetzt wird, um den Studenten und wissenschaftlichen Mitarbeitern überall einen Netzwerkzugang zu ermöglichen, spricht man hier auch von „Campus-Ausleuchtung“.

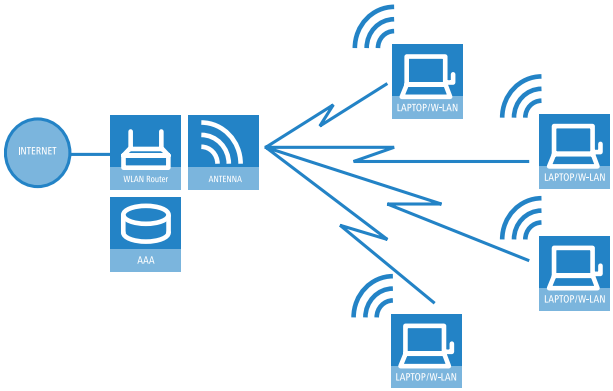


12.3.2 Hotspot oder Gastzugang

Bei einem Hotspot handelt es sich um eine spezielle Variante des zuvor beschriebenen Infrastruktur-Modus. Während der normale Infrastruktur-Modus nur den Mitgliedern einer geschlossenen Benutzergruppe einen Zugang zum Netzwerk mit allen erforderlichen Diensten erlaubt, bietet ein Hotspot gegen Zahlung einer entsprechenden Gebühr allen WLAN-Clients in Reichweite den Netzwerkzugang an (in der Regel beschränkt auf Internetnutzung). Neben den Unterschieden in der Konfiguration der APs werden für den Aufbau eines Hotspots Authentisierungs-, Authorisierungs- und Accountingfunktionen (AAA)

benötigt, wie sie beispielsweise die Public Spot Optionen bereitstellen. Hotspots werden üblicherweise an öffentlichen Orten eingesetzt, an denen sich viele Personen mit Bedarf für einen vorübergehenden Internetzugang aufhalten, z. B. auf Flughäfen, in Cafés oder Hotels.

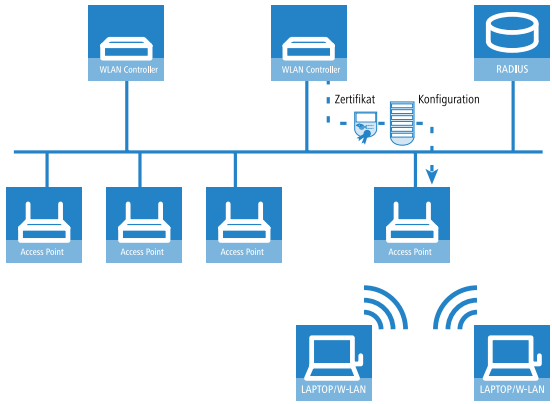
Ein Hotspot bietet einem WLAN-Client ohne Konfigurationsaufwand im AP und nur für eine bestimmte Zeit einen Zugang zum Netzwerk – daher wird diese Variante auch häufig in Unternehmen eingesetzt, um Gästen z. B. einen vorübergehenden Internetzugang zu ermöglichen.



12.3.3 Managed-Modus

Der weit verbreitete Einsatz von Wireless-Geräten hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt. Mit einem zentralen WLAN-Management wird die Konfiguration der APs im Managed-Modus nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC).

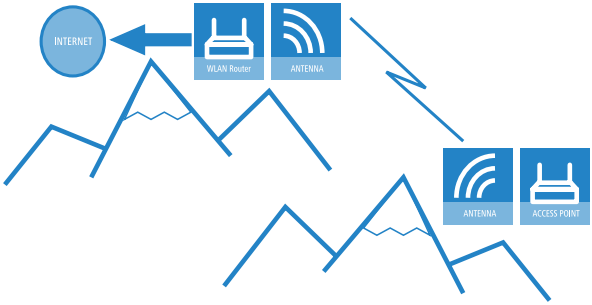
Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten ein Zertifikat und eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus.



12.3.4 WLAN-Bridge (Point-to-Point)

Während es sich bei den bisher vorgestellten Anwendungsszenarien immer um die Anbindung von mehreren WLAN-Clients an einen AP handelt (Point-to-Multipoint), spielen die WLAN-Systeme gerade im Outdoor-Bereich ihre Stärken auch und vor allem bei der Verbindung von zwei APs aus (Point-to-Point). Mit der Einrichtung einer Funkstrecke zwischen zwei APs kann z. B. ein Produktionsgebäude auf einem weitläufigen Unternehmensgelände sehr einfach in das Netzwerk eingebunden werden.

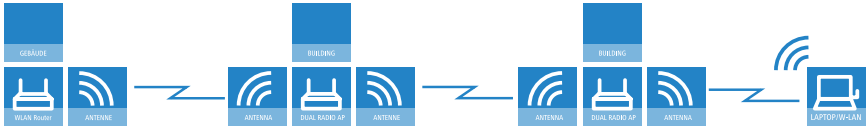
Mit einer Punkt-zu-Punkt-Verbindung kann aber z. B. auch in schwierigem Gelände (z. B. in den Bergen oder auf einer Insel) ein Internetzugang an Orten bereitgestellt werden, an denen eine Verkabelung zu aufwendig wäre. Bei direkter Sichtbeziehungen zwischen den beiden APs können mit diesen Funkstrecken Distanzen von mehreren Kilometern überbrückt werden.



12.3.5 WLAN-Bridge im Relais-Betrieb

In manchen Fällen müssen größere Distanzen zwischen zwei Standorten überbrückt werden als mit einer einfachen Funkstrecke realisiert werden kann. Das ist z. B. dann der Fall, wenn die Distanz zwischen den APs über die tatsächliche Reichweite hinausgeht oder wenn Hindernisse zwischen den APs die direkte Funkübertragung stören oder verhindern.

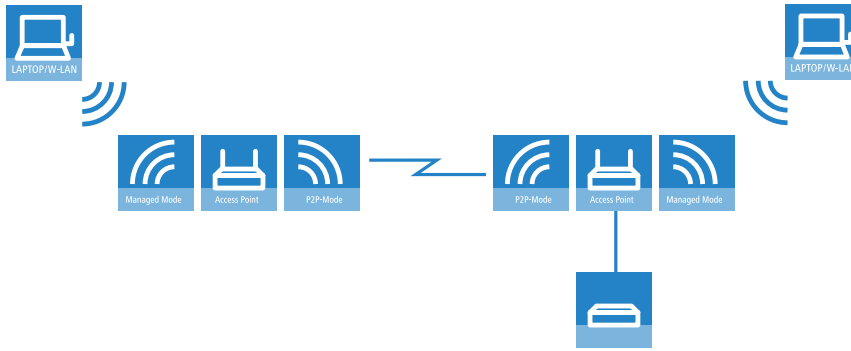
In solchen Fällen kann durch eine Verkettung von mehreren APs mit jeweils zwei WLAN-Modulen eine Verbindung zwischen den beiden Endpunkten hergestellt werden. Da die APs an den Zwischenstationen in der Regel nur als Schaltstelle dienen, nennt man diese Betriebsart der APs auch „Relais-Modus“.



Obwohl Hirschmann APs auch pro Radio-Modul neben WLAN-Clients auch noch mehrere P2P-Strecken gleichzeitig bedienen können, empfiehlt sich aus Performance-Gründen die Verwendung von Hirschmann Access Points mit zwei Funkmodulen für die Relais-Stationen.

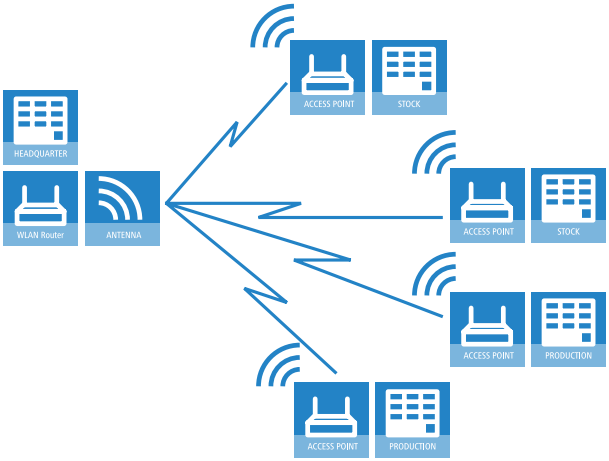
12.3.6 WLAN-Bridge zum AP – managed und unmanaged gemischt

Die von einem zentralen WLC verwalteten APs werden in der Regel direkt mit dem kabelgebundenen Ethernet verbunden. Wenn das nicht möglich ist, können die managed APs auch über eine WLAN-Bridge in das LAN eingebunden werden, sofern sie über zwei WLAN-Module verfügen. Ein WLAN-Modul wird in diesem Anwendungsfall als managed AP betrieben, dieses WLAN-Modul bezieht seine Konfiguration immer zentral vom WLC. Das andere WLAN-Modul wird dabei fest als WLAN-Bridge konfiguriert.



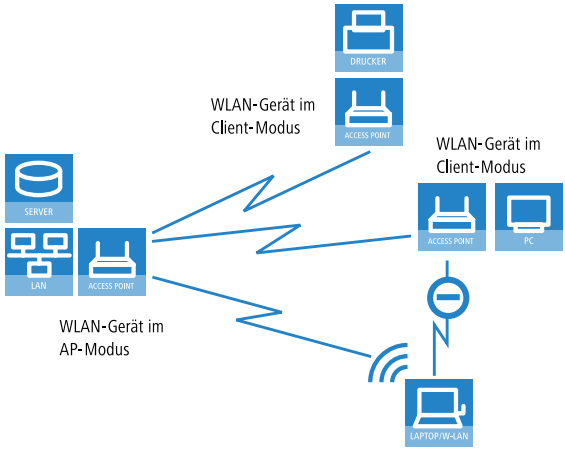
12.3.7 Wireless Distribution System (Point-to-Multipoint)

Eine besondere Variante der Funkstrecken ist die Anbindung von mehreren verteilten APs an eine zentrale Station – das Point-to-Multipoint-WLAN (P2MP) wird auch als Wireless Distribution System bezeichnet (WDS). In dieser Betriebsart werden z. B. mehrere Gebäude auf einem Betriebsgelände mit dem Verwaltungsgebäude verbunden. Der zentrale AP wird dabei als „Master“ konfiguriert, die WDS-Gegenstellen als „Slave“.



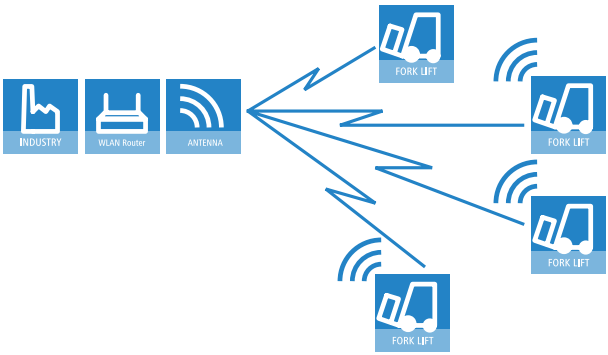
12.3.8 Client-Modus

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können APs in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Adapter verhalten und nicht wie ein AP. Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein WLAN einzubinden.



12.3.9 Client-Modus bei bewegten Objekten im Industriebereich

Völlig neue Anwendungen ermöglichen WLAN-Systeme im industriellen Bereich durch die Datenübertragung zu bewegten Objekten. So ist z. B. in der Logistik eine kontinuierliche Anbindung von Gabelstaplern über WLAN an das Firmennetzwerk möglich. Mit mobilen Barcode-Scannern ausgestattet können so alle Warenbewegungen in einem Lager in Echtzeit an das Warenwirtschaftssystem weitergegeben werden, sodass alle Mitarbeiter jederzeit auf einen aktuellen Lagerbestand zugreifen können.



12.4 WLAN-Standards

Hirschmann WLAN-Geräte arbeiten nach dem IEEE-Standard 802.11. Diese Standard-Familie stellt eine Erweiterung der bereits vorhandenen IEEE-Normen für LANs dar, von denen IEEE 802.3 für Ethernet die bekannteste ist. Innerhalb der IEEE 802.11 Familie gibt es verschiedene Standards für die Funkübertragung in unterschiedlichen Frequenzbereichen und mit unterschiedlichen Geschwindigkeiten. Hirschmann APs unterstützen je nach Ausführung unterschiedliche Standards:

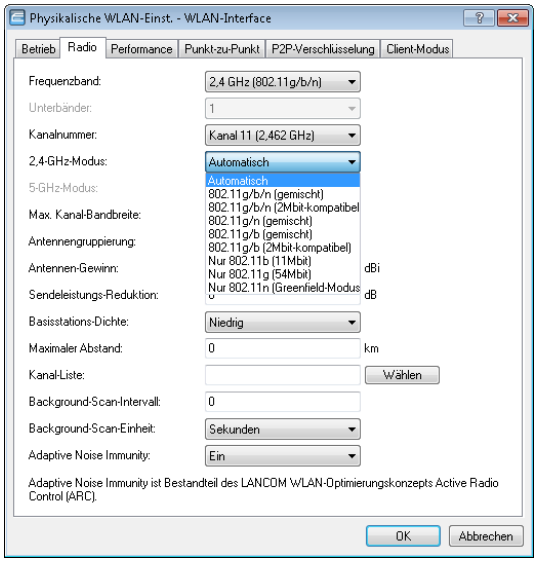
- IEEE 802.11n mit bis zu 300 MBit/s Übertragungsrate im 5 GHz oder 2,4 GHz Frequenzband, mit neuen Mechanismen wie zum Beispiel die Nutzung von MIMO, 40-MHz-Kanälen, Packet Aggregation und Block Acknowledgement.
- IEEE 802.11a mit bis zu 54 MBit/s Übertragungsrate im 5 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).
- IEEE 802.11g mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz Frequenzband, bis zu 108 MBit/s mit Turbo-Modus (Ergänzung zum Standard).
- Auch wenn aktuelle WLAN-Adapter in der Regel nach 802.11a/g/n betrieben werden, untertsützen Hirschmann APs aus Gründen der Kompatibilität zu älteren WLAN-Adaptern auch den Standard IEEE 802.11b mit bis zu 11 MBit/s Übertragungsrate im 2,4 GHz Frequenzband.

Durch die Einhaltung der IEEE-Standards arbeiten die Hirschmann WLAN-Geräte problemlos und zuverlässig auch mit Geräten anderer Hersteller zusammen. Ihr Hirschmann AP unterstützt je nach Modell die Standards IEEE 802.11g (abwärtskompatibel zu IEEE 802.11b) und/oder IEEE 802.11a sowie IEEE 802.11n Draft 2.0.

Der Betrieb des integrierten WLAN-Moduls der APs ist jeweils nur in einem Frequenzband, also entweder 2,4 GHz oder 5 GHz möglich. Der gleichzeitige Betrieb verschiedener Frequenzbänder in einem WLAN-Modul ist nicht möglich – APs mit zwei WLAN-Modulen (Dual-Radio) können hingegen für jedes WLAN-Modul ein anderes Frequenzband nutzen. Da die Standards im 2,4 GHz-Band IEEE 802.11b/g/n abwärtskompatibel zueinander sind, ist der gleichzeitige Betrieb dieser Standards auf einem WLAN-Modul mit Geschwindigkeitseinbußen möglich.

Übertragungsraten im Kompatibilitätsmodus

Bitte beachten Sie, dass die erreichten Datenübertragungsraten bei IEEE 802.11b/g/n-Geräten vom verwendeten 2,4-GHz-Modus abhängen. Werden die langsameren Stationen in einem Funknetzwerk mit eingeschaltetem Kompatibilitätsmodus aktiv, sinkt die tatsächliche Übertragungsrate ab.



Hinweis: Bitte beachten Sie, dass nicht alle Frequenzen in jedem Land erlaubt sind! Eine Tabelle mit den Frequenzen und die Zulassungsvorschriften finden Sie im Anhang des Handbuchs zum jeweiligen Gerät.

12.4.1 IEEE 802.11n

Mit einer Reihe von technologischen Veränderungen erlaubt 802.11n, die Performance von WLAN-Systemen im 5 GHz oder 2,4 GHz Frequenzband etwa um das Fünffache zu steigern. Die Änderungen sind zwar noch nicht offiziell von der IEEE beschlossen, aber die Auswirkungen des absehbaren Technologiesprungs sind so faszinierend, dass die Industrie bereits vor der Verabschiedung des Standards entsprechende WLAN-Geräte auf den Markt bringt. Der aktuelle Stand der Diskussion wird als so genannter „Draft 2.0“ definiert, auf den sich die aktuell im Markt verfügbaren Geräte beziehen.

Hinweis: Wenn in diesem Dokument von „802.11n“ die Rede ist, wird daher immer der aktuelle Draft 2.0 gemeint, es handelt sich nicht um einen verabschiedeten IEEE-Standard.

Einige der Verbesserungen beziehen sich auf den Physical Layer (PHY), der die Übertragung der einzelnen Bits auf dem physikalischen Medium beschreibt – wobei in diesem Fall die Luft das physikalische Medium darstellt. Andere Erweiterungen beziehen sich auf den MAC-Layer (MAC), der u. a. den Zugriff auf das Übertragungsmedium regelt. Beide Bereiche werden im Folgenden separat betrachtet.

Vorteile von 802.11n

Zu den Vorteilen der neuen Technologie gehören unter anderem die folgenden Aspekte:

Höherer effektiver Datendurchsatz

- Der 802.11n Draft 2.0 beinhaltet zahlreiche neue Mechanismen um die verfügbare Bandbreite signifikant zu erhöhen. Bei den aktuellen WLAN-Standards nach 802.11a/g sind physikalische Datenraten (Brutto-Datenraten) von bis zu 54 Mbit/s möglich, netto werden ca. 22 Mbit/s erreicht. Netzwerke nach 802.11n erzielen **derzeit** einen Brutto-Datendurchsatz

von bis zu 300 Mbit/s (netto in der Praxis ca. 120 bis 130 Mbit/s) – prinzipiell definiert der Standard bis zu 600 Mbit/s mit vier Datenströmen. Die maximal realisierbaren Geschwindigkeiten überschreiten zum ersten Mal den Fast-Ethernet-Standard mit 100 Mbit/s in einem kabelgebundenen Netzwerk, was aktuell an den meisten Arbeitsplätzen den Standard darstellt.

Bessere und zuverlässigere Funkabdeckung

- Die neuen Technologien bei 802.11n steigern nicht nur den Datendurchsatz, sondern bringen gleichzeitig Verbesserungen in der Reichweite und reduzieren die Funklöcher bei vorhandenen a/b/g Installationen.

  Das Ergebnis sind bessere Signalabdeckung und höhere Stabilität, die insbesondere für Anwender im professionellen Umfeld eine deutliche Verbesserung bei der Nutzung des drahtlosen Netzwerkes bieten.

Höhere Reichweite

- Mit der Entfernung des Empfängers vom Sender nimmt im Allgemeinen der Datendurchsatz ab. Durch den insgesamt verbesserten Datendurchsatz erzielen WLAN-Netze nach 802.11n auch eine höhere Reichweite, da in einer bestimmten Entfernung vom Access Point ein wesentlich stärkeres Funksignal empfangen wird als in 802.11a/b/g-Netzen.

Kompatibilität mit anderen Standards

Der 802.11n Standard ist rückwärts-kompatibel mit bisherigen Standards (IEEE 802.11a/b/g). Einige Vorteile der neuen Technologie sind jedoch nur verfügbar, wenn neben den APs auch die WLAN-Clients 802.11n-kompatibel sind.

Um die Co-Existenz von WLAN-Clients nach 802.11a/b/g zu ermöglichen (die im Sprachgebrauch von 802.11n als „Legacy-Clients“ bezeichnet werden), bieten die 802.11n-APs besondere Mechanismen für den gemischten Betrieb an, in denen die Performance-Steigerungen gegenüber 802.11a/b/g geringer ausfallen. Nur in reinen 802.11n-Umgebungen wird der „Greenfield-Modus“ verwendet, der alle Vorteile der neuen Technologien ausnutzen kann. Im Greenfield-Modus unterstützen sowohl APs als auch WLAN-Clients den 802.11n-Draft und die APs lehnen Verbindungen von Legacy Clients ab.

Der physikalische Layer

Der physikalische Layer beschreibt, wie die Daten umgewandelt werden müssen, damit sie als Folge von einzelnen Bits über das physikalische Medium übertragen werden können. Bei einem WLAN-Gerät werden dazu die beiden folgenden Schritte vollzogen:

- Modulation der digitalen Daten auf analoge Trägersignale
- Modulation der Trägersignale auf ein Funksignal im gewählten Frequenzband, bei WLAN entweder 2,4 oder 5 GHz.

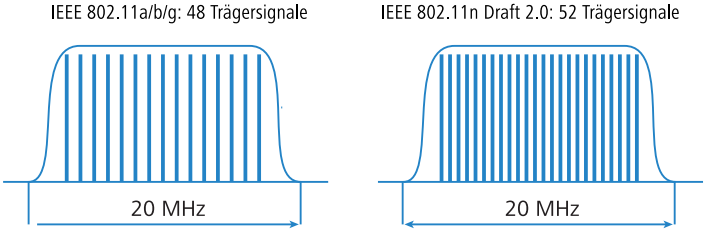
Die zweite der beiden Modulationen läuft bei IEEE 802.11n genau so ab wie bei den bisherigen WLAN-Standards und ist daher keine weitere Betrachtung wert. Für die Modulation der digitalen Daten auf analoge Trägersignale ergeben sich durch 802.11n jedoch zahlreiche Änderungen.

Technische Aspekte von 802.11n

Verbesserte OFDM-Modulation (MIMO-OFDM)

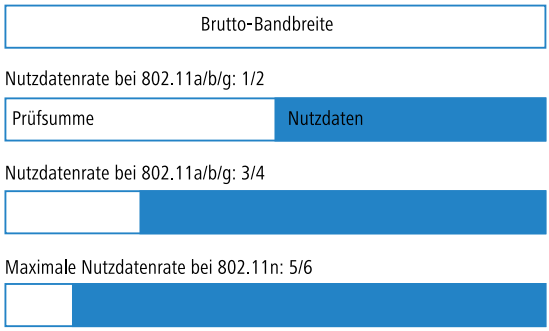
802.11n nutzt wie auch 802.11a/g das OFDM-Verfahren (Orthogonal Frequency Division Multiplex) als Modulationstechnik. Dabei wird das Datensignal nicht nur auf ein einzelnes, sondern parallel auf mehrere Trägersignale moduliert. Der Datendurchsatz, der mit dem OFDM-Verfahren zu erzielen ist, hängt u. a. von folgenden Parametern ab:

- Anzahl der Trägersignale: Während bei 802.11a/g 48 Trägersignale verwendet werden, nutzt 802.11n maximal 52 Trägersignale.



- Nutzdatenrate: Die Übertragung der Daten über die Luft ist grundsätzlich nicht zuverlässig. Schon leichte Störungen im WLAN-System können zu Fehlern in der Datenübertragung führen. Um diese Fehler auszugleichen, werden sogenannte Prüfsummen verwendet, die einen Teil der verfügbaren

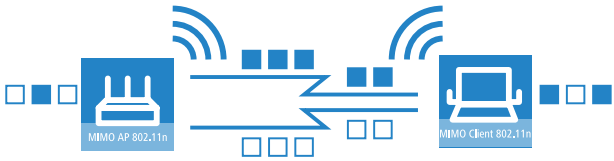
Bandbreite beanspruchen. Die Nutzdatenrate gibt das Verhältnis der theoretisch verfügbaren Bandbreite zu den tatsächlichen Nutzdaten an. 802.11a/g können mit Nutzdatenraten von 1/2 oder 3/4 arbeiten, 802.11n kann bis zu 5/6 der theoretisch verfügbaren Bandbreite für die Nutzdaten verwenden.



Mit diesen beiden Maßnahmen steigt die nutzbare Bandbreite von maximal 54 Mbit/s bei 802.11a/g auf 65 Mbit/s bei 802.11n. Diese Steigerung ist noch nicht spektakulär, sie wird jedoch durch die noch folgenden Maßnahmen weiter verbessert.

Die MIMO-Technologie

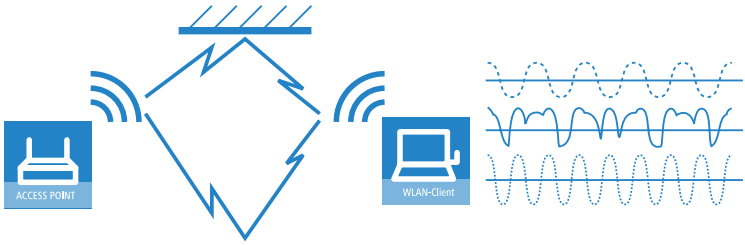
MIMO (Multiple Input Multiple Output) ist die wichtigste neue Technologie in 802.11n. MIMO benutzt mehrere Sender und mehrere Empfänger, um bis zu vier parallele Datenströme auf dem gleichen Übertragungskanal zu übertragen (derzeit werden nur zwei parallele Datenströme realisiert). Das Resultat ist eine Steigerung des Datendurchsatzes und Verbesserung des Funkabdeckung.



Die Daten werden also z. B. beim AP in zwei Gruppen aufgeteilt, die jeweils über separate Antennen, aber gleichzeitig zum WLAN-Client gesendet werden. Mit dem Einsatz von zwei Sende- und Empfangsantennen kann also der Datendurchsatz verdoppelt werden.

Wie aber können auf einem Kanal mehrere Signale gleichzeitig übertragen werden, was bei den bisherigen WLAN-Anwendungen immer für unmöglich gehalten wurde?

Betrachten wir dazu die Datenübertragung in „normalen“ WLAN-Netzen: Die Antenne eines APs sendet Daten je nach Antennentyp in mehrere Richtungen gleichzeitig. Die elektromagnetischen Wellen werden an vielen Flächen in der Umgebung reflektiert, sodass ein ausgesendetes Signal auf vielen unterschiedlichen Wegen die Antennen des WLAN-Clients erreicht – man spricht auch von „Mehrwegeausbreitung“. Jeder dieser Wege ist unterschiedlich lang, sodass die einzelnen Signale mit einer gewissen Zeitverzögerung den Client erreichen.

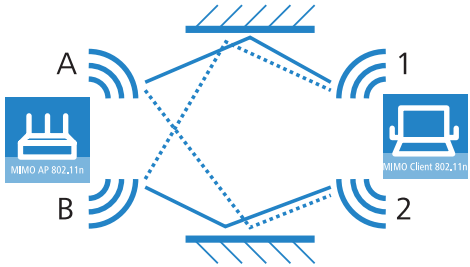


Die zeitverzögerten Signale überlagern sich beim WLAN-Client so, dass aus diesen Interferenzen eine deutliche Verschlechterung des Signals resultiert. Aus diesem Grund werden in den bisherigen WLAN-Netzwerken die direkten Sichtbeziehungen zwischen Sender und Empfänger (englisch: Line of Sight – LOS) angestrebt, um den Einfluss der Reflexionen zu reduzieren.

Die MIMO-Technologie wandelt diese Schwäche der WLAN-Übertragung in einen Vorteil, der eine enorme Steigerung des Datendurchsatzes ermöglicht. Wie schon angemerkt ist es eigentlich unmöglich, zur gleichen Zeit auf dem gleichen Kanal unterschiedliche Signale zu übertragen, da der Empfänger diese Signale nicht auseinanderhalten kann. MIMO nutzt die Reflexionen der

elektromagnetischen Wellen, um mit dem räumlichen Aspekt ein drittes Kriterium zur Identifizierung der Signale zu gewinnen.

Ein von einem Sender A ausgestrahltes und vom Empfänger 1 empfangenes Signal legt einen anderen Weg zurück als ein Signal von Sender B zu Empfänger 2 – beide Signale erfahren auf dem Weg andere Reflexionen und Polarisationsänderungen, haben also einen charakteristischen Weg hinter sich. Zu Beginn der Datenübertragung wird dieser charakteristische Weg in einer Trainingsphase mit normierten Daten aufgezeichnet. In der Folgezeit kann aus den empfangenen Daten zurückgerechnet werden, zu welchem Datenstrom die Signale gehören. Der Empfänger kann also selbst entscheiden, welches der anliegenden Signale verarbeitet wird und vermeidet so die Verluste durch die Interferenzen der ungeeigneten Signale.



MIMO ermöglicht also die gleichzeitige Übertragung mehrerer Signale auf einem geteilten Medium wie der Luft. Die einzelnen Sender und Empfänger müssen dazu jeweils einen räumlichen Mindestabstand einhalten, der allerdings nur wenige Zentimeter beträgt. Dieser Abstand schlägt sich in unterschiedlichen Reflexionen bzw. Signalwegen nieder, die zur Trennung der Signale verwendet werden können.

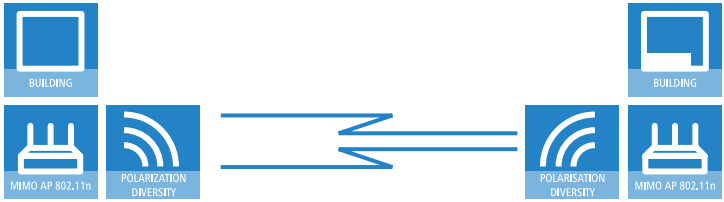
Generell sieht MIMO bis zu vier parallele Datenströme vor, die auch als „Spatial Streams“ bezeichnet werden. In der aktuellen Chipsatz-Generation werden jedoch nur zwei parallele Datenströme realisiert, da die Trennung der Datenströme anhand der charakteristischen Wegeinformationen sehr rechenintensiv ist und daher relativ viel Zeit und Strom benötigt. Gerade Letzteres ist aber besonders bei WLAN-Systemen eher unerwünscht, da oft eine Unabhängigkeit vom Stromnetz auf der Seite der WLAN-Clients bzw. eine PoE-Versorgung der APs angestrebt wird.

Auch wenn das Ziel von vier Spatialströmen derzeit nicht erreicht wird, führt die Verwendung von zwei separaten Datenverbindungen zu einer Verdoppelung des Datendurchsatzes, was einen wirklichen Technologiesprung im Bereich der WLAN-Systeme darstellt. Zusammen mit den Verbesserungen in der OFDM-Modulation steigt der erreichbare Datendurchsatz damit auf maximal 130 Mbit/s.

Mit der Kurzbezeichnung „Sender x Empfänger“ wird die tatsächliche Anzahl der Sender- und Empfänger-Antennen wiedergegeben. Ein 3x3-MIMO beschreibt also drei Sender- und drei Empfänger-Antennen. Die Anzahl der Antennen ist jedoch nicht gleichbedeutend mit der Anzahl der Datenströme: Die verfügbaren Antennen begrenzen nur die maximale Anzahl der Spatial Streams. Der Grund für den Einsatz von mehr Antennen als für die Übertragung der Datenströme eigentlich notwendig sind, liegt in der Zuordnung der Signale über den charakteristischen Weg: Mit einem dritten Signal werden zusätzliche räumliche Informationen übertragen. Sollten sich die Daten aus den beiden ersten Signalen einmal nicht eindeutig zuordnen lassen, kann die Berechnung mithilfe des dritten Signals dennoch gelingen. Die Verwendung von zusätzlichen Antennen trägt also nicht zur Steigerung des Datendurchsatzes bei, resultiert aber in einer gleichmäßigeren und besseren Abdeckung für die Clients.

MIMO im Outdoor-Einsatz

Bei Outdoor-Anwendungen von 802.11n können die natürlichen Reflexionen nicht genutzt werden, da die Signalübertragung üblicherweise auf direktem Weg zwischen den entsprechend ausgerichteten Antennen stattfindet. Um auch hier zwei Datenströme parallel übertragen zu können, werden spezielle Antennen verwendet, die gezielt zwei um 90° gedrehte Polarisationsrichtungen verwenden. Bei diesen sogenannten „Dual-Slant-Antennen“ handelt es sich also eigentlich um zwei Antennen in einem gemeinsamen Gehäuse. Da ein drittes Signal hier keine zusätzliche Sicherheit bringen würde, werden bei Outdoor-Anwendungen üblicherweise genau so viele Antennen (bzw. Polarisationsrichtungen) eingesetzt, wie Datenströme übertragen werden.

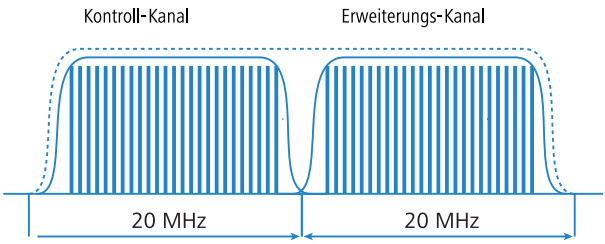


40 MHz-Kanäle

Bei den Ausführungen zur OFDM-Modulation wurde bereits beschrieben, dass der Datendurchsatz mit zunehmender Anzahl von Trägersignalen steigt, weil so mehrere Signale gleichzeitig übertragen werden können. Wenn in einem Kanal mit einer Bandbreite von 20 MHz nicht mehr als 48 (802.11a/g) bzw. 52 (802.11n) Trägersignale genutzt werden können, liegt es nahe, einen zweiten Kanal mit weiteren Trägersignalen zu verwenden.

Bereits in der Vergangenheit wurde diese Technik von einigen Herstellern (u. a. Hirschmann) eingesetzt und als „Turbo-Modus“ bezeichnet, der Datenraten von bis zu 108 Mbit/s ermöglicht. Der Turbo-Modus ist zwar nicht Bestandteil der offiziellen IEEE-Standards, wird aber z. B. auf Point-to-Point-Verbindungen häufig eingesetzt, weil dabei die Kompatibilität zu anderen Herstellern eine eher untergeordnete Rolle spielt.

Der Erfolg hat der zugrunde liegenden Technik aber dazu verholfen, in die Entwicklung von 802.11n einzufließen. Der IEEE 802.11n Draft 2.0 verwendet den zweiten Übertragungskanal allerdings in einer Art und Weise, dass die Kompatibilität zu Geräten nach IEEE 802.11a/g erhalten bleibt. 802.11n überträgt die Daten über zwei direkt benachbarte Kanäle. Einer davon übernimmt die Aufgabe des Kontroll-Kanals, über den u. a. die gesamte Verwaltung der Datenübertragung abgewickelt wird. Durch diese Konzentration der Basisaufgaben auf den Kontroll-Kanal können auch Geräte angebunden werden, die nur Übertragungen mit 20 MHz unterstützen. Der zweite Kanal fungiert als Erweiterungs-Kanal, der nur dann zum Zuge kommt, wenn die Gegenstelle auch 40 MHz-Übertragungen unterstützt. Die Nutzung des zweiten Kanals bleibt dabei optional, Sender und Empfänger können während der Übertragung dynamisch entscheiden, ob einer oder beide Kanäle verwendet werden sollen.

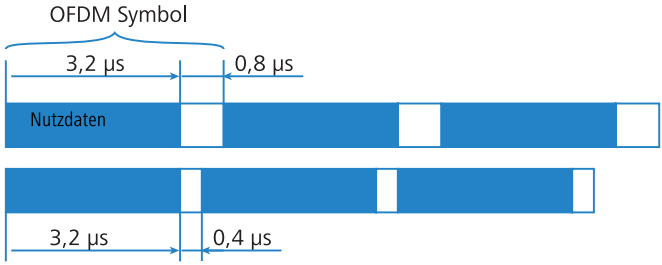


Da die 40 MHz-Implementation im 802.11n-Draft durch die Aufteilung in Kontroll- und Erweiterungskanal etwas effizienter geregelt ist als im bisherigen Turbo-Modus, können statt der doppelten Anzahl sogar noch ein paar zusätzliche Trägersignale gewonnen werden (in Summe 108). So steigt der maximale Datendurchsatz damit bei Nutzung der verbesserten OFDM-Modulation und zwei parallelen Datenströmen auf maximal 270 Mbit/s.

Short Guard Interval

Die letzte Verbesserung des 802.11n-Draft bezieht sich auf die Verbesserung der zeitlichen Abläufe in der Datenübertragung. Ein Signal zur Datenübertragung in einem WLAN-System wird nicht nur zu einem diskreten Zeitpunkt ausgestrahlt, sondern es wird für eine bestimmte Sendezeit konstant „in der Luft gehalten“. Um Störungen auf der Empfangsseite zu verhindern, wird nach dem Ablauf der Sendezeit eine kleine Pause eingelegt, bevor die Übertragung des nächsten Signals beginnt. Die gesamte Dauer aus Sendezeit und Pause wird in der WLAN-Terminologie als „Symbol“ bezeichnet, die Pause selbst ist als „Guard Interval“ bekannt.

Bei IEEE 802.11a/g wird ein Symbol mit einer Länge von 4 µs genutzt: Nach einer Übertragung von 3,2 µs und einer Pause von 0,8 µs wechselt die auf dem Trägersignal übertragene Information. 802.11n reduziert die Pause zwischen den Übertragungen auf das sogenannte „Short Guard Interval“ von nur noch 0,4 µs.



Durch die Übertragung der Datenmenge in kürzeren Intervallen steigt der maximale Datendurchsatz damit bei Nutzung der verbesserten OFDM-Modulation, zwei parallelen Datenströmen und Übertragung mit 40 MHz auf maximal 300 Mbit/s.

Optimierung des Netto-Datendurchsatzes

Die bisher beschriebenen Verfahren haben zum Ziel, den physikalisch möglichen Datendurchsatz zu verbessern. Mit den im Folgenden beschriebenen Verfahren optimieren 802.11n-Netzwerke auch den Durchsatz, der netto zu erzielen ist – also den Durchsatz für die tatsächlichen Nutzdaten.

Frame-Aggregation

Jedes Datenpaket enthält neben den eigentlichen Nutzdaten auch Verwaltungsinformationen, die für den reibungslosen Datenaustausch wichtig sind. Mit der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst. Als Folge davon müssen die Verwaltungsinformationen nur einmal für das gesammelte Paket angegeben werden, der Anteil der Nutzdaten am gesamten Datenvolumen steigt.

Block Acknowledgement

Jedes Datenpaket wird nach dem Empfang sofort bestätigt. Der Sender wird so informiert, dass das Paket richtig übertragen wurde und nicht wiederholt werden muss. Dieses Prinzip gilt auch für die aggregierten Frames bei 802.11n.

Aus einem solchen aggregierten Frame können aber unter Umständen einige Pakete erfolgreich zugestellt werden, andere jedoch nicht. Um nicht unnötig

einen ganzen aggegierten Frame erneut zustellen zu müssen, aus dem vielleicht nur ein Paket **nicht** zugestellt wurde, wird für jedes einzelne WLAN-Paket aus einem aggregierten Frame eine separate Bestätigung erstellt. Diese Bestätigungen werden wieder zu einem Block zusammengefasst und gemeinsam an den Sender zurückgemeldet (Block Acknowledgement). Der Sender erhält eine Information über den Empfangsstatus von jedem einzelnen WLAN-Paket und kann so bei Bedarf auch gezielt nur die nicht erfolgreichen Pakete erneut übertragen.

Der MAC-Layer

Frame-Aggregation

Die Verbesserungen im Physical Layer durch die neuen Technologien mit 802.11n beschreiben zunächst nur den theoretisch möglichen Datendurchsatz des physikalischen Mediums. Der tatsächlich für Nutzdaten verfügbare Teil dieser theoretischen Bandbreite wird jedoch durch zwei Aspekte geschmälert:

- Jedes Datenpaket im WLAN-System enthält neben den eigentlichen Nutzdaten weitere Informationen, z. B. die Präambel und die MAC-Adress-Information.
- Beim tatsächlichen Zugriff auf das Übertragungsmedium gehen durch die Verwaltungsvorgänge Zeit verloren. So muss der Sender vor der Übertragung eines jeden Datenpakets (Frame) mit den anderen vorhandenen Sendern die Zugriffsberechtigung aushandeln; durch Kollisionen von Datenpaketen und andere Vorgänge entstehen weitere Verzögerungen.

Dieser als „Overhead“ bezeichnete Verlust kann reduziert werden, wenn mehrere Datenpakete zu einem größeren Frame zusammengefasst und gemeinsam übertragen werden. Dabei werden Informationen wie die Präambel nur einmal für alle zusammengefassten Datenpakete übertragen und Verzögerungen durch die Zugriffsregelung auf das Übertragungsmedium werden erst in größeren Abständen nötig.

Der Einsatz dieses als Frame-Aggregation bezeichneten Verfahrens unterliegt aber gewissen Einschränkungen:

- Damit auch Informationen wie die MAC-Adressen nur einmal für den aggregierten Frame übertragen werden müssen, können nur solche Datenpakete zusammengefasst werden, die an die gleiche Adresse gerichtet sind.

- Alle Datenpakete, die zu einem größeren Frame aggregiert werden sollen, müssen zum Zeitpunkt der Aggregation beim Sender anliegen – in der Folge müssen einige Datenpakete möglicherweise warten, bis ausreichend andere Pakete für das gleiche Ziel vorhanden sind, mit denen sie aggregiert werden können. Dieser Aspekt stellt für zeitkritische Übertragungen wie Voice over IP möglicherweise eine wichtige Einschränkung dar.

Block Acknowledgement

Jedes Datenpaket, das an einen bestimmten Adressaten gerichtet ist (also keine Broadcast- oder Multicast-Pakete), wird nach dem Empfang sofort bestätigt. Der Sender wird so informiert, dass das Paket richtig übertragen wurde und nicht wiederholt werden muss. Dieses Prinzip gilt auch für die aggregierten Frames bei 802.11n.

Für die Frame-Aggregation werden zwei verschiedene Verfahren eingesetzt, die hier nicht näher erläutert werden, die sich allerdings bei der Bestätigung der aggregierten Frames unterscheiden:

- Bei der Mac Service Data Units Aggregation (MSDUA) werden mehrere Ethernet-Pakete zu einem gemeinsamen WLAN-Paket zusammengefasst. Dieses Paket wird nur einmal als Block bestätigt und gilt somit für alle aggregierten Pakete. Bleibt die Bestätigung aus, wird der gesamte Block erneut zugestellt.
- Bei der Mac Protocol Data Units Aggregation (MPDUA) werden einzelne WLAN-Pakete zu einem gemeinsamen, größeren WLAN-Paket zusammengefasst. Hier wird jedes einzelne WLAN-Paket bestätigt, die Bestätigungen werden wieder zusammengefasst und als Block übertragen. Der Sender erhält hier jedoch anders als bei MSDUA eine Information über den Empfangsstatus von jedem einzelnen WLAN-Paket und kann so bei Bedarf auch gezielt nur die nicht erfolgreichen Pakete erneut übertragen.

Resultierender Datendurchsatz

Der gesamte Datendurchsatz in einem 802.11n-Netzwerk wird von der Nutzung der vorher beschriebenen Techniken bestimmt. Eine eindeutige Kombination aus Modulationsverfahren, Nutzdatenrate und Anzahl der Spatial Streams wird als Modulation Coding Scheme (MCS) bezeichnet. Der Datendurchsatz hängt weiter davon ab, ob das kurze Guard-Intervall und die Kanalbündelung auf 40 MHz genutzt werden.

802.11n verwendet den Begriff „Datendurchsatz“ anstelle von „Datenrate“ bei älteren WLAN-Standards, weil die Datenrate keine ausreichende Beschreibung mehr ist. Die folgende Tabelle zeigt den maximalen Brutto-Datendurchsatz bei Nutzung von kurzem Guard-Intervall mit 40 MHz-Kanälen.

Der Netto-Datendurchsatz – also die Menge an tatsächlich übertragenen IP-Paketen – erreicht für einen 802.11n-Datenstrom bis zu 90 Mbit/s, bei zwei Spatial Streams entsprechend bis zu 180 Mbit/s. Der in der Praxis zu beobachtende Netto-Datendurchsatz liegt Stand Anfang 2008 meist im Bereich zwischen 80 und 130 Mbit/s, was am individuellen Reifegrad der Hardware- und Software-Optimierung sowie an der Chipsatz-Abstimmung zwischen verschiedenen Herstellern liegt.

Datenströme	*Modulation*	*Nutzdatenrate*	*Datendurchsatz (GI=0,4 µs, 40 MHz)*
1	BPSK	1/2	15
1	QPSK	1/2	30
1	QPSK	3/4	45
1	16QAM	1/2	60
1	16QAM	3/4	90
1	64QAM	1/2	120
1	64QAM	3/4	135
1	64QAM	5/6	150
2	BPSK	1/2	30
2	QPSK	1/2	60
2	QPSK	3/4	90
2	16QAM	1/2	120
2	16QAM	3/4	180
2	64QAM	1/2	240
2	64QAM	3/4	270
2	64QAM	5/6	300

12.4.2 IEEE 802.11a: 54 MBit/s

IEEE 802.11a sieht den Betrieb von Funk-LANs im 5 GHz Frequenzband (5,15 GHz bis 5,75 GHz) mit bis zu 54 MBit/s maximaler Übertragungsrate vor. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung,

beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 48 MBit/s, danach auf 36 MBit/s usw. bis auf minimal 6 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 125 m, in Gebäuden typischerweise bis zu 25 m. Der IEEE 802.11a Standard verwendet OFDM (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) als Modulationsverfahren.

Bei OFDM handelt es sich um ein Modulationsverfahren, das mehrere unabhängige Trägerfrequenzen für die Übertragung des Datensignals verwendet und diese Trägerfrequenzen mit einer verringerten Übertragungsrate moduliert. Das OFDM Modulationsverfahren ist dabei insbesondere sehr unempfindlich gegen Echos und andere Beeinträchtigungen und ermöglicht hohe Übertragungsraten.

Im 'Turbo-Modus' können Hirschmann WLAN-Geräte zwei Funkkanäle gleichzeitig nutzen und damit die Übertragungsrate auf maximal 108 MBit/s steigern. Der Turbo-Modus kann in Verbindung mit dem IEEE 802.11a-Standard genutzt werden zwischen Hirschmann Basis-Stationen. Diese Steigerung der Übertragungsrate muss in der Basisstation entsprechend eingeschaltet werden und kann zu einer Reduzierung der Sendeleistung und damit der Reichweite der Funkverbindung führen.

12.4.3 IEEE 802.11h – ETSI 301 893

Im November 2002 wurde das 5 GHz-Band in Deutschland für die private Nutzung freigegeben und machte den Weg frei für deutlich schnellere WLAN-Verbindungen nach dem schon länger verfügbaren IEEE 802.11a-Standard. Der breitere Einsatz von 5 GHz-WLANs wurde dabei jedoch durch den ausschließlichen Einsatz in geschlossenen Räumen und die Übertragung mit relativ geringen Sendeleistungen beschränkt.

Mit der Erweiterung 802.11h wurde im September 2003 die private Nutzung des 5 GHz-Bandes schließlich auch außerhalb geschlossener Räume ermöglicht. Dabei wurden zum Schutz der militärischen Anwendungen im 5 GHz-Band die Verfahren DFS (Dynamic Frequency Selection) und TPC (Transmission Power Control) vorgeschrieben. Allerdings können bei Nutzung von DFS und TPC mit maximal 1000 mW deutliche höhere Sendeleistungen als in allen anderen bis dahin gültigen Standards erzielen.

ETSI-Standards

Die ETSI verabschiedete schon 1996 den ersten Standard zur Regelung von Datenfernübertragungen unter dem Namen Hiperlan (High Performance Radio Local Area Networks). Die erste Fassung (Hiperlan Typ1) war für den Einsatz im Frequenzbereich von 5,15 bis 5,30 GHz mit einer Übertragungsrate von 20 MBit/s vorgesehen. Da sich in der Industrie keine Hersteller für Produkte nach diesem Standard fanden, blieb Hiperlan zunächst ohne praktische Bedeutung.

Mit der im Jahre 2000 vorgestellten neuen Fassung des Hiperlan Typ 2 stellt die ETSI eine WLAN-Lösung vor, die wie IEEE 802.11a im 5 GHz-Band arbeitet und eine Bruttodatenrate von ebenfalls 54 MBit/s anbietet. Die Überlagerung der verwendeten Frequenzen und das ebenfalls wie bei 802.11a verwendete OFDM-Modulationsverfahren machen jedoch eine Anpassung der Standards zwischen IEEE und ETSI notwendig, um Störungen der Systeme untereinander zu vermeiden.

Europäische Harmonisierung

Um die Nutzung des 5GHz-Bandes in Europa zu vereinheitlichen, hat die Europäische Kommission am 11.07.2005 den Standard ETSI 301 893 erlassen. Die Mitgliedsländer der EU waren verpflichtet, diese bis zum 31.10.2005 umzusetzen.

Anstelle der in den 802.11a/h-Standards beschriebenen drei Unterbändern (5150 - 5350 MHz, 5470 - 5725 MHz und 5725 - 5875 MHz für UK) regelt die Norm ETSI 301 893 die drei folgenden Bereiche mit unterschiedlichen Vorschriften:

- 5150 - 5250 MHz (Unterband 1)
- 5250 - 5350 MHz (Unterband 1)
- 5470 - 5725 MHz (Unterband 2)

Der Kern der Richtlinie sind Vorkehrungen zur Vermeidung von Störungen mit anderen Systemen, die das gleiche Frequenzband verwenden. Hierunter fallen z. B. Radaranlagen, die als „Primäranwendungen“ gelten. Die „Sekundäranwendungen“ wie WLAN müssen die Frequenz wechseln, sobald ein Konflikt festgestellt wird.

- Dynamic Frequency Selection – DFS

Zur Priorisierung der Primäranwendungen wird das Verfahren der dynamischen Frequenzwahl (DFS) vorgeschrieben. DFS geht zunächst davon aus, dass kein Kanal im entsprechenden Frequenzband verfügbar ist. Das WLAN-Gerät wählt beim Start zufällig einen Kanal aus und führt einen sogenannten Channel availability Check (CAC) durch. Dabei wird **vor** dem Senden auf einem Kanal für 60 Sekunden (Channel Observation Time, COT) geprüft, ob ein anderes Gerät auf diesem Kanal bereits arbeitet und der Kanal somit belegt ist. Ist das der Fall, so wird ein weiterer Kanal mit CAC geprüft. Andernfalls kann das WLAN-Gerät den Sendebetrieb aufnehmen.

Auch während des Betriebes wird überprüft, ob eine Primäranwendung wie z. B. ein Radargerät diesen Kanal benutzt. Dabei wird ausgenutzt, dass Radare häufig nach dem Rotationsverfahren arbeiten, bei dem ein eng gebündelter Richtfunkstrahl durch eine rotierende Antenne ausgestrahlt wird. Durch die Rotation der Antenne nimmt ein entfernter Empfänger das Radar-Signal als einen kurzen Impuls (Radar-Peak) wahr. Empfängt ein Gerät einen solchen Radar-Peak, so stellt es zunächst den Sendebetrieb ein und überwacht den Kanal auf weitere Impulse. Treten während der COT weitere Radar Peaks auf, wird automatisch ein neuer Kanal gewählt.

Vorgeschrieben ist, dass eine solche Überprüfung alle 24 Stunden stattfinden muss. Daher ist eine Unterbrechung der Datenübertragung für 60 Sekunden unvermeidlich.

DFS ist für die Frequenzbereiche von 5250 - 5350 MHz und von 5470 - 5725 MHz fest vorgeschrieben. Für den Frequenzbereich von 5150 - 5250 MHz ist es optional einsetzbar.

- Transmission Power Control – TPC

  Für eine Verminderung der funktechnischen Störungen soll eine dynamische Anpassung der Sendeleistung sorgen.

  Die dynamische Anpassung der Sendeleistung erleichtert die gemeinsame Nutzung der Frequenzbänder 5250-5350 MHz und 5470 - 5725 MHz mit Sattelitendiensten. TPC soll eine durchschnittliche Abschwächung der Sendeleistung gegenüber der max. zulässigen Sendeleistung von mindestens drei dB bewirken. Dazu ermittelt TPC die minimal notwendige Sendeleistung, um die Verbindung zum Partner (z. B. einem AP) aufrecht zu erhalten. Verzichtet man innerhalb dieser Frequenzbänder auf TPC, so verringert sich die höchstzulässige mittlere EIRP und die entsprechende

maximale geforderter TPC-Regelbereich um 3 dB. Im Frequenzbereich von 5150-5250 MHz gilt diese Einschränkung nicht.

Im Betrieb ohne DFS und TPC sind nur maximal 30 mW EIRP erlaubt. Unter Verwendung von DFS und TPC sind maximal 200 mW (bei 5150 bis 5350 MHz) bzw. 1000 mW EIRP bei (5470 bis 5725 MHz) als Sendeleistung erlaubt (zum Vergleich: 100 mW bei 802.11 b/g, 2,4 GHz, DFS und TPC sind hier nicht nötig). Die höhere maximale Sendeleistung gleicht nicht nur die höhere Dämpfung der Luft für die 5 GHz-Funkwellen aus, sondern ermöglicht sogar deutlich größere Reichweiten als im 2,4 GHz-Bereich möglich sind.

Unterschiede zu USA und Asien

In den USA und in Asien werden vom europäischen Standard abweichende Frequenzbänder und maximale Signalstärken verwendet.

In den USA werden für Funknetze im 5 GHz-Band drei je 100 MHz breite Unterbänder verwendet. Das "Lower Band" (UNII-1) reicht von 5150–5250 MHz, das "Middle Band" (UNII-2) von 5250–5350 MHz, das "extended Middle Band" (UNII-2e) von 5470–5725 MHz und das "Upper Band" (UNII-3) von 5725–5825 MHz. Im Lower Band ist eine maximale mittlere EIRP von 50 mW, im Middle Band von 250 mW sowie im Upper Band von 1 W zugelassen.

In Japan ist die Nutzung des 5 GHz-Bandes bisher nur sehr eingeschränkt möglich: hier ist nur das untere Band von 5150–5250 MHz für die private Nutzung freigegeben.

Zulässige Funkkanäle

Im nutzbaren Frequenzraum von 5,13 bis 5,805 GHz stehen bis zu 16 Kanäle in Europa zur Verfügung, unterteilt in Frequenzbereiche, für die unterschiedliche Nutzungsbedingungen gelten können:

- 5150 - 5250 MHz (Kanäle 36, 40, 44 und 48)
- 5250 - 5350 MHz (Kanäle 52, 56, 60 und 64)
- 5470 - 5725 MHz (Kanäle 100, 104, 108, 112, 116, 132, 136 und 140)
- 5725 - 5875 MHz (Kanäle 147, 151, 155, 167)

In der folgenden Übersicht sehen Sie, welche Kanäle in den verschiedenen Regionen verwendet werden dürfen.

Kanal	Frequenz	***Unterband***	ETSI (EU)	FCC (US)	Japan
36	5,180 GHz	1	ja	ja	ja
40	5,200 GHz	1	ja	ja	ja
44	5,220 GHz	1	ja	ja	ja
48	5,240 GHz	1	ja	ja	ja
52	5,260 GHz*	1	ja	ja	nein
56	5,280 GHz*	1	ja	ja	nein
60	5,300 GHz*	1	ja	ja	nein
64	5,320 GHz*	1	ja	ja	nein
100	5,500 GHz*	2	ja	nein	nein
104	5,520 GHz*	2	ja	nein	nein
108	5,540 GHz*	2	ja	nein	nein
112	5,560 GHz*	2	ja	nein	nein
116	5,580 GHz*	2	ja	nein	nein
132	5,660 GHz*	2	ja	nein	nein
136	5,680 GHz*	2	ja	nein	nein
140	5,700 GHz*	2	ja	nein	nein
147	5,735 GHz*	3	nein	ja	nein
151	5,755 GHz*	3	nein	ja	nein
155	5,775 GHz*	3	nein	ja	nein
167	5,835 GHz*	3	nein	ja	nein

*In diesem Frequenzbereich ist der Einsatz von DFS erforderlich (Kanäle 5–167).

Frequenzbereiche für Indoor- und Outdoor-Verwendung

Der Einsatz der in der ETSI 301 893 beschriebenen Verfahren zur Reduzierung der gegenseitigen Störungen im 5 GHz-Band (TPC und DFS) sind nicht für alle Einsatzbereiche vorgeschrieben. Die folgende Tabelle gibt Aufschluss über die zulässige Verwendung und die zugehörigen Sendeleistungen innerhalb der EU:

Frequenz (GHz)	*Sendeleistung (mW/dBm)*	*Verwendung*	*DFS*	*TPC*
5,15-5,25	30/13	Indoor		
5,15-5,25	60/14	Indoor		4
5,15-5,25	200/23	Indoor	4	4
5,25-5,35	200/23	Indoor	4	4
5,470-5,725	1000/30	Indoor/Outdoor	4	4

Hinweis: Beim Einsatz in anderen Ländern können ggf. andere Vorschriften gelten. Bitte informieren Sie sich über die aktuellen Funk-Regelungen des Landes, in dem Sie ein Funk-LAN-Gerät in Betrieb nehmen wollen, und stellen Sie in den WLAN-Einstellungen unbedingt das Land ein, in dem Sie das Gerät betreiben.

12.4.4 IEEE 802.11g: 54 MBit/s

Der IEEE 802.11g Standard arbeitet ebenfalls mit bis zu 54 MBit/s Übertragungsrate im 2,4 GHz ISM-Frequenzband. Im Gegensatz zu IEEE 802.11b wird jedoch bei IEEE 802.11g die OFDM Modulation verwendet wie schon bei IEEE 802.11a. IEEE 802.11g enthält einen besonderen Kompatibilitätsmodus der eine Abwärtskompatibilität zu dem weit verbreiteten IEEE 802.11b Standard gewährleistet. Wird dieser Kompatibilitätsmodus verwendet, so ist jedoch mit Geschwindigkeitseinbußen bei der Datenübertragung zu rechnen. IEEE 802.11g ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a. Die Reichweiten von IEEE 802.11g Produkten sind vergleichbar mit denen von IEEE 802.11b Produkten.

Auch im 802.11g-Standard kann mit dem 'Turbo-Modus' durch die parallele Nutzung von zwei Funkkanälen die Übertragungsrate auf maximal 108 MBit/s gesteigert werden. Da im 2,4 GHz-Band jedoch weniger Kanäle als im 5 GHz-Band genutzt werden können, schränkt die Verwendung des Turbo-Modus hier die Kanalwahl deutlich ein.

12.4.5 IEEE 802.11b: 11 MBit/s

IEEE 802.11b sieht den Betrieb von lokalen Funk-LANs im ISM-Frequenzband vor (**I**ndustrial, **S**cientific, **M**edical: 2.4 bis 2.483 GHz). Die maximale Bandbreite der Datenübertragung beträgt bis zu 11 MBit/s. Der tatsächliche Durchsatz ist allerdings abhängig von der Entfernung, beziehungsweise von der Qualität der Verbindung. Bei zunehmender Entfernung und abnehmender Verbindungsqualität sinkt die Übertragungsgeschwindigkeit auf 5,5 MBit/s, danach auf 2 und schließlich auf 1 MBit/s. Die Reichweite der Übertragung beträgt im Freien bis zu 150 m, in Gebäuden typischerweise bis zu 30 m. IEEE 802.11b ist wegen der unterschiedlichen Frequenzbänder nicht kompatibel zu IEEE 802.11a.

Zur Abschirmung gegen Störungen durch andere Sender, die gegebenenfalls das gleiche Frequenzband verwenden, wird im 2,4 GHz Frequenzband für IEEE 802.11b das DSSS-Verfahren verwendet (**D**irect **S**equence **S**pread **S**pectrum). Normalerweise benutzt ein Sender nur einen sehr schmalen Bereich des verfügbaren Frequenzbandes zur Übertragung. Wird genau dieser Bereich auch von einem weiteren Sender verwendet, kommt es zu Störungen in der Übertragung. Beim DSSS-Verfahren nutzt der Sender einen breiteren Teil des möglichen Frequenzbandes und wird so unempfindlicher gegen schmalbandige Störungen.

12.4.6 Maximaler EIRP-Wert abhängig vom Übertragungsstandard

Um die Sendeleistungsdichte im 802.11b-Übertragungsstandard nicht zu überschreiten, ist ein EIRP-Wert von maximal 18dBm möglich. Im Übertragungsstandard 802.11gn kann der EIRP-Wert maximal 20dBm betragen. Ab HiLCOS-Version 8.84 richtet sich der maximale EIRP-Wert eines WLAN-fähigen Hirschmann-Gerätes automatisch nach dem verwendeten Übertragungsstandard.

12.5 WLAN-Sicherheit

12.5.1 Grundbegriffe

Auch wenn immer wieder in Zusammenhang mit Computernetzen pauschal von 'Sicherheit' gesprochen wird, so ist es doch für die folgenden Ausführungen wichtig, die dabei gestellten Forderungen etwas näher zu differenzieren.

Authentifizierung

Als ersten Punkt der Sicherheit betrachten wir den Zugangsschutz:

- Dabei handelt es sich zum einen um einen Schutzmechanismus, der nur autorisierten Nutzern den Zugang zum Netzwerk gewährt.
- Zum anderen soll aber auch sichergestellt werden, dass der Client sich mit genau dem gewünschten AP verbindet, und nicht mit einem von unbefugten Dritten eingeschmuggelten AP mit dem gleichen Netzwerk-Namen. So eine Authentifizierung kann z. B. durch Zertifikate oder Passwörter gewährleistet werden.

Authentizität

Authentizität: Nachweis der Urheberschaft von Daten und der Echtheit des Datenmaterials; die Durchführung eines solchen Nachweises bezeichnet man als Authentifizierung

Integrität

Ist der Zugang einmal gewährt, so möchte man sicherstellen, dass Datenpakete den Empfänger unverfälscht erreichen, d. h. dass niemand die Pakete verändert oder andere Daten in den Kommunikationsweg einschleusen kann. Die Manipulation der Datenpakete selbst kann man nicht verhindern; aber man kann durch geeignete Prüfsummenverfahren veränderte Pakete identifizieren und verwerfen.

Vertraulichkeit

Vom Zugangsschutz getrennt zu sehen ist die Vertraulichkeit, d. h. unbefugte Dritte dürfen nicht in der Lage sein, den Datenverkehr mitzulesen. Dazu werden die Daten verschlüsselt. Solche Verschlüsselungsverfahren sind z. B. DES, AES, RC4 oder Blowfish. Zur Verschlüsselung gehört natürlich auf der Empfängerseite eine entsprechende Entschlüsselung, üblicherweise mit dem gleichen Schlüssel (so genannte symmetrische Verschlüsselungsverfahren). Dabei ergibt sich natürlich das Problem, wie der Sender dem Empfänger den verwendeten Schlüssel erstmalig mitteilt – eine einfache Übertragung könnte von einem Dritten sehr einfach mitgelesen werden, der damit den Datenverkehr leicht entschlüsseln könnte.

Im einfachsten Fall überlässt man dieses Problem dem Anwender, d.h. man setzt die Möglichkeit voraus, dass er die Schlüssel auf beiden Seiten der Verbindung bekannt machen kann. In diesem Fall spricht man von Pre-Shared-Keys oder kurz 'PSK'.

Ausgefeiltere Verfahren kommen dann zum Einsatz, wenn der Einsatz von Pre-Shared-Keys nicht praktikabel ist, z. B. in einer über SSL aufgebauten HTTP-Verbindung – hierbei kann der Anwender nicht so einfach an den Schlüssel von einem entfernten Web-Server gelangen. In diesem Falle werden so genannte asymmetrische Verschlüsselungsverfahren wie z. B. RSA eingesetzt, d.h. zum **Ent**schlüsseln der Daten wird ein anderer Schlüssel als zum **Ver**schlüsseln benutzt, es kommen also Schlüsselpaare zum Einsatz. Solche Verfahren sind jedoch viel langsamer als symmetrische Verschlüsselungsverfahren, was zu einer zweistufigen Lösung führt:

- Der Sender verfügt über ein asymmetrisches Schlüsselpaar. Den öffentlichen Teil dieses Schlüsselpaares, also den Schlüssel zum **Ver**schlüsseln, überträgt er an den Empfänger, z. B. in Form eines Zertifikats. Da dieser Teil des Schlüsselpaares nicht zum **Ent**schlüsseln genutzt werden kann, gibt es hier keine Bedenken bzgl. der Sicherheit.
- Der Empfänger wählt einen beliebigen symmetrischen Schlüssel aus. Dieser symmetrische Schlüssel, der sowohl zum **Ver**- als auch zum **Ent**schlüsseln dient, muss nun gesichert zum Sender übertragen werden. Dazu wird er mit dem öffentlichen Schlüssel des Senders verschlüsselt und an den Sender zurückgeschickt. Der symmetrische Schlüssel kann nun ausschließlich mit dem privaten Schlüssel des Senders wieder entschlüsselt werden. Ein potenzieller Mithörer des Schlüsselaustauschs kann

diese Information aber nicht entschlüsseln, die Übertragung des symmetrischen Schlüssels ist also gesichert.

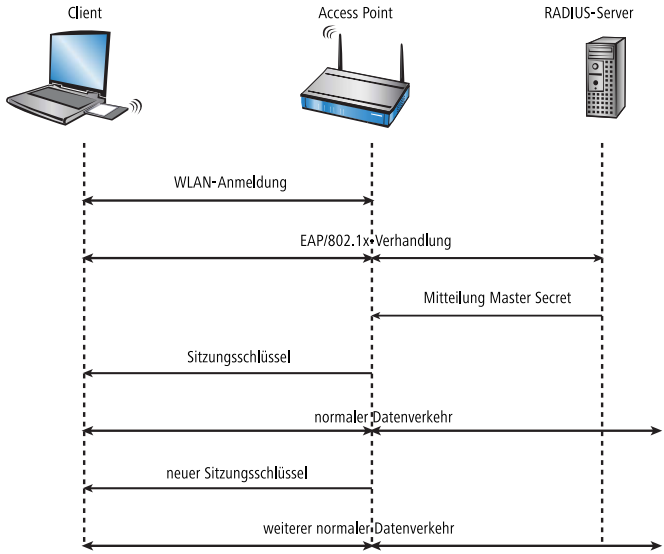
12.5.2 IEEE 802.11i / WPA2

Mitte 2004 wurde der Standard 802.11i vom IEEE verabschiedet, der auch als Wi-Fi Protected Access 2 (WPA2) bekannt ist. WPA2 stellt den derzeit höchsten Sicherheitsstandard für WLANs dar, da es zum einem die Authentifizierung und Autorisierung der Benutzer über IEEE 802.1X erlaubt und zum anderen eine Unterstützung des Verschlüsselungsverfahrens AES, das eine weitaus höhere Sicherheit bietet als die in WEP oder WPA verwendeten Verfahren. Die folgenden Abschnitte stellen einige der relevanten technischen Aspekte vor.

EAP und IEEE 802.1x

Eine deutliche Steigerung in der Absicherung von WLANs kann erzielt werden, wenn für eine Verbindung keine festen Schlüssel definiert werden sondern diese Schlüssel dynamisch ausgehandelt werden. Als dabei anzuwendendes Verfahren hat sich dabei das Extensible Authentication Protocol durchgesetzt. Wie der Name schon nahelegt, ist der ursprüngliche Zweck von EAP die Authentifizierung, d.h. der geregelte Zugang zu einem WLAN – die Möglichkeit, einen für die folgende Sitzung gültigen Schlüssel zu installieren, fällt dabei sozusagen als Zusatznutzen ab. Die folgende Abbildung zeigt den grundsätzlichen Ablauf einer mittels EAP geschützten Sitzung.

Hinweis: Der Einsatz von EAP / 802.1X ist grundsätzlich auch bei WEP möglich. In der Regel wird dieses Verfahren jedoch bei WLANs nach WPA2 eingesetzt.



In der ersten Phase meldet sich der Client wie gewohnt beim AP an und erreicht einen Zustand, in dem er bei früher verwendeten WEP jetzt über den AP Daten senden und empfangen könnte – nicht so jedoch bei EAP, denn in diesem Zustand verfügt der Client ja noch über keinerlei Schlüssel, mit denen man den Datenverkehr vor Abhören schützen könnte. Stattdessen steht der Client aus Sicht des APs in einem 'Zwischenzustand', in dem er nur bestimmte Pakete vom Client weiter leitet, und diese auch nur gerichtet an einen Authentifizierungs-Server. Bei diesen Paketen handelt es sich um das bereits erwähnte EAP/802.1x. Der AP packt diese Pakete in RADIUS-Anfragen um und reicht sie an den Authentifizierungs-Server weiter. Umgekehrt wandelt der AP darauf vom RADIUS-Server kommende Antworten wieder in EAP-Pakete um und reicht sie an den Client weiter.

Der AP dient dabei sozusagen als 'Mittelsmann' zwischen Client und Server: er muss den Inhalt dieser Pakete nicht prüfen, er stellt lediglich sicher, dass kein anderer Datenverkehr von oder zu dem Client erfolgen kann. Über den so gebildeten „Tunnel“ durch den AP versichern sich Client und Server nun ihrer gegenseitigen Authentizität, d.h. der Server überprüft die Zugangsberechtigung des Clients zum Netz, und der Client überprüft, ob er wirklich mit dem

richtigen Netz verbunden ist. Von Hackern aufgestellte „wilde“ APs lassen sich so erkennen.

Es gibt eine ganze Reihe von Authentifizierungsverfahren, die in diesem Tunnel angewendet werden können. Ein gängiges (und seit Windows XP unterstütztes) Verfahren ist z. B. TLS, bei dem Server und Client Zertifikate austauschen, ein anderes ist TTLS, bei dem nur der Server ein Zertifikat liefert – der Client authentifiziert sich über einen Benutzernamen und ein Passwort.

Nachdem die Authentifizierungsphase abgeschlossen ist, ist gleichzeitig auch ein ohne Verschlüsselung gesicherter Tunnel entstanden, in den im nächsten Schritt der AP eingebunden wird. Dazu schickt der RADIUS-Server das sogenannte 'Master Secret', einen während der Verhandlung berechneten Sitzungsschlüssel, zum AP. Das LAN hinter dem AP wird in diesem Szenario als sicher betrachtet, von daher kann diese Übertragung im Klartext erfolgen.

Mit diesem Sitzungsschlüssel übernimmt der AP jetzt den gebildeten Tunnel und kann ihn nutzen, um dem Client die eigentlichen Schlüssel mitzuteilen. Je nach Fähigkeiten der Access-Point-Hardware kann das ein echter Sitzungsschlüssel sein, d.h. ein Schlüssel, der nur für Datenpakete zwischen dem AP und genau diesem Client benutzt wird. Ältere WEP-Hardware verwendet meistens nur Gruppenschlüssel, den der AP für die Kommunikation mit mehreren Clients benutzt.

Der besondere Vorteil dieses Verfahrens ist es, dass der AP über den EAP-Tunnel die Schlüssel regelmäßig wechsel kann, d.h. ein sogenanntes Rekeying durchführen kann. Auf diese Weise lassen sich Schlüssel gegen andere ersetzen, lange bevor sie durch IV-Kollisionen Gefahr laufen, geknackt zu werden. Eine gängige 'Nutzungszeit' für so einen Schlüssel sind z. B. 5 Minuten.

Status-Zähler für IEEE 802.1X-Anmeldevorgänge

Eine Übersichtstabelle mit der Anzahl akzeptierter und zurückgewiesener Verbindungsanfragen je logischer Schnittstelle finden Sie im LCOS-Menübaum unter **Status** > **IEEE802.1x** > **Ports**.

Zusätzlich zeigt Ihnen die Übersicht an, wie oft bei einer Schnittstelle das Authorisierungslimit erreicht wurde.

Ports

Port	Anzahl-Accept	Anzahl-Reject	Anzahl-ReauthMax-erreicht
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

WPA mit Passphrase

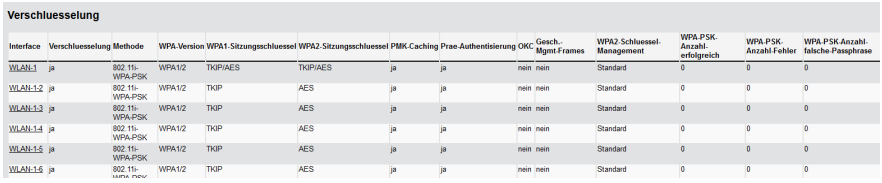
Der bei EAP/802.1x beschriebene Handshake läuft bei WPA grundsätzlich ab, d.h. der Anwender wird niemals selber irgendwelche Schlüssel definieren müssen. In Umgebungen, in denen kein RADIUS-Server zur Erteilung des Master-Secrets vorhanden ist (z. B. bei kleineren Firmen) sieht WPA deshalb neben der Authentifizierung über einen RADIUS-Server noch das PSK-Verfahren vor; dabei muss der Anwender sowohl auf dem AP als auch auf allen Stationen eine zwischen 8 und 63 Zeichen lange Passphrase eingeben, aus der zusammen mit der verwendeten SSID das Master-Secret über ein Hash-Verfahren berechnet wird. Das Master Secret ist in so einem PSK-Netz also konstant, trotzdem ergeben sich immer unterschiedliche Sitzungs-Schlüssel.

In einem PSK-Netz hängen sowohl Zugangsschutz als auch Vertraulichkeit davon ab, dass die Passphrase nicht in unbefugte Hände gerät. Solange dies aber gegeben ist, bietet WPA-PSK eine deutlich höhere Sicherheit gegen Einbrüche und Abhören als jede WEP-Variante. Für größere Installationen, in denen eine solche Passphrase einem zu großen Nutzerkreis bekannt gemacht werden müsste, als dass sie geheimzuhalten wäre, wird EAP/802.1x in Zusammenhang mit dem hier beschriebenen Key-Handshake genutzt.

Status-Zähler für WPA-PSK-Anmeldevorgänge

Eine Übersicht über die Anzahl fehlgeschlagener WPA-PSK Anmeldevorgänge finden Sie im LCOS-Menübaum unter **Status** > **WLAN** > **Verschlüsselung**.

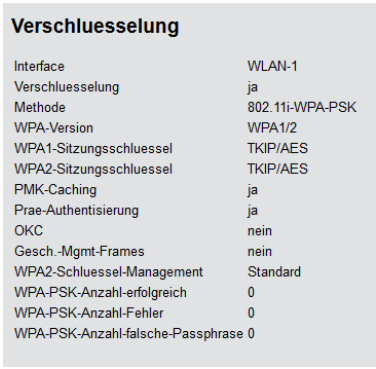
Zusätzlich erhalten Sie eine Übersicht über erfolgreiche Anmeldeversuche sowie die Anzahl zurückgewiesener Anmeldungen aufgrund falscher Passphrasen.



Verschluesselung

Interface	Verschluesselung	Methode	WPA-Version	WPA1-Sitzungsschluessel	WPA2-Sitzungsschluessel	PMK-Caching	Prae-Authentisierung	OKC	Gesch.-Mgmt-Frames	WPA2-Schluessel-Management	WPA-PSK-Anzahl-erfolgreich	WPA-PSK-Anzahl-Fehler	WPA-PSK-Anzahl-falsche-Passphrase
WLAN-1	ja	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1:2	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1:3	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1:4	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1:5	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0
WLAN-1:6	ja	802.11i-WPA-PSK	WPA1/2	TKIP	AES	ja	ja	nein	nein	Standard	0	0	0

Wählen Sie in der Tabelle eine Schnittstelle aus (z. B. WLAN-1), um sich Informationen für die gewählte Schnittstelle anzeigen zu lassen.



Verschluesselung

Interface	WLAN-1
Verschluesselung	ja
Methode	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Sitzungsschluessel	TKIP/AES
WPA2-Sitzungsschluessel	TKIP/AES
PMK-Caching	ja
Prae-Authentisierung	ja
OKC	nein
Gesch.-Mgmt-Frames	nein
WPA2-Schluessel-Management	Standard
WPA-PSK-Anzahl-erfolgreich	0
WPA-PSK-Anzahl-Fehler	0
WPA-PSK-Anzahl-falsche-Passphrase	0

TKIP

TKIP steht für Temporal **K**ey **I**ntegrity **P**rotocol. Wie der Name nahelegt, handelt es sich dabei um eine Zwischenlösung, die nur übergangsweise bis zur Einführung eines wirklich starken Verschlüsselungsverfahrens genutzt werden soll, aber trotzdem einige Probleme des bis dahin verwendeten WEP löst. Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg für AES bieten.

Hinweis: Wenn eine SSID ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Standard-Verschlüsselung mit WPA2

Unkonfigurierte APs können im Auslieferungszustand nicht über die WLAN-Schnittstelle in Betrieb genommen werden. Die WLAN-Module sind ausgeschaltet, die Geräte suchen selbstständig im LAN einen WLC, von dem sie automatisch eine Konfiguration beziehen können.

Der Preshared Key für die Standard-WPA-Verschlüsselung setzt sich aus dem Anfangsbuchstaben „L“ gefolgt von der LAN-MAC-Adresse des Access Points in ASCII-Schreibweise zusammen. Die LAN-MAC-Adressen der Hirschmann-Geräte beginnen immer mit der Zeichenfolge „00A057“. Sie finden die LAN-MAC-Adresse auf einem Aufkleber auf der Unterseite des Gerätes. Verwenden Sie **nur** die als „LAN MAC address“ gekennzeichnete Nummer, die mit „00A057“ beginnt. Bei den anderen ggf. angegebenen Nummern handelt es sich **nicht** um die LAN-MAC-Adresse!

Für ein Gerät mit der LAN-MAC-Adresse „00A05713B178“ lautet der Preshared Key also „L00A05713B178“. Dieser Schlüssel ist in den 'WPA-/Einzel-WEP-Einstellungen' des Gerätes für jedes logische WLAN-Netzwerk als 'Schlüssel 1/Passphrase' eingetragen.

Hinweis: Ändern Sie den Preshared Key für WPA nach der ersten Anmeldung, um eine sichere Verbindung zu gewährleisten.

AES

Die augenfälligste Erweiterung betrifft die Einführung eines neuen Verschlüsselungsverfahrens, nämlich AES-CCM. Wie der Name schon andeutet, basiert dieses Verschlüsselungsverfahren auf dem DES-Nachfolger AES, im Gegensatz zu WEP und TKIP, die beide auf RC4 basieren. Da ältere WLAN-Clients zum Teil nur TKIP unterstützen, definiert 802.11i auch weiterhin TKIP, allerdings mit umgekehrtem Vorzeichen: eine 802.11i-standardkonforme

Hardware muss AES unterstützen, während TKIP optional ist – bei WPA war es genau umgekehrt, hier ist die Verwendung von AES optional.

Der Zusatz CCM bezieht sich auf die Art und Weise, wie AES auf WLAN-Pakete angewendet wird. Das Verfahren ist insgesamt recht kompliziert, weshalb CCM sinnvoll eigentlich nur in Hardware implementiert werden wird – software-basierte Implementationen sind zwar möglich, führen aber auf den üblicherweise in Access Points eingesetzten Prozessoren zu erheblichen Geschwindigkeitseinbußen.

Im Gegensatz zu TKIP benötigt AES nur noch einen 128 Bit langen Schlüssel, mit dem sowohl die Verschlüsselung als auch der Schutz gegen unerkanntes Verändern von Paketen erreicht wird. Des weiteren ist CCM voll symmetrisch, d.h. es wird der gleiche Schlüssel in beide Kommunikationsrichtungen angewendet – eine standardkonforme TKIP-Implementierung hingegen verlangt die Verwendung unterschiedlicher Michael-Schlüssel in Sende- und Empfangsrichtung, so dass CCM in seiner Anwendung deutlich unkomplizierter ist als TKIP.

Ähnlich wie TKIP verwendet CCM einen 48 Bit langen Initial Vector in jedem Paket – eine IV-Wiederholung ist damit in der Praxis ausgeschlossen. Wie bei TKIP merkt der Empfänger sich den zuletzt benutzten IV und verwirft Pakete mit einem IV, der gleich oder niedriger als der Vergleichswert ist.

Prä-Authentifizierung und PMK-Caching

802.11i soll den Einsatz von WLAN auch für Sprachverbindungen (VoIP) in Unternehmensnetzen erlauben. Vor allem in Zusammenhang mit WLAN-basierten schnurlosen Telefonen kommt einem schnellen Roaming, d.h. dem Wechsel zwischen APs ohne längere Unterbrechungen, eine besondere Bedeutung zu. Bei Telefongesprächen sind bereits Unterbrechungen von wenigen 100 Millisekunden störend, allerdings kann eine vollständige Authentifizierung über 802.1x inklusive der folgenden Schlüsselverhandlung mit dem AP deutlich länger dauern.

Als erste Maßnahme wurde deshalb das sogenannte PMK-Caching eingeführt. Das PMK dient nach einer 802.1x-Authentifizierung zwischen Client und AP als Basis für die Schlüsselverhandlung. In VoIP-Umgebungen ist es denkbar, dass ein Anwender sich zwischen einer relativ kleinen Zahl von APs hin- und herbewegt. Dabei wird es vorkommen, dass ein Client wieder zu einem AP wechselt, an dem er bereits früher einmal angemeldet war. In so einem Fall

wäre es unsinnig, die ganze 802.1x-Authentifizierung noch einmal zu wiederholen. Aus diesem Grund kann der AP das PMK mit einer Kennung, der sogenannten PMKID, versehen, die er an den Client übermittelt. Bei einer Wiederanmeldung fragt der Client mittels der PMKID, ob er dieses PMK noch vorrätig hat. Falls ja, kann die 802.1x-Phase übersprungen werden und die Verbindung ist schnell wieder verfügbar. Diese Optimierung greift naturgemäß nicht, wenn das PMK in einem WLAN aufgrund einer Passphrase berechnet wird, denn dann ist es ja ohnehin überall gleich und bekannt.

Eine weitere Maßnahme erlaubt auch für den Fall der erstmaligen Anmeldung eine Beschleunigung, sie erfordert aber etwas Vorausschau vom Client: dieser muss bereits im Betrieb eine schlechter werdende Verbindung zum AP erkennen und einen neuen AP selektieren, während er noch Verbindung zum alten AP hat. In diesem Fall hat er die Möglichkeit, die 802.1x-Verhandlung über den alten AP mit dem neuen AP zu führen, was wiederum die 'Totzeit' um die Zeit der 802.1x-Verhandlung verkürzt.

12.5.3 TKIP und WPA

Wie in den letzten Abschnitten klar geworden ist, ist der WEP-Algorithmus prinzipiell fehlerhaft und unsicher; die bisherigen Maßnahmen waren im wesentlichen entweder 'Schnellschüsse' mit nur geringen Verbesserungen oder so kompliziert, dass sie für den Heimbenutzer oder kleine Installationen schlicht unpraktikabel sind.

Die IEEE hatte nach Bekanntwerden der Probleme mit WEP mit der Entwicklung des Standards IEEE 802.11i begonnen. Als Zwischenlösung wurde von der WiFi-Alliance der 'Standard' Wifi Protected Access (WPA) definiert. WPA setzt auf die folgenden Änderungen:

- TKIP und Michael als Ersatz für WEP
- Ein standardisiertes Handshake-Verfahren zwischen Client und AP zur Ermittlung/Übertragung der Sitzungsschlüssel.
- Ein vereinfachtes Verfahren zur Ermittlung des im letzten Abschnitt erwähnten Master Secret, das ohne einen RADIUS-Server auskommt.
- Aushandlung des Verschlüsselungsverfahrens zwischen AP und Client.

Bei der Verschlüsselung werden bekannte Bestandteile des WEP-Verfahrens weiter verwendet, aber an den entscheidenden Stellen um den „Michael-Hash“ zur besseren Verschlüsselung und das TKIP-Verfahren zur Berechnung der RC4-Schlüssel erweitert. Desweiteren ist der intern hochgezählte und im

Paket im Klartext übertragene IV statt 24 jetzt 48 Bit lang – damit ist das Problem der sich wiederholenden IV-Werte praktisch ausgeschlossen.

Als weiteres Detail mischt TKIP in Berechnung der Schlüssel auch noch die MAC-Adresse des Senders ein. Auf diese Weise ist sichergestellt, dass eine Verwendung gleicher IVs von verschiedenen Sendern nicht zu identischen RC4-Schlüsseln und damit wieder zu Angriffsmöglichkeiten führt.

Der Michael-Hash stell jedoch keine besonders hohe kryptographische Hürde dar: kann der Angreifer den TKIP-Schlüssel brechen oder verschlüsselte Pakete durch Modifikationen ähnlich wie bei WEP an der CRC-Prüfung vorbeischleusen, bleiben nicht mehr allzu viele Hürden zu überwinden. WPA definiert aus diesem Grund Gegenmaßnahmen, wenn ein WLAN-Modul mehr als zwei Michael-Fehler pro Minute erkennt: sowohl Client als auch AP brechen dann für eine Minute den Datentransfer ab und handeln danach TKIP- und Michael-Schlüssel neu aus.

Verhandlung des Verschlüsselungsverfahrens

Da die ursprüngliche WEP-Definition feste Schlüssellänge von 40 Bit vorschrieb, musste bei der Anmeldung eines Clients an einem AP lediglich angezeigt werden, ob eine Verschlüsselung genutzt wird oder nicht. Bereits bei Schlüssellängen von mehr als 40 Bit muss aber auch die Länge des verwendeten Schlüssels bekannt gegeben werden. WPA stellt einen Mechanismus bereit, mit dem sich Client und AP über das zu verwendende Verschlüsselungs- und Authentifizierungsverfahren verständigen können. Dabei werden folgenden Informationen bereitgestellt:

- Eine Liste von Verschlüsselungsverfahren, die der AP für den Pairwise Key anbietet – hier ist WEP explizit nicht mehr erlaubt.
- Eine Liste von Authentifizierungsverfahren, über die sich ein Client gegenüber dem WLAN als zugangsberechtigt zeigen kann – mögliche Verfahren sind im Moment EAP/802.1x oder PSK.

Wie erwähnt, sieht der ursprüngliche WPA-Standard einzig TKIP/Michael als verbessertes Verschlüsselungsverfahren vor. Mit der Weiterentwicklung des 802.11i-Standards wurde das weiter unten beschriebene AES/CCM-Verfahren hinzugenommen. So ist es heutzutage in einem WPA-Netz möglich, dass einige Clients über TKIP mit dem AP kommunizieren, andere Clients jedoch über AES.

12.5.4 WEP

WEP ist eine Abkürzung für Wired **E**quivalent **P**rivacy. Die primäre Zielsetzung von WEP ist die Vertraulichkeit von Daten. Im Gegensatz zu Signalen, die über Kabel übertragen werden, breiten sich Funkwellen beliebig in alle Richtungen aus – auch auf die Straße vor dem Haus und an andere Orte, wo sie gar nicht erwünscht sind. Das Problem des unerwünschten Mithörens tritt bei der drahtlosen Datenübertragung besonders augenscheinlich auf, auch wenn es prinzipiell auch bei größeren Installationen kabelgebundener Netze vorhanden ist – allerdings kann man den Zugang zu Kabeln durch entsprechende Organisation eher begrenzen als bei Funkwellen.

Hinweis: WEP bietet deutlich geringere Sicherheit als IEEE 802.1x/WPA2. Aus Gründen der Kompatibilität zu älteren WLAN-Clients unterstützen OpenBAT APs weiterhin dieses Verschlüsselungsverfahren. Hirschmann empfiehlt jedoch ausdrücklich, nach Möglichkeit eine bessere Absicherung der WLANs (z. B. nach IEEE 802.1x/WPA2) zu verwenden.

12.5.5 LEPS – LANCOM Enhanced Passphrase Security

LEPS behebt die Unsicherheit von globalen Passphrases

Mit den modernen Verschlüsselungsverfahren WPA und IEEE 802.11i kann der Datenverkehr im WLAN deutlich besser als mit WEP gegen unerwünschte „Lauschangriffe“ geschützt werden. Die Verwendung einer Passphrase als zentraler Schlüssel ist sehr einfach zu handhaben, ein RADIUS-Server wie in 802.1x-Installationen wird nicht benötigt.

Dennoch birgt die Verwendung der abhörsicheren Verfahren WPA und IEEE 802.11i einige Schwachstellen:

- Eine Passphrase gilt **global** für **alle** WLAN-Clients
- Die Passphrase kann durch Unachtsamkeit ggf. an Unbefugte weitergegeben werden
- Mit der „durchgesickerten“ Passphrase kann jeder Angreifer in das Funknetzwerk eindringen

In der Praxis bedeutet das: Falls die Passphrase „verloren geht“ oder ein Mitarbeiter mit Kenntnis der Passphrase das Unternehmen verlässt, müsste aus Sicherheitsaspekten die Passphrase im AP geändert werden – und damit auch in allen WLAN-Clients. Da das nicht immer sichergestellt werden kann, würde sich also ein Verfahren anbieten, bei dem nicht eine globale Passphrase für alle WLAN-Clients gemeinsam gilt, sondern für jeden Benutzer im WLAN eine eigene Passphrase konfiguriert werden kann. In diesem Fall muss z. B. beim Ausscheiden eines Mitarbeiters aus dem Unternehmen nur seine „persönliche“ Passphrase gelöscht werden, alle anderen behalten ihre Gültigkeit und Vertraulichkeit.

Mit LEPS (**L**ANCOM **E**nhanced **P**assphrase **S**ecurity) hat LANCOM Systems ein effizientes Verfahren entwickelt, das die einfache Konfigurierbarkeit von IEEE 802.11i mit Passphrase nutzt und dabei die möglichen Unsicherheiten bei der Nutzung einer globalen Passphrase vermeidet.

Bei LEPS wird jeder MAC-Adresse in einer zusätzlichen Spalte der ACL (Access Control List) eine **individuelle** Passphrase zugeordnet – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt die Anmeldung am AP und die anschließende Verschlüsselung per IEEE 802.11i oder WPA.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA oder 802.11i verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

LEPS kann sowohl lokal im Gerät genutzt werden als auch mit Hilfe eines RADIUS-Servers zentral verwaltet werden. LEPS funktioniert mit sämtlichen am Markt befindlichen WLAN-Client-Adaptern, ohne dass dort eine Änderung stattfinden muss. Da LEPS ausschließlich im AP konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Hinweis: Ein weiterer Sicherheitsaspekt: Mit LEPS können auch einzelne Point-to-Point-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein AP entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS

abgesicherten WLAN-Strecken weiterhin sicher, insbesondere wenn die ACL auf einem RADIUS-Server abgelegt ist.

Konfiguration

Bei der Konfiguration von LEPS wird lediglich jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dazu wird der MAC-Filter positiv eingestellt, d. h., die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Hinweis: Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Die client-spezifische Passphrase ist in der Benutzertabelle des RADIUS-Servers gespeichert. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS nutzen.

12.5.6 Background WLAN Scanning

Zur Erkennung anderer APs in der eigenen Funkreichweite können OpenBAT Wireless Geräte aktiv alle verfügbaren Kanälen prüfen (so wie das ein WLAN-Client machen würde, der nach verfügbaren APs sucht). Wenn dort ein anderer AP aktiv ist, werden die entsprechenden Informationen in der Scan-Tabelle gespeichert. Da diese Aufzeichnung im Hintergrund neben der „normalen“ Funktätigkeit der APs abläuft, wird diese Funktion auch als „Background Scan“ bezeichnet.

Das Background-Scanning wird vorwiegend für die folgenden Aufgaben eingesetzt:

- Rogue AP Detection
- Schnelles Roaming von WLAN-Clients

Rogue AP Detection

Als Rogue bezeichnet man solche WLAN-Geräte, die unerlaubt versuchen, als AP oder Client Teilnehmer in einem WLAN zu werden. Rogue APs sind solche APs, die z. B. von den Mitarbeitern einer Firma ohne Kenntnis und

Erlaubnis der System-Administratoren an das Netzwerk angeschlossen werden und so über ungesicherte WLAN-Zugänge bewusst oder unbewusst Tür und Tor für potentielle Angreifer öffnen. Nicht ganz so gefährlich, aber zumindest störend sind z. B. APs in der Reichweite des eigenen WLAN, die zu fremden Netzwerken gehören. Verwenden solche Geräte dabei z. B. die gleiche SSID und den gleichen Kanal wie die eigenen APs (Default-Einstellungen), können die eigenen WLAN-Clients versuchen, sich bei dem fremden Netzwerk einzubuchen.

Da alle unbekannten APs in der Reichweite des eigenen Netzwerks oft eine mögliche Bedrohung und Sicherleitslücke, zumindest aber eine Störung darstellen, können mit dem Background-Scanning Rogue APs identifiziert werden, um ggf. weitere Maßnahmen zur Sicherung des eigenen Netzwerks einzuleiten.

Schnelles Roaming im Client-Modus

Das Verfahren des Background-Scanning kann aber auch mit anderen Zielen als der Rogue AP Detection verwendet werden. Ein AP im Client-Modus, der sich selbst bei einem anderen AP anmeldet, kann in einer mobilen Installation auch das Roaming-Verfahren nutzen. Dies ist z. B. dann der Fall, wenn der AP in einer Industrieanwendung auf einem Gabelstapler befestigt ist, der sich durch mehrere Hallen mit separaten APs bewegt. Normalerweise würde der WLAN-Client sich nur dann bei einem anderen AP einbuchen, wenn er die Verbindung zu dem bisherigen Access Point vollständig verloren hat. Mit der Funktion des Background-Scanning kann der AP im Client-Modus schon vorher Informationen über andere verfügbare APs sammeln. Die Umschaltung auf einen anderen AP erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer AP in Reichweite über ein stärkeres Signal verfügt.

Auswertung des Background-Scans

Die Informationen über die gefundenen APs können in der Statistik des APs eingesehen werden. Sehr komfortabel stellt der WLANmonitor die Scan-Ergebnisse dar und bietet darüber hinaus zusätzliche Funktionen wie das Gruppieren der APs oder die automatische Benachrichtigung per E-Mail beim Auftauchen neuer WLAN-Geräte.

12.5.7 Erkennung von Replay-Attacken

Bei mit AES oder TKIP verschlüsselten Paketen erhält jedes Paket eine eindeutige Sequenznummer, damit der Empfänger Replays erkennen und verwerfen kann. Sofern QoS aktiviert ist, muss der Empfänger sogar pro Prioritäts-Stufe einen solchen Replay-Zähler mithalten.

Damit ergibt sich eine Angriffsmöglichkeit, bei der ein Angreifer ein mitgesnifftes Paket auf einer anderen Prio-Stufe 'replayen' kann. Einige Ansätze für Angriffe auf TKIP beruhen auf diesem Umstand.

Seit HiLCOS-Version 7.70 gibt es im Empfänger neben der Replay-Prüfung pro Prio-Stufe eine weitere 'globale' Prüfung, die zuletzt von der Gegenstelle genutzte Sequenznummern mithält. Da Sequenznummern vom Sender nicht auf verschiedenen Prio-Stufen mehrfach genutzt werden dürfen, kann man so Replay-Attacken auf einer anderen Prio-Stufe in begrenztem Umfang erkennen.

Einige WLAN-Clients, z. B. aus dem Bereich der Mobiltelefone, nutzen eine fehlerhafte AES-Implementierung mit einem separaten Sequenzzähler im Sender pro Prio-Stufe, so dass die beschriebenen Mehrfachverwendungen bei diesen Geräten normal sind.

Um auch für diese Geräte einen Betrieb zu ermöglichen, kann die globale Prüfung der Krypto-Sequenz ausgelassen werden.

WEBconfig: HiLCOS-Menübaum / Setup / WLAN

- **Globale-Krypto-Sequenz-Pruefung-auslassen**

  Stellen Sie hier die globale Prüfung der Krypto-Sequenz ein.

  Mögliche Werte:

  – Auto, Ja, Nein

  Default:

  – Auto

  Besondere Werte:

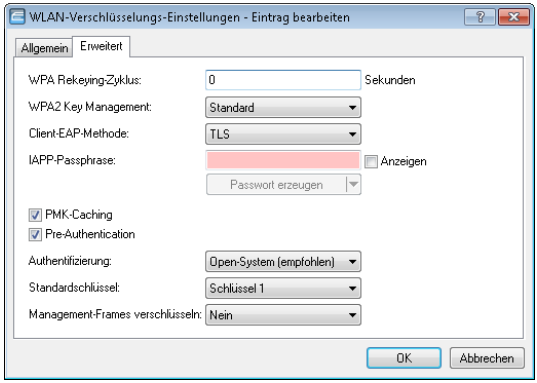
  – Auto: HiLCOS enthält eine Liste der für diese Verhalten bekannten Geräte und schaltet in der Einstellung 'Auto' die globale Sequenzprüfung ab. Für andere, noch nicht in der Liste enthaltenen Geräte muss die globale Sequenzprüfung manuell deaktiviert werden.

12.5.8 WLAN Protected Management Frames (PMF)

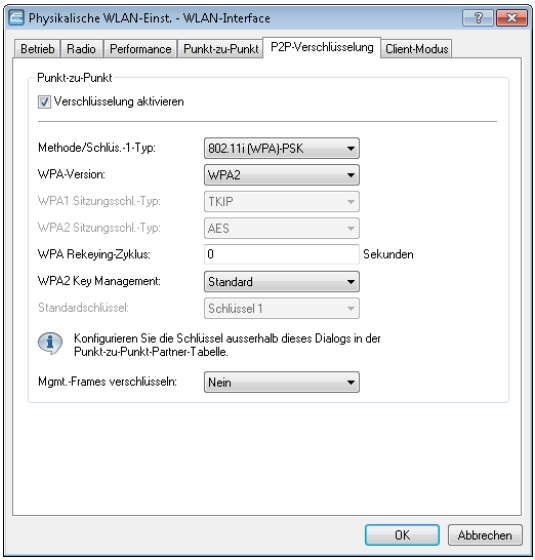
Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem AP angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen, so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

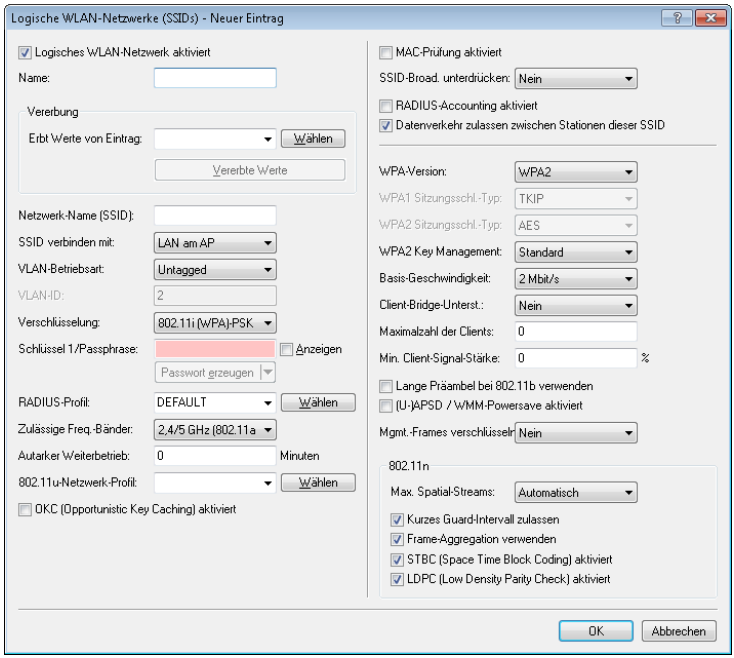
Um Protected Management Frames für ein logisches WLAN-Interface zu aktivieren, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **Verschlüsselung**, klicken auf **WLAN-Verschlüsselungs-Einstellungen**, öffnen die Konfiguration der entsprechenden WLAN-Schnittstelle, wechseln auf den Reiter **Erweitert** und wählen in der Auswahlliste **Management-Frames verschlüsseln** die entsprechende Option.



Um die Management-Frames bei P2P-Verbindung zwischen den Basisstationen zu verschlüsseln, wechseln Sie in LANconfig in die Ansicht **Wireless-LAN** > **General**, klicken auf **Physikalische WLAN-Einst.** und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Um die Verschlüsselung von Management-Frames über einen WLAN-Controller zu verwalten, wechseln Sie in LANconfig in die Ansicht **WLAN-Controller** > **Profiles**, klicken auf **Logische WLAN-Netze (SSIDs)** und wählen in der Auswahlliste **Mgmt.-Frames verschlüsseln** die entsprechende Option.



Folgende Optionen stehen bei allen Konfigurationen zur Auswahl:

Nein

Das WLAN-Interface unterstützt kein PMF. Die WLAN-Management-Frames sind nicht verschlüsselt.

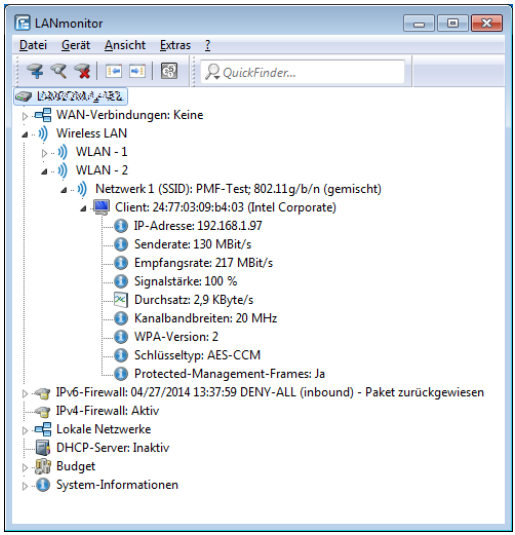
Erzwingen

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind immer verschlüsselt. Eine Verbindung zu WLAN-Clients, die PMF nicht unterstützen, ist nicht möglich.

Optional

Das WLAN-Interface unterstützt PMF. Die WLAN-Management-Frames sind je nach PMF-Unterstützung des WLAN-Clients verschlüsselt oder unverschlüsselt.

Der LANmonitor zeigt unterhalb des entsprechenden Clients an, ob dieser die WLAN-Management-Frames verschlüsselt.



12.6 Konfiguration der WLAN-Parameter

Die Einstellungen für die Funknetzwerke erfolgen an verschiedenen Stellen in der Konfiguration:

- Manche Parameter betreffen die physikalische WLAN-Schnittstellen. Einige Hirschmann-Modelle verfügen über eine WLAN-Schnittstelle (Single Radio), andere Modelle haben ein zweites WLAN-Modul integriert (Dual Radio). Die Einstellungen für die physikalischen WLAN-Schnittstellen gelten für alle logischen Funknetzwerke, die mit diesem Modul aufgespannt werden. Zu diesen Parametern gehören z. B. die Sendeleistung der Antenne und die Betriebsart des WLAN-Moduls (AP oder Client).
- Andere Parameter beziehen sich nur auf die jeweiligen logischen Funknetze, die mit einem physikalischen Interface aufgespannt werden. Dazu gehört z. B. die SSID oder die Aktivierung der Verschlüsselung, z. B. 802.11i mit AES.
- Eine dritte Gruppe von Parametern hat zwar Auswirkungen auf den Betrieb des Funknetzwerks, ist aber nicht nur für WLANs von Bedeutung. Dazu gehören z. B. die Protokollfilter in der LAN-Bridge.

12.6.1 Allgemeine WLAN-Einstellungen

LANconfig: Wireless-LAN / Allgemein

WEBconfig: HiLCOS-Menübaum / Setup / WLAN

- Ländereinstellung

  Der Betrieb von WLAN-Modulen ist international nicht einheitlich geregelt. Die Verwendung von bestimmten Funkkanälen ist z. B. in manchen Ländern nicht erlaubt. Um den Betrieb der APs auf die in dem jeweiligen Land zulässigen Parameter zu begrenzen, wird für alle physikalischen WLAN-Interfaces gemeinsam das Land eingestellt, in dem der AP betrieben wird.

- ARP-Behandlung

  Mobile Stationen im Funknetz, die sich im Stromsparmodus befinden, beantworten die ARP-Anfragen anderer Netzteilnehmer nicht oder nur unzuverlässig. Mit dem Aktivieren der 'ARP-Behandlung' übernimmt der AP diese Aufgabe und beantwortet die ARP Anfragen an Stelle der Stationen im Stromsparmodus.

- Link-Fehler-Erkennung

  Die 'Link-Fehler-Erkennung' schaltet das WLAN-Modul ab, wenn der AP keine Verbindung zum LAN mehr hat.

- Indoor-Funktion für WLAN-Kanäle

  Mit der Auswahl des Frequenzbandes (2,4 oder 5 GHz) legen Sie u.a. die möglichen Kanäle fest, die für die Übertragung verwendet werden dürfen. Aus diesen möglichen Kanälen wählt ein AP bei automatischer Kanalwahl einen freien Kanal aus, um z. B. Störungen mit anderen Funksignalen zu vermeiden.

  In einigen Ländern gelten spezielle Vorschriften, welche Frequenzbänder und Kanäle für die WLAN-Nutzung im Indoor- und Outdoor-Betrieb verwendet werden dürfen. So dürfen z. B. in Frankreich im 2,4 GHz-Band nicht alle verfügbaren Kanäle im Outdoor-Betrieb genutzt werden. In manchen Ländern ist das DFS-Verfahren für den Outdoor-Betrieb im 5 GHz-Band vorgeschrieben, um Störungen von Radaranlagen zu vermeiden.

  Mit der Option 'Indoor-Only' kann ein AP auf den ausschließlichen Betrieb innerhalb von geschlossenen Gebäuden beschränkt werden. Durch diese

Einschränkung können auf der anderen Seite bei der automatischen Kanalwahl die Kanäle flexibler gehandhabt werden.

Hinweis: Die Indoor-Only-Funktion kann nur zuverlässig aktiviert werden, wenn das Land eingestellt wurde, in dem der AP betrieben wird.

Hinweis: Die Aktivierung der Indoor-Only-Funktion ist nur erlaubt, wenn sich der AP sowie alle verbundenen Clients in einem geschlossenen Raum befinden.

- Mail-Adresse

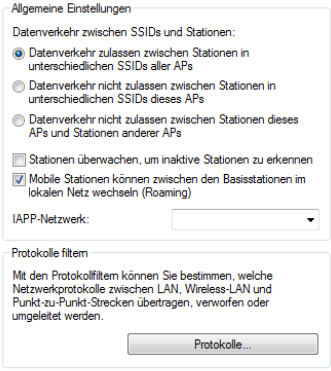
  An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet.

12.6.2 WLAN-Sicherheit

In diesem Konfigurationsbereich schränken Sie die Kommunikation der Teilnehmer im Funknetzwerk ein. Dazu wird die Datenübertragung zwischen bestimmten Teilnehmer-Gruppen, nach einzelnen Stationen oder nach verwendetem Protokoll begrenzt. Außerdem werden hier die Schlüssel für die jeweilige Verschlüsselung im WLAN eingestellt.

Allgemeine Einstellungen

Hier finden Sie allgemeine Einstellungen zum WLAN.



LANconfig: Wireless-LAN / Security

- Datenverkehr zwischen SSIDs und Stationen

  Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem AP angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Die Kommunikation der Clients in unterschiedlichen SSIDs kann mit dieser Option erlaubt oder verhindert werden. Bei Modellen mit mehreren WLAN-Modulen gilt diese Einstellung global für allem WLANs aller Module.

  Hinweis: Die Kommunikation der Clients innerhalb eines logischen WLANs wird separat bei den logischen WLAN-Einstellungen gesteuert (Inter-Station-Verkehr). Wenn der Inter-SSID-Verkehr aktiviert ist und der Inter-Station-Verkehr deaktiviert, kann ein Client aus einem logischen WLAN mit den Clients in anderen logischen WLANs kommunizieren. Diese Möglichkeit kann über VLAN-Einstellungen oder Protokollfilter verhindert werden.

- Stationen überwachen, um inaktive Stationen zu erkennen

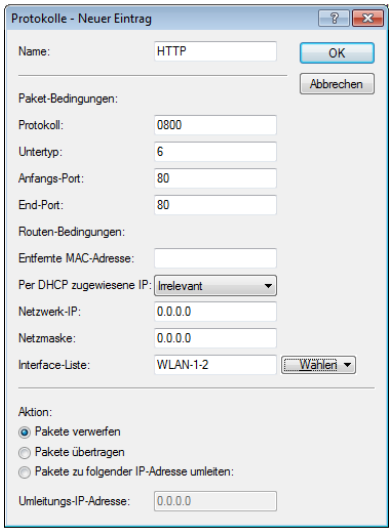
  Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der AP zur Überwachung in regelmäßigen Abständen Pakete an die eingebuchten Stationen schicken. Kommen von einer Station keine Antworten mehr auf diese Pakete, wird sie als nicht mehr aktiv an das Abrechnungssystem gemeldet.

- Mobile Stationen können zwischen den Basisstationen im lokalen Netz wechseln (Roaming)

  Neben der Kommunikation der Clients untereinander kann hier auch eingestellt werden, ob die benachbarten APs beim Roaming Informationen über das IAPP austauschen. Das Inter Access Point Protocol (IAPP) ist ein Protokoll zur Kommunikation zwischen APs. Der “abgebende AP” bekommt so die Nachricht, dass ein bei ihm eingebuchter WLAN-Client nun zu einem anderen AP wechselt und kann den Client sofort aus seiner Liste entfernen.

Protokoll-Filter

Mit dem Protokoll-Filter können Sie die Behandlung von bestimmten Datenpaketen bei der Übertragung aus dem WLAN ins LAN beeinflussen. Mit Hilfe von entsprechenden Regeln wird dabei festgelegt, welche Datenpakete erfasst werden sollen, für welche Interfaces der Filter gilt und welche Aktion mit den Datenpaketen ausgeführt werden soll.



LANconfig: Wireless LAN / Security / Protokolle

WEBconfig: HiLCOS-Menübaum / Setup / LAN-Bridge / Protokoll-Tabelle

Ein Protokoll-Filter besteht ähnlich einer Firewall-Regel aus zwei Teilen:

- Die Paket-Bedingung definiert die Bedingungen, die zutreffen müssen, damit der Filter auf ein Paket angewendet werden muss.
- Die Aktion definiert, was mit dem Paket geschehen soll, wenn die Bedingung zutrifft.

Ein Paketfilter wird durch die folgenden Parameter beschrieben:

- **Name**: frei wählbarer Name für den Filtereintrag
- **Protokoll**: Protokoll, für das dieser Filter gelten soll. Wird als Protokoll eine '0' eingetragen, so gilt dieser Filter für **alle** Pakete.
- **Untertyp**: Unterprotokoll, für das dieser Filter gelten soll. Wird als Unterprotokoll eine '0' eingetragen, so gilt dieser Filter für **alle** Pakete des eingetragenen Protokolls.
- **Anfangs-Port** und **End-Port**: Portbereich, für den dieser Filter gelten soll. Wird für den Anfangs-Port eine '0' eingetragen, so gilt dieser Filter für alle Ports des entsprechenden Protokolls/Unterprotokolls. Wird für den End-Port eine '0' eingetragen, gilt der Anfangs-Port auch als End-Port.

  Hinweis: Listen mit den offiziellen Protokoll- und Portnummern finden Sie im Internet unter www.iana.org.

- **Entfernte MAC-Adresse**: Die MAC-Adresse des Clients, zu dem das Paket übertragen werden soll. Wird keine Ziel-MAC-Adresse eingetragen, so gilt dieser Filter für **alle** Pakete.
- **DHCP-Source-MAC**: Aktivierung des DHCP-Adress-Tracking.
  - **Ja**: Die Regel trifft zu, wenn die Quell-MAC-Adresse des Pakets in der Tabelle unter `Status > LAN-Bridge-Statistiken > DHCP-Tabelle` als Adresse verzeichnet ist, die eine IP-Adresse per DHCP bezogen hat.
  - **Nein**: Die Regel trifft zu, wenn dies nicht der Fall ist.
  - **Irrelevant**: Die Quell-MAC-Adresse findet keine Beachtung.

  Hinweis: Wenn das DHCP-Adress-Tracking aktiviert ist, werden die in der Regel evtl. eingetragenen IP-Adressen nicht beachtet.

- **IP-Netzwerk** und IP-Netzmaske: Die IP-Adresse des Netzwerks, für das dieser Filter gilt. Nur IP-Pakete, deren Quell- und Ziel-IP-Adressen in diesem Netzwerk liegen, werden von der Regel erfasst.

  Wird kein Netzwerk eingetragen, so gilt dieser Filter für **alle** Pakete.

- **Interface-Liste**: Liste der Schnittstellen, für die der Filter gilt.

  Als Interfaces können alle LAN-Interfaces, DMZ-Interfaces, die logischen WLAN-Netze und die Point-to-Point-Strecken im WLAN eingetragen werden.

  Die Interfaces werden z. B. in der Form 'LAN-1' für das erste LAN-Interface oder 'WLAN-2-3' für das dritte logische WLAN-Netz auf dem zweiten physikalischen WLAN-Interface oder 'P2P-1-2' für die zweite Point-to-Point-Strecke auf dem ersten physikalischen WLAN-Interface angegeben.

  Gruppen von Interfaces können in der Form 'WLAN-1-1~WLAN-1-6' (logische WLANs 1 bis 6 auf dem ersten physikalischen WLAN-Interface) oder mit Wildcard als 'P2P-1-*' (alle P2P-Strecken auf dem ersten physikalischen Interface) angegeben werden.

  Hinweis: Nur Filter-Regeln mit gültigen Einträgen in der Interface-Liste sind aktiv. Eine Regel ohne Angabe der Interfaces gilt nicht für alle, sondern wird ignoriert.

- **Aktion**: Aktion, für die Datenpakete ausgeführt wird, die mit dieser Regel erfasst werden:
- **Umleite-IP-Adresse**: Ziel-IP-Adresse für die Aktion 'Umleiten'

  Bei einem Redirect wird die Ziel-IP-Adresse der Pakete durch die hier eingetragene Umleite-IP-Adresse ersetzt. Zusätzlich wird die Ziel-MAC-Adresse durch die MAC-Adresse ersetzt, die über ARP für die Umleite-IP-Adresse ermittelt wurde.

  Hinweis: Wenn die Ziel-MAC-Adresse nicht über ARP ermittelt werden konnte, wird das Paket nicht umgeleitet, sondern verworfen.

Beispiel:

Name	*DHCP-Src-MAC*	*Ziel-MAC-Adr.*	*Prot.*	*IP-Adresse*	*IP-Netzwerk*	*Untertyp*	*Anfangs-Port*	*EndPort*	*Interface-Liste*	*Aktion*	*Umleite-IP-Adresse*
ARP	irrelevant	000000000000	0806	0.0.0.0	0.0.0.0	0	0	0	WLAN-1-2	Durchlassen	0.0.0.0

Name	DHCP-Src-MAC	Ziel-MAC-Adr.	Prot.	IP-Adresse	IP-Netzwerk	Untertyp	Anfangs-Port	End-Port	Interface-Liste	Aktion	Umleit-IP-Adresse
DHCP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	17	67	68	WLAN-1-2	Durchlassen	0.0.0.0
TELNET	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	23	23	WLAN-1-2	Umleiten	192.168.11.5
ICMP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	1	0	0	WLAN-1-2	Durchlassen	0.0.0.0
HTTP	irrelevant	000000000000	0800	0.0.0.0	0.0.0.0	6	80	80	WLAN-1-2	Umleiten	192.168.11.5

ARP, DHCP, ICMP werden durchgelassen, Telnet und HTTP werden umgleitet auf 192.168.11.5, alle anderen Pakete werden verworfen.

Solange für ein Interface keine Filter-Regeln definiert sind, werden alle Pakete von diesem Interface sowie alle Pakete für dieses Interface ohne Veränderung übertragen. Sobald für ein Interface eine Filter-Regel definiert wurde, werden alle Pakete, die über dieses Interface übertragen werden sollen, vor der Bearbeitung geprüft.

1. Im ersten Schritt werden aus den Pakete die zur Prüfung benötigten Informationen ausgelesen:

- DHCP-Source-MAC
- Ziel-MAC-Adresse des Paketes
- Protokoll, z. B. IPv4, IPX, ARP
- Subprotokoll, z. B. TCP, UDP oder ICMP für IPv4-Pakete, ARP Request oder ARP Response für ARP-Pakete
- IP-Adresse und Netzmaske (Quelle und Ziel) für IPv4-Pakete
- Quell- und Ziel-Port für IPv4-TCP- oder IPv4-UDP-Pakete

2. Diese Informationen werden im zweiten Schritt gegen die Angaben aus den Filter-Regeln geprüft. Dabei werden alle Regeln berücksichtigt, bei denen das Quell- **oder** das Ziel-Interface in der Interface-Liste enthalten sind. Die Prüfung der Regeln verhält sich für die einzelnen Werte wie folgt:

- Für DHCP-Source-MAC, Protokoll und Unterprotokoll werden die aus den Paketen ausgelesenen Werte mit den Werten der Regel auf Übereinstimmung geprüft.
- Bei IP-Adressen werden die Quell- **und** die Ziel-Adresse des Pakets daraufhin geprüft, ob sie in dem Bereich liegen, der durch die IP-Adresse und die Netzmaske der Regel gebildet wird.
- Quell- und den Zielports werden daraufhin geprüft, ob sie im Bereich zwischen Anfangs- und End-Port liegen.

Wenn keiner der spezifizierten (nicht durch Wildcards gefüllten) Werte der Regel mit den aus dem Paket ausgelesenen Werten übereinstimmt, wird

die Regel als nicht zutreffend betrachtet und ausgelassen. Falls mehrere Regeln zutreffen, wird die Aktion der Regel ausgeführt, die am genauesten zutrifft. Dabei gelten die Parameter als genauer, je weiter unten Sie in der Liste der Parameter stehen bzw. je weiter rechts sie in der Protokoll-Tabelle auftauchen.

Hinweis: Wenn für ein Interface Regeln definiert sind, bei einem Paket von bzw. für dieses Interface jedoch keine Übereinstimmung mit einer der Regeln gefunden werden kann, dann wird für das Paket die Default-Regel für das Interface verwendet. Die Default-Regel ist für jedes Interface mit der Aktion 'verwerfen' vorkonfiguriert, aber nicht sichtbar in der Protokoll-Tabelle. Um die Default-Regel für ein Interface zu modifizieren, wird eine Regel mit dem Namen 'default-drop' angelegt, die neben den entsprechenden Interface-Bezeichnungen nur Wildcards und die gewünschte Aktion enthält.

Die Prüfung der MAC-Adressen verhält sich bei Paketen, die über das entsprechende Interface verschickt werden, anders als bei eingehenden Paketen.

- Bei den ausgehenden Paketen wird die aus dem Paket ausgelesene Quell-MAC-Adresse gegen die in der Regel eingetragene Ziel-MAC-Adresse geprüft.
- Die aus dem Paket ausgelesene Ziel-MAC-Adresse wird daraufhin geprüft, ob sie in der Liste der aktuell aktiven DHCP-Clients enthalten sind.
- Regeln mit der Aktion 'Umleiten' werden ignoriert, wenn sie für ein Interface zutreffen, auf dem das Paket verschickt werden soll.

3. Im dritten Schritt wird die Aktion der zutreffenden Regel ausgeführt.

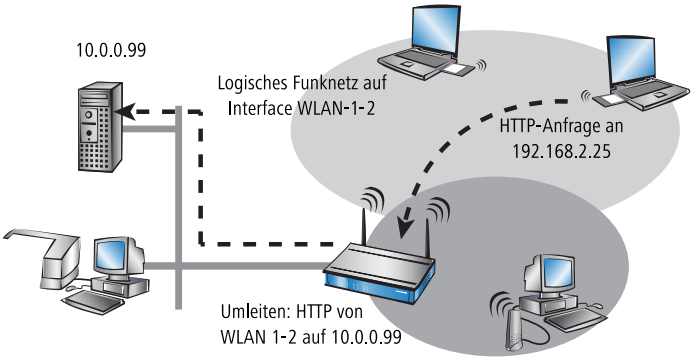
Mit der Aktion 'Umleiten' (Redirect) können IPv4-Pakete nicht nur übertragen oder verworfen werden, sondern gezielt zu einem bestimmten Ziel übermittelt werden. Dazu wird die Ziel-IP-Adresse des Pakets durch die in der Regel eingetragene Umleite-IP-Adresse ersetzt, die Ziel-MAC-Adresse des Pakets wird durch die per ARP ermittelte, zur Umleite-IP-Adresse gehörige MAC-Adresse ersetzt.

Damit die umgeleiteten Pakete auf dem „Rückweg“ auch wieder den richtigen Absender finden, werden in einer dynamischen Tabelle automatisch Filter-Regeln angelegt, die für die ausgehenden Pakete auf diesem Interface genutzt

werden. Diese Tabelle kann unter `Status > LAN-Bridge-Statistiken > Verbindungs-Tabelle` eingesehen werden. Die Regeln in dieser Tabelle haben eine höhere Priorität als andere passende Regeln mit den Aktionen 'Übertragen' oder 'Verwerfen'.

Die Teilnehmer (Clients) in Funknetzwerken haben vor allem eine Eigenschaft oft gemeinsam: eine hohe Mobilität. Die Clients verbinden sich also nicht unbedingt immer mit dem gleichen AP, sondern wechseln den AP und das zugehörige LAN relativ häufig.

Die Redirect-Funktion hilft dabei, die Anwendungen von WLAN-Clients bei der Übertragung in das LAN automatisch immer auf den richtigen Zielrechner einzustellen. Wenn die Anfragen von WLAN-Clients über HTTP aus einem bestimmten logischen Funknetzwerk immer auf einen bestimmten Server im LAN umgeleitet werden sollen, wird für das entsprechende Protokoll ein Filtereintrag mit der Aktion 'Umleiten' für das gewünschte logische WLAN-Interface aufgestellt.



Alle Anfragen mit diesem Protokoll aus diesem logischen Funknetz werden dann automatisch umgeleitet auf den Zielserver im LAN. Bei der Rückübertragung der Datenpakete werden die entsprechenden Absenderadressen und Ports aufgrund der Einträge in der Verbindungsstatistik wieder eingesetzt, so dass ein störungsfreier Betrieb in beiden Richtungen möglich ist.

Mit dem DHCP-Adress-Tracking wird nachgehalten, welche Clients ihre IP-Adresse über DHCP erhalten haben. Die entsprechenden Informationen werden für ein Interface automatisch in einer Tabelle unter `Status >`

`LAN-Bridge-Statistiken > DHCP-Tabelle` geführt. DHCP-Tracking wird auf einem Interface aktiviert, wenn für dieses Interface mindestens eine Regel definiert ist, bei denen 'DHCP-Source-MAC' auf 'Ja' steht.

Hinweis: Die Anzahl der Clients, die über DHCP mit einem Interface verbunden sein dürfen, kann in der Port-Tabelle unter `Setup > LAN-Bridge > Port-Daten` eingestellt werden. Mit dem Eintrag von '0' können sich beliebig viele Clients an diesem Interface über DHCP anmelden. Würde die maximale Anzahl der DHCP-Clients bei einem weiteren Anmeldeversuch überschritten, so wird der älteste Eintrag aus der Liste entfernt.

Bei der Prüfung der Datenpakete werden die in der Regel definierten IP-Adresse und die IP-Netzmaske nicht verwendet. Es wird also nicht geprüft, ob die Ziel-IP-Adresse des Paketes im vorgegebenen Bereich liegt. Stattdessen wird geprüft, ob die Quell-IP-Adresse des Pakets mit derjenigen IP-Adresse übereinstimmt, die dem Client per DHCP zugewiesen wurde. Die Verbindung der beiden IP-Adressen findet anhand der Quell-MAC-Adresse statt.

Mit dieser Prüfung können Clients geblockt werden, die zwar eine IP-Adresse via DHCP empfangen haben, dann aber (versehentlich oder bewusst) tatsächlich eine andere IP-Adresse verwenden. Eine Regel mit dem Parameter DHCP-Source-MAC = 'Ja' würde also nicht zutreffen, da die beiden Adressen nicht übereinstimmen. Stattdessen würde eine andere Regel oder die Default-Regel das Paket verarbeiten.

Damit DHCP-Tracking funktionieren kann, müssen mindestens zwei weitere Regeln für dieses Interface konfiguriert werden, die nicht auf DHCP-Tracking beruhen. Das ist erforderlich, da die erforderliche DHCP-Information erst am Ende der DHCP-Verhandlung ausgetauscht wird. Daher müssen die vorher zu übertragenden Pakete über Regeln zugelassen werden, die kein DHCP-Tracking verwenden. Dazu gehören normalerweise Pakete über TCP / UDP auf Port 67 und 68 und ARP-Pakete.

Hinweis: Ist DHCP-Tracking auf einem Interface aktiviert, so werden automatisch auf diesem Interface empfangene Pakete von DHCP-Servern verworfen.

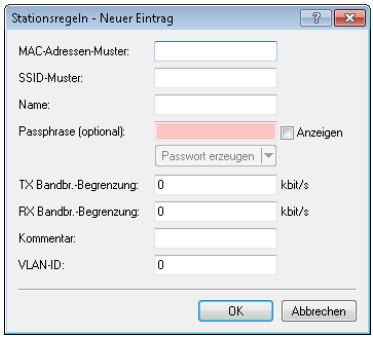
12.6.3 Auswahl der im WLAN zulässigen Stationen

Access Control List

Mit der **A**ccess **C**ontrol **L**ist (ACL) gewähren oder untersagen Sie einzelnen WLAN-Clients den Zugriff auf Ihr WLAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der WLAN-Adapter.

Hinweis: Bei der zentralen Verwaltung der und Hirschmann APs über einen WLC finden Sie die Stationstabelle unter **WLAN-Controller** > **Stationen** unter der Schaltfläche **Stationen**.

Kontrollieren Sie unter **Wireless-LAN** > **Stationen**, ob die Einstellung **Daten von den aufgeführten Stationen übertragen, alle anderen Stationen ausfiltern** aktiviert ist. Fügen Sie neue Stationen, die an Ihrem Funk-Netzwerk teilnehmen sollen, ggf. über die Schaltfläche **Stationen** hinzu.



MAC-Adressen-Muster

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Hinweis: Die Verwendung von Wildcards ist möglich.

SSID-Muster

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Hinweis: Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

TX Bandbreitenbegrenzung

Sende-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

RX Bandbreitenbegrenzung

Empfangs-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Ein-

stellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Hinweis: Die RX-Bandbreiten-Begrenzung ist nur aktiv für WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

VLAN-ID

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden. Bei der VLAN-ID '0' wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von Einträgen darauf zu achten, dass sich die Filterregeln nicht widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

Wichtig: Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

12.6.4 Verschlüsselungs-Einstellungen

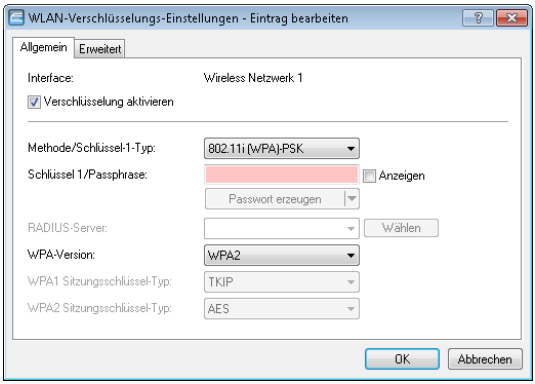
Die APs der Hirschmann-Familie unterstützen die aktuellsten Verfahren zur Verschlüsselung und Absicherung der Daten, die über eine WLAN-Verbindung übertragen werden.

- Der IEEE-Standard 802.11i/WPA steht für die höchste Sicherheit, die derzeit für WLAN-Verbindungen erreicht werden kann. Dieser Standard setzt u.a auf ein neues Verschlüsselungsverfahren (AES-CCM) und erreicht im Zusammenspiel mit einigen anderen Methoden eine Sicherheit, die bisher nur von VPN-Verbindungen erzielt werden konnte. Beim Einsatz von AES-fähiger Hardware (wie den 54-MBit-Hirschmann-APs) ist die Übertragung jedoch deutlich schneller als bei einer entsprechenden VPN-Absicherung.

- Aus Gründen der Kompatibilität zu älterer Hardware wird auch weiterhin das WEP-Verfahren unterstützt. WEP (**W**ired **E**quivalent **P**rivacy) war das ursprünglich im 802.11-Standard vorgesehene Verfahren zur Verschlüsselung der Daten bei Funkübertragungen. Dabei kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Im Laufe der Zeit sind bei WEP jedoch einige Sicherheitslücken bekannt geworden, weshalb nach Möglichkeit nur noch die aktuellen 802.11i/WPA-Methoden eingesetzt werden sollten.

WLAN-Verschlüsselungs-Einstellungen

Die Schlüsseleinstellungen konfigurieren Sie unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen**. Markieren Sie die entsprechende Schnittstelle und klicken Sie auf **Bearbeiten**. Auf dem Reiter **Allgemein** finden Sie die folgenden Einstellungen:



Verschlüsselung aktivieren

Aktivieren bzw. deaktivieren Sie die Verschlüsselung für diese WLAN-Schnittstelle.

Methode/Schlüssel-1-Typ

Stellen Sie hier das zu verwendende Verschlüsselungsverfahren ein. Mögliche Werte sind:

- 802.11i (WPA)-PSK – Die Verschlüsselung nach dem 802.11i-Standard bietet die höchste Sicherheit. Die dabei eingesetzte 128-Bit-AES-Verschlüsselung entspricht der Sicherheit einer VPN-Verbindung.

Wählen Sie diese Einstellung, wenn kein RADIUS-Server zur Verfügung steht und die Authentifizierung mit Hilfe eines Preshared Keys erfolgt.

- 802.11i (WPA)-802.1x – Wenn die Authentifizierung über einen RADIUS-Server erfolgt, wählen Sie die Option '802.11i (WPA)-802.1x'. Achten Sie bei dieser Einstellung darauf, auch den RADIUS-Server bei den 802.1x-Einstellungen zu konfigurieren.
- WEP 152, WEP 128, WEP 64 – Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit. Diese Einstellung ist nur zu empfehlen, wenn die verwendete Hardware der WLAN-Clients die modernen Verfahren nicht unterstützt.
- WEP 152-802.1x, WEP 128-802.1x, WEP 64-802.1x – Verschlüsselung nach dem WEP-Standard mit Schlüssellängen von 128, 104 bzw. 40 Bit und zusätzlicher Authentifizierung über 802.1x/EAP. Auch diese Einstellung kommt i.d.R. dann zum Einsatz, wenn die verwendete Hardware der WLAN-Clients den 802.11i-Standard nicht unterstützt. Durch die 802.1x/EAP-Authentifizierung bietet diese Einstellung eine höhere Sicherheit als eine reine WEP-Verschlüsselung.

Schlüssel-1/Passphrase

Je nach eingestelltem Verschlüsselungsverfahren können Sie hier einen speziellen WEP-Schlüssel für das jeweilige logische WLAN-Interface bzw. eine Passphrase bei der Verwendung von WPA-PSK eintragen:

- Die Passphrase – also das “Passwort” für das WPA-PSK-Verfahren – wird als Kette aus mindestens 8 und maximal 63 ASCII-Zeichen eingetragen.

  Hinweis: Bitte beachten Sie, dass die Sicherheit des Verschlüsselungssystems bei der Verwendung einer Passphrase von der vertraulichen Behandlung dieses Kennworts abhängt. Die Passphrase sollte nicht einem größeren Anwenderkreis bekannt gemacht werden.

- Der WEP-Schlüssel-1, der nur speziell für das jeweilige logische WLAN-Interface gilt, kann je nach Schlüssellänge unterschiedlich eingetragen werden. Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel.

RADIUS-Server

Wenn Sie unter **Methode/Schlüssel-1-Typ** eine Authentifizierung nach dem Standard IEEE 802.1X auswählen, geben Sie hier das Profil eines RADIUS-Servers an.

WPA-Version

WPA-Version die der Access Point den WLAN-Clients zur Verschlüsselung anbietet.

- WPA1: Nur WPA1
- WPA2: Nur WPA2
- WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)

WPA 1 Sitzungs-Schlüssel-Typ

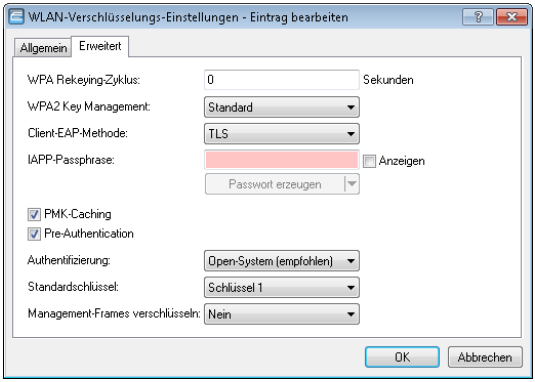
Wenn als Verschlüsselungsmethode '802.11i (WPA)-PSK' eingestellt wurde, kann hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA 1ausgewählt werden:

- AES – Es wird das AES-Verfahren verwendet.
- TKIP – Es wird das TKIP-Verfahren verwendet.
- AES/TKIP – Es wird das AES-Verfahren verwendet. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wird TKIP eingesetzt.

WPA 2 Sitzungs-Schlüssel-Typ

Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA 2.

Auf dem Reiter **Erweitert** finden Sie die folgenden Einstellungen:



WPA Rekeying-Zyklus

Ein 48 Bit langer Initialization Vector (IV) erschwert die Berechnung des WPA-Schlüssels für Angreifer. Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels würde erst nach 16 Millionen Paketen erfolgen. In stark genutzten WLANs also erst nach einigen Stunden. Um die Wiederholung des echten Schlüssels zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen.

Geben Sie hier einen Wert in Sekunden an, nachdem der Schlüssel neu ausgehandelt wird.

In der Standardeinstellung ist der Wert auf '0' eingestellt, so dass keine vorzeitige Aushandlung des Schlüssels erfolgt.

WPA2 Key Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll. Mögliche Werte sind:

- Standard: Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.
- SHA256: Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11w mit SHA-256-basierten Schlüsseln.
- Fast Roaming: Aktiviert Fast Roaming über 802.11r
- Kombinationen der drei Einstellungen

Wichtig: Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am AP anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als **Standard** aktiviert ist.

Client-EAP-Methode

APs in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen AP authentifizieren. Zur Aktivierung der EAP/802.1X-Authentifizierung im Client-Modus wird bei den Verschlüsselungsmethoden

für das erste logische WLAN-Netzwerk die Client-EAP-Methode ausgewählt.

Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des Access Points passen muss, bei dem sich der AP einbuchen will.

Hinweis: Beachten Sie neben der Einstellung der Client-EAP-Methode auch die entsprechende Einstellung der Betriebsart als WLAN-Client. Bei anderen logischen WLAN-Netzwerken als WLAN-1 ist die Einstellung der Client-EAP-Methode ohne Funktion.

PMK-Caching

Beim Verbindungsaufbau eines WLAN-Clients zu einem AP handeln die beiden Gegenstellen im Rahmen der 802.1x-Authentifizierung einen gemeinsamen Schlüssel für die nachfolgende Verschlüsselung aus, den Pairwise Master Key (PMK). Bei Anwendungen mit bewegten WLAN-Clients (Notebooks in größeren Büro-Umgebungen, bewegte Objekte mit WLAN-Anbindung im Industriebereich) wechseln die WLAN-Clients häufig den AP, bei dem sie sich in einem WLAN-Netz anmelden. Die WLAN-Clients roamen also zwischen verschiedenen, aber in der Regel immer den gleichen APs hin und her.

APs speichern üblicherweise einen ausgehandelten PMK für eine bestimmte Zeit. Auch ein WLAN-Gerät in der Betriebsart als WLAN-Client speichert den PMK. Sobald ein WLAN-Client einen Anmeldevorgang bei einem AP startet, zu dem zuvor schon einer Verbindung bestand, kann der WLAN-Client direkt den vorhandenen PMK zur Prüfung an den AP übermitteln. Die beiden Gegenstellen überspringen so die Phase der PMK-Aushandlung während des Verbindungsaufbaus, WLAN-Client und AP stellen die Verbindung deutlich schneller her.

Der WLAN-Client speichert den ausgehandelten PMK für die unter dem Parameter "Vorgabe-Lebenszeit" eingestellte Dauer.

Pre-Authentication

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2/802.1x unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1x-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1x-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Hinweis: Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.

- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

Hinweis: Client-seitig ist die Anzahl gleichzeitiger Prä-Authentifizierungen auf vier begrenzt, um in Netzwerk-Umgebungen mit vielen APs die Netzlast für den zentralen RADIUS-Server gering zu halten.

Authentifizierung

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, stehen zwei verschiedene Verfahren für die Authentifizierung der WLAN-Clients zur Verfügung:

- Beim "OpenSystem"-Verfahren wird komplett auf eine Authentifizierung verzichtet. Die Datenpakete müssen von Beginn an richtig verschlüsselt übertragen werden, um von der Basisstation akzeptiert zu werden.

- Beim "SharedKey"-Verfahren wird das erste Datenpakte unverschlüsselt übertragen und muss vom Client richtig verschlüsselt zurückgesendet werden. Bei diesem Verfahren steht einem potenziellen Angreifer mindestens ein Datenpaket unverschlüsselt zur Verfügung.

Standardschlüssel

Wenn als Verschlüsselungsmethode eine WEP-Verschlüsselung eingestellt wurde, kann der AP für jedes logische WLAN-Interface aus vier verschiedenen WEP-Schlüsseln wählen:

- Drei WEP-Schlüssel für das physikalische Interface
- Ein zusätzlicher WEP-Schlüssel speziell für jedes logische WLAN-Interface

Bei den Einzel-WEP-Einstellungen wird der zusätzliche Schlüssel für jedes logische WLAN-Interface eingestellt (siehe 'Schlüssel-1/Passphrase'). Wählen Sie außerdem aus, welcher der vier eingestellten Schlüssel aktuell für die Verschlüsselung der Daten verwendet werden soll (Standardschlüssel). Mit dieser Einstellung können Sie den Schlüssel häufiger wechseln, um die Abhörsicherheit zusätzlich zu steigern.

Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel.

Mgmt.-Frames verschlüsseln

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem AP angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen, so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

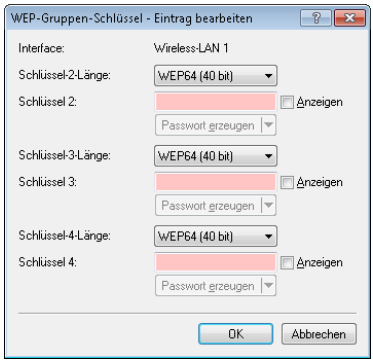
WEP-Gruppen-Schlüssel

Bei WEP kommen Schlüssel von 40 (WEP64), 104 (WEP128) oder 128 Bit (WEP152) Länge zum Einsatz. Für jedes WLAN-Interface stehen vier WEP-

Schlüssel zur Verfügung: ein spezieller Schlüssel für jedes logische WLAN-Interface und drei gemeinsame Gruppen-WEP-Schlüssel für jedes physikalische WLAN-Interface.

Hinweis: Wenn bei der Verwendung von 802.1x/EAP die 'dynamische Schlüssel-Erzeugung und -Übertragung' aktiviert ist, werden die Gruppen-Schlüssel von 802.1x/EAP verwendet und stehen damit für die WEP-Verschlüsselung nicht mehr zur Verfügung.

Die Regeln für die Eingabe der Schlüssel finden Sie bei der Beschreibung der WEP-Gruppenschlüssel.



LANconfig: Wireless LAN / 802.11i/WEP / WEP-Gruppen-Schlüssel

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Gruppen-Schluessel

Regeln für die Eingabe von WEP-Schlüsseln

Die WEP-Schlüssel können als ASCII-Zeichen oder in Hexadezimaler Darstellung eingetragen werden. Die hexadezimale Darstellung beginnt jeweils mit den Zeichen '0x'. Die Schlüssel haben je nach WEP-Verfahren folgende Länge:

Verfahren	*ASCII*	*HEX*
WEP 64	5 Zeichen Beispiel: 'aR45Z'	10 Zeichen Beispiel: '0x0A5C1B6D8E'
WEP 128	13 Zeichen	26 Zeichen

Verfahren	*ASCII*	*HEX*
WEP 152	16 Zeichen	32 Zeichen

Der ASCII-Zeichensatz umfasst die Zeichen '0' bis'9', 'a' bis 'z', 'A' bis 'Z' sowie die folgenden Sonderzeichen: ! ” # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ‘ { | } ~

In der HEX-Darstellung wird jedes Zeichen durch ein Zeichenpaar aus den Ziffern '0' bis'9' und den Buchstaben 'A' bis 'F' dargestellt, daher benötigen die HEX-Schlüssel die doppelte Anzahl an Zeichen zur Darstellung.

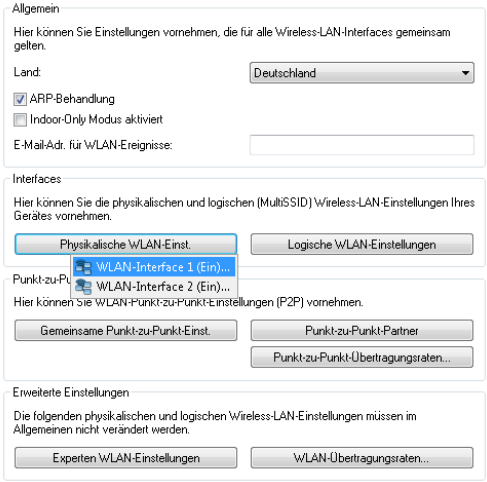
Wählen Sie die Länge und das Format (ASCII oder HEX) der Schlüssel immer nach den Möglichkeiten der Funknetzwerkkarten aus, die sich in Ihrem WLAN anmelden sollen. Wenn Sie im AP eine Verschlüsselung nach WEP 152 eingestellt haben, können manche Clients sich nicht mehr in diesem WLAN anmelden, weil sie die entsprechende Schlüssellänge nicht unterstützen.

Passwortfeld-Schutz für WLAN-Schlüssel

Ab HiLCOS 8.90 stellt das System WPA- sowie WEP-Gruppen-Schlüssel an der Konsole nicht mehr im Klartext, sondern als Passworteingabe dar (********). In Folge dessen ist es nicht mehr möglich, diese Schlüssel z. B. per SNMP auszulesen.

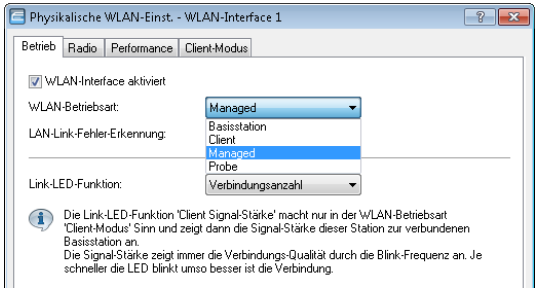
12.6.5 Die physikalischen WLAN-Schnittstellen

Neben den allgemeinen WLAN-Parametern gelten eine Reihe von Einstellungen für jedes WLAN-Modul des APs speziell.



Betriebseinstellungen

Hier finden Sie die Betriebseinstellungen.



LANconfig: Wireless LAN / Allgemein / Physikalische WLAN-Einstellungen / Betrieb

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Betriebs-Einstellungen

- WLAN-Betriebsart

  Hirschmann APs können grundsätzlich in verschiedenen Betriebsarten arbeiten:

- Als Basisstation (AP) stellt es für die WLAN-Clients die Verbindung zu einem kabelgebundenen LAN her.
- Als Client sucht das Gerät selbst die Verbindung zu einem anderen AP und versucht sich in einem Funknetzwerk anzumelden. In diesem Fall dient das Gerät also dazu, ein kabelgebundenes Gerät über eine Funkstrecke an eine Basisstation anzubinden.
- Als Managed-AP sucht das Gerät einen zentralen WLC, von dem es eine Konfiguration beziehen kann.
- In der Betriebsart 'Probe' sammelt das Gerät nur WLAN-Informationen z. B. für einen integrierten Spektrum-Analyser.

Wenn das WLAN-Interface nicht benötigt wird, kann es vollständig deaktiviert werden.

▶ Link-LED-Funktion

Bei der Einrichtung von Point-to-Point-Verbindungen oder in der Betriebsart als WLAN-Client ist es für eine möglichst gute Positionierung der Antennen wichtig, die Empfangsstärke in verschiedenen Positionen zu erkennen. Die WLAN-Link-LED kann z. B. für die Phase der Einrichtung zur Anzeige der Empfangsqualität genutzt werden. In der entsprechenden Betriebsart blinkt die WLAN-Link-LED umso schneller, je besser die Empfangsqualität in der jeweiligen Antennenposition ist.

- Verbindungsanzahl: In dieser Betriebsart zeigt die LED mit einem „inversen Blitzen“ die Anzahl der WLAN-Clients an, die bei dem AP als Client eingebucht sind. Nach der Anzahl der Blitzer für jeden Client erfolgt eine kurze Pause. Wählen Sie diese Betriebsart dann, wenn Sie das Gerät als Basisstation betreiben.
- Client-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des APs an, bei dem ein AP selbst als Client eingebucht ist. Je schneller die LED blinkt, umso besser ist das Signal. Wählen Sie diese Betriebsart nur, wenn Sie den AP im Client-Modus betreiben.
- P2P1- bis P2Px-Signalstärke: In dieser Betriebsart zeigt die LED die Signalstärke des jeweiligen P2P-Partners, mit dem ein AP eine P2P-Strecke bildet. Je schneller die LED blinkt, umso besser ist das Signal.

Broken-Link-Detection

Wenn ein AP keine Verbindung zum kabelgebundenen LAN hat, kann er in den meisten Fällen seine wesentliche Aufgabe – den eingebuchten WLAN-

Clients einen Zugang zum LAN zu ermöglichen – nicht mehr erfüllen. Mit der Funktion der Broken-Link-Detection (Link-Fehler-Erkennung) können die WLAN-Module eines Geräts deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim AP eingebuchten Clients einen anderen AP (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden.

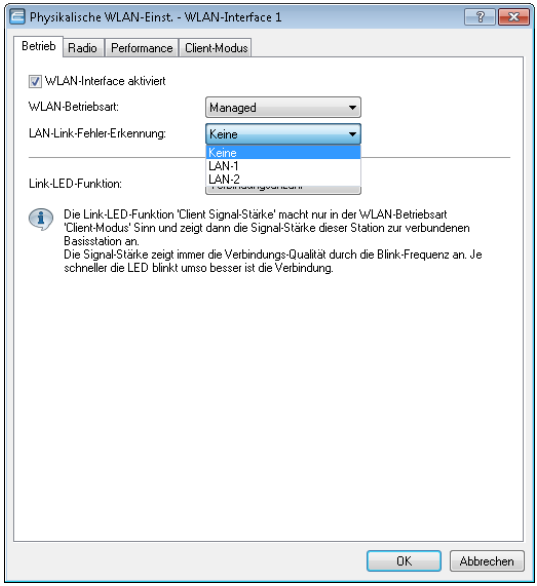
Bis zur HiLCOS-Version 7.80 bezog sich die Aktivierung der Link-Fehler-Erkennung immer auf LAN-1, auch wenn das Gerät über mehrere LAN-Interfaces verfügte. Außerdem wirkte sich die Deaktivierung auf alle verfügbaren WLAN-Module des Gerätes aus.

Ab HiLCOS-Version 8.00 kann die Link-Fehler-Erkennung gezielt an ein bestimmtes LAN-Interface gebunden werden.

Die Einstellung für die Link-Fehler-Erkennung finden Sie auf folgenden Pfaden:

LANconfig: Wireless-LAN / Allgemein / Physikalische WLAN-Einst. / Betrieb

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Betriebs-Einstellungen



▶ LAN-Link-Fehler-Erkennung

Mit dieser Funktion werden die WLAN-Module des Geräts deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

Mögliche Werte:

- Nein: Link-Fehler-Erkennung wird nicht genutzt.
- LAN-1 bis LAN-n (je nach verfügbaren LAN-Interfaces im Gerät): Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

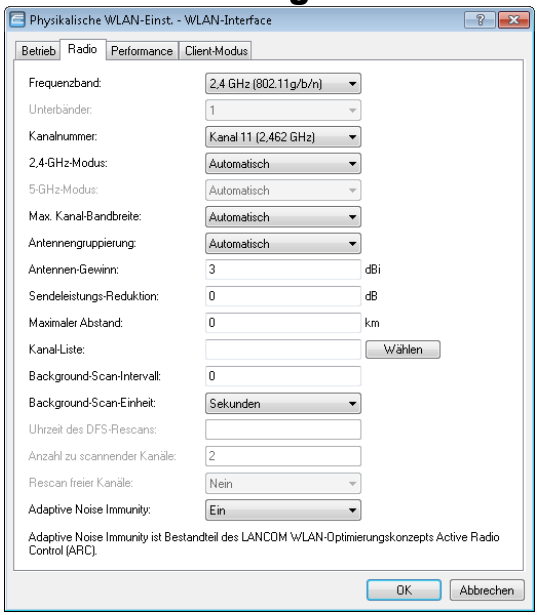
Default:

- Nein

Hinweis: Die Interface-Bezeichnungen LAN-1 bis LAN-n repräsentieren die logischen LAN-Schnittstellen. Die verfügbaren physikalischen Ethernet-Ports des Geräts müssen zur Nutzung dieser Funktion ggf. auf die entsprechenden Werte LAN-1 bis LAN-n eingestellt werden.

Hinweis: Die Link-Fehler-Erkennung kann auch für WLAN-Geräte in der Betriebsart als WLAN-Client genutzt werden. Bei eingeschalteter Link-Fehler-Erkennung werden die WLAN-Module eines WLAN-Clients nur dann aktiviert, wenn die entsprechenden LAN-Schnittstellen eine Verbindung zum kabelgebunden LAN haben.

Radio-Einstellungen



Frequenzband, Unterbänder

Mit der Auswahl des Frequenzbandes auf der Registerkarte **Radio** bei den Einstellungen für die physikalischen Interfaces legen Sie fest, ob das WLAN-Modul im 2,4 GHz- oder im 5 GHz-Band arbeitet, und damit gleichzeitig die möglichen Funkkanäle.

Im 5 GHz-Band kann außerdem ein Unterband gewählt werden, an das wiederum bestimmte Funkkanäle und maximale Sendeleistungen geknüpft sind.

Hinweis: In einigen Ländern ist das DFS-Verfahren mit automatischer Kanalsuche vorgeschrieben. Mit der Wahl des Unterbands wird damit auch der Bereich der Funkkanäle festgelegt, die für die automatische Kanalauswahl verwendet werden kann.

Kanalnummer

Hier bestimmen Sie den Kanal für die Datenübertragung im Funktnetz.

Hinweis: Im 2,4 GHz-Band müssen zwei getrennte Funknetze mindestens drei Kanäle auseinander liegen, um Störungen zu vermeiden.

2,4-GHz-Modus / 5-GHz-Modus

Geben Sie an, welche(n) Funkstandard(s) die von Ihnen konfigurierte physikalische WLAN-Schnittstelle gegenüber einem WLAN-Client unterstützt.

Sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband existieren inzwischen unterschiedliche Funk-Standards, nach denen ein AP senden kann. Im 2,4-GHz-Frequenzband umfasst dies bislang die Standards IEEE 802.11b, IEEE 802.11g und IEEE 802.11n; im 5-GHz-Frequenzband die Standards IEEE 802.11a, IEEE 802.11n und IEEE 802.11ac. Je nach Gerätetyp und gewähltem Frequenzband haben Sie die Möglichkeit, einen AP exklusiv in einem bestimmten Modus zu betreiben oder einen der verschiedenen Kompatibilitätsmodi einzustellen.

Wichtig: Beachten Sie, dass WLAN-Clients, die lediglich einen langsameren Standard unterstützen, sich nicht mehr in Ihrem WLAN anmelden können, wenn Sie den Modus auf einen zu hohen Wert einstellen. Die Kompatibilität geht jedoch immer zu Lasten der Performance. Erlauben Sie daher ausschließlich jene Betriebsarten, die aufgrund der vorhandenen WLAN-Clients unbedingt erforderlich sind.

Sofern sich in Ihrem WLAN z. B. ausschließlich 802.11n-fähige WLAN-Clients befinden, empfiehlt sich die Wahl des Greenfield-Modus (“Nur 802.11n”): Hierdurch unterbinden Sie die Anmeldung langsamerer Clients, welche das Netz andernfalls ausbremsen würden.

Um eine möglichst hohe Übertragungsgeschwindigkeit zu erreichen, gleichzeitig aber auch langsamere WLAN-Clients nicht auszuschließen, empfiehlt sich die Wahl eines Kompatibilitätsmodus (bei 2,4 GHz z. B. “802.11g/b/n (gemischt)”; bei 5 GHz “802.11a/n (gemischt)”). Im Kompatibilitätsmodus arbeitet eine physikalische WLAN-Schnittstelle grundsätzlich nach dem schnellsten Standard, fällt aber auf einen langsameren Standard zurück, wenn sich ein entsprechender WLAN-Client im Netz anmeldet. Im Rahmen von 802.11b können Sie dabei auswählen, ob die physikalische WLAN-Schnittstelle ausschließlich den 11-MBit-Modus oder auch den älteren 2-MBit-Modus unterstützten soll (“… (2Mbit-kompatibel)”).

Bei APs nach dem 802.11g-Standard haben Sie darüber hinaus die Möglichkeit, die Übertragungsgeschwindigkeit auf bis zu 108MBit/s zu steigern. Im sogenannten Turbo-Modus nutzt ein AP gleichzeitig zwei benachbarte freie Kanäle für die Funkübertragung. Wenn Sie einen AP in den 108Mbit/s-Turbo-Modus schalten, können ausschließlich noch diejenigen WLAN-Clients eine Verbindung zu dem AP aufbauen, welche ebenfalls im Turbo-Modus betrieben werden.

Hinweis: Der Turbo-Modus wird dem 802.11g-Standard zugeordnet, entspricht jedoch keinem offiziellen IEEE-Standard. Die Technik repräsentiert eigene Erweiterungen unterschiedlicher Chipsatz-Hersteller, die diese Technik auch unter der Bezeichnung “802.11g+” oder “802.11g++” vermarkten. Der Turbo-Modus ist daher ausschließlich auf APs mit reiner 802.11g-Hardware verfügbar.

Sofern Sie über die Einstellung “Automatisch” die Wahl des 2,4-/5-GHz-Modus dem Gerät überlassen, ist die Wahl des besten Modus vom verwendeten Frequenzband und den Fähigkeiten der Geräte-Hardware abhängig:

- Innerhalb des 2,4-GHz-Modus führt die Automatik entweder zu **802.11g/b/n (gemischt)** oder zu **802.11g/b (gemischt)**.
- Innerhalb des 5-GHz-Modus führt die Automatik entweder zu **802.11ac/a/n (gemischt)**, **802.11a/n (gemischt)** oder **54Mbit/s-Modus**.

APs nach 802.11n sind im 2,4-GHz-Frequenzband prinzipiell abwärtskompatibel zu den vorhergehenden Standards IEEE 802.11b und IEEE 802.11g. Für im 802.11b- oder 802.11g-Modus betriebene 802.11n-Hardware sind lediglich die 802.11n-spezifischen Funktionen nicht verfügbar. Im 5-GHz-Frequenzband hingegen besteht diese Abwärtskompatibilität nicht: Die betreffenden 802.11n-Geräte müssen 802.11a explizit unterstützen.

Max. Kanal-Bandbreite

Legen Sie hier fest, wie und in welchem Umfang der AP die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Folgende Werte sind möglich:

- **Automatisch**: Der AP stellt die Kanal-Bandbreite automatisch optimal ein. Dabei lässt der AP die maximal verfügbare Bandbreite zu, sofern

die momentanen Betriebsbedingungen dies erlauben. Andernfalls begrenzt der AP die Kanal-Bandbreite auf 20MHz.

- **20MHz**: Der AP benutzt auf 20MHz gebündelte Kanäle.
- **40MHz**: Der AP benutzt auf 40MHz gebündelte Kanäle.
- **80MHz**: Der AP benutzt auf 80MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Antennengruppierung

Hinweis: Nur verfügbar für 802.11n.

Hirschmann-APs mit 802.11n-Unterstützung können bis zu drei Antennen zum Senden und Empfangen der Daten einsetzen. Der Einsatz mehrerer Antennen kann bei 802.11n unterschiedliche Ziele verfolgen:

- Verbesserung des Datendurchsatzes: Mit dem Einsatz von “Spatial Multiplexing” können zwei parallele Datenströme realisiert werden, mit denen die doppelte Datenmenge übertragen werden kann.
- Verbesserung der Funk-Abdeckung: Mit dem Einsatz von “Cyclic Shift Diversity (CSD)” kann ein Funksignal in unterschiedlichen Phasenlagen gesendet werden. Damit sinkt die Gefahr, dass es an bestimmten Stellen der Funkzelle zu Auslöschungen des Signals kommt.

Je nach Anwendung kann die Nutzung der Antennen eingestellt werden:

- Beim Einsatz des Geräts im AP-Modus zur Anbindung von WLAN-Clients ist in der Regel die parallele Nutzung aller drei Antennen zu empfehlen, um eine gute Netzabdeckung zu erzielen.
- Für die Nutzung von zwei parallelen Datenströmen z. B. bei Point-to-Point-Verbindungen mit einer entsprechenden Dual-Slant-Antenne

werden die Antennen-Anschlüsse 1 + 2 **oder** 1 + 3 verwendet. Der nicht genutzte Antennen-Anschluss wird dabei jeweils deaktiviert.

- Bei Anwendungen mit nur einer Antenne (z. B. Outdoor-Anwendung mit einer Antenne) wird die Antennen an den Anschluss 1 angeschlossen, die Anschlüsse 2 und 3 werden deaktiviert.
- Mit der Einstellung “Auto” werden alle verfügbaren Antennen genutzt.

Wichtig: Bitte beachten Sie für den Anschluss der Antennen: Der Antennen-Anschluss 1 muss immer verwendet werden. Je nach Montage und Verkabelung kann für die zweiten Antenne entweder Anschluss 2 oder Anschluss 3 gewählt werden. Die softwareseitige Konfiguration des Gerätes muss dabei mit dem Anschluss der Antennenkabel übereinstimmen.

Diversity-Einstellungen

Hinweis: Nur verfügbar für 802.11abg.

Die Diversity-Einstellungen legen fest, welche Antennen zum Senden bzw. zum Empfangen verwendet werden:

- “Nur auf der primären Antenne senden” (Rx-Diversity): In dieser Standardeinstellung wird über die am Main-Anschluss des APs angeschlossene Antenne gesendet. Zum Empfangen (RX) wird die Antennen ausgewählt, die den besten Empfang hat (an Main oder AUX).
- “Automatisch die beste Antenne zum Senden selektieren” (Tx- und Rx-Diversity): Wird die Diversity-Funktion auch auf das Senden angewendet (TX), wird auch zum Senden die Antenne mit dem stärksten Signal ausgewählt.
- “Auf der primären Antennen Senden und auf der sekundären empfangen” (kein Diversity): Hierbei wird nur die Main-Antenne zum Senden verwendet, zum Empfangen bevorzugt die Antenne den AUX-Anschluss. Mit dieser Variante können Antennen mit sehr hohen Leistungen zum Empfangen eingesetzt werden, die aus rechtlichen Gründen nicht zum Senden verwendet werden dürfen.

Antennen-Gewinn / Sendeleistungs-Reduktion

Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist eine Dämpfung der Leistung auf den zulässigen Wert erforderlich.

- In das Feld **Antennen-Gewinn** wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.
- Im Gegensatz dazu reduziert der Eintrag im Feld **Sendeleistungs-Reduktion** die Leistung immer statisch um den dort eingetragenen Wert, ohne Berücksichtigung der anderen Parameter.

Hinweis: Durch die Sendeleistungs-Reduktion wird nur die abgestrahlte Leistung reduziert. Die Empfangsempfindlichkeit (der Empfangs-Antennengewinn) der Antennen bleibt davon unberührt. Mit dieser Variante können z. B. bei Funkbrücken große Entfernungen durch den Einsatz von kürzeren Kabeln überbrückt werden. Der Empfangs-Antennengewinn wird erhöht, ohne die gesetzlichen Grenzen der Sendeleistung zu übersteigen. Dadurch wird die maximal mögliche Distanz und insbesondere die erreichbare Datenübertragungsgeschwindigkeit verbessert.

Basisstations-Dichte

Mit zunehmender Dichte von APs überlagern sich die Empfangsbereiche der Antennen. Die Information über die 'Basisstations-Dichte' wird in den Beacons mitgeteilt und von älteren Agere-Clients ausgewertet.

Maximaler Abstand

Bei sehr großen Entfernungen zwischen Sender und Empfänger im Funknetz steigt die Laufzeit der Datenpakete. Ab einer bestimmten Grenze erreichen die Antworten auf die ausgesandten Pakete den Sender nicht mehr innerhalb der erlaubten Zeit. Mit der Angabe des maximalen Abstands kann die Wartezeit auf die Antworten erhöht werden. Diese Distanz wird umgerechnet in eine Laufzeit, die den Datenpakete bei der drahtlosen Kommunikation zugestanden werden soll.

Background-Scan-Intervall

Wird hier ein Wert angegeben, so sucht der AP innerhalb dieses Intervalls zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren APs ab.

- Für Geräte im AP-Modus wird die Background-Scan-Funktion üblicherweise zur Rogue AP Detection eingesetzt. Das Scan-Intervall sollte hier der Zeitspanne angepasst werden, innerhalb derer unbefugte APs erkannt werden sollen, z. B. 1 Stunde.
- Für Geräte im Client-Modus wird die Background-Scan-Funktion hingegen meist für ein besseres Roaming von mobilen WLAN-Clients genutzt. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit hierbei auf z. B. 260 Sekunden beschränkt.
- Mit einer Hintergrund-Scan-Zeit von '0' wird die Funktion des Background-Scanning ausgeschaltet.

Background-Scan-Intervall

Das Background-Scan-Intervall gibt an, in welchen zeitlichen Abständen ein AP nach fremden WLAN-Netzen in Reichweite sucht.

Mit der Zeiteinheit kann ausgewählt werden, ob der eingetragene Wert für Millisekunden, Sekunden, Minuten, Stunden oder Tage gilt, um einen möglichst anschaulichen Werte für das angestrebte Verhalten darzustellen.

Hinweis: Um Beeinträchtigungen der Datenübertragungsrate zu verhindern, beträgt das Intervall zwischen den einzelnen Kanal-Scans im AP-Modus mindestens 20 Sekunden. Kleinere Eingaben werden automatisch auf dieses Mindestintervall korrigiert. Zum Beispiel wird bei 13 zu scannenden Funkkanälen im 2.4 GHz-Band das gesamte Spektrum minimal innerhalb von 13 x 20s = 260 Sekunden einmal gescannt.

Hinweis: Das Background-Scanning kann auf eine geringere Anzahl von Kanälen beschränkt werden, wenn der Indoor-Modus aktiviert wird. Auf diese Weise kann das Roaming für mobile APs im Client-Modus noch weiter verbessert werden.

DFS-Konfiguration

Konfigurieren Sie hier die DFS-Einstellungen.

Informationen zu Dynamic Frequency Selection finden Sie unter *Dynamic Frequency Selection (DFS)*.

Adaptive Noise Immunity

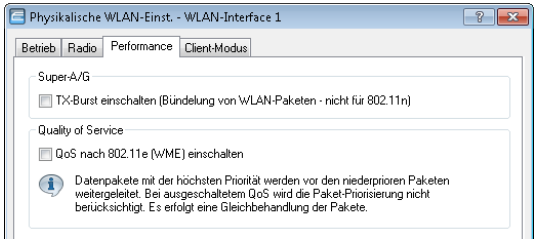
Aktivieren oder deaktivieren Sie hier die Adaptive Noise Immunity.

Informationen zu Adaptive Noise Immunity finden Sie unter *Adaptive Noise Immunity*.

Performance

LANconfig: Wireless LAN / Allgemein / Physikalische WLAN-Einstellungen / Performance

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Leistung



- TX-Burst

  Erlaubt/Verbietet das Paket-Bursting, was den Durchsatz erhöht, jedoch die Fairness auf dem Medium verschlechtert.

- Hardware-Kompression

  Erlaubt oder verbietet eine Hardwarekompression von Paketen.

- QoS nach 802.11e

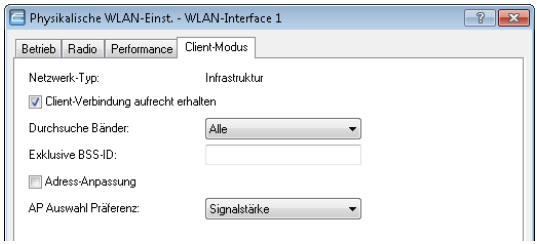
  Mit der Erweiterung der 802.11-Standards um 802.11e können auch für WLAN-Übertragungen definierte Dienstgüten angeboten werden (Quality of Service). 802.11e unterstützt u. a. eine Priorisierung von bestimmten Datenpaketen. Die Erweiterung stellt damit eine wichtige Basis für die Nutzung von Voice-Anwendungen im WLAN dar (Voice over WLAN – VoWLAN). Die Wi-Fi-Alliance zertifiziert Produkte, die Quality of Service nach 802.11e unterstützen, unter dem Namen WMM (Wi-Fi Multimedia, früher WME für Wireless Multimedia Extension). WMM definiert vier

Kategorien (Sprache, Video,Best Effort und Hintergrund) die in Form separater Warteschlangen zur Prioritätensteuerung genutzt werden. Der 802.11e-Standard nutzt Steuerung der Prioritäten die VLAN-Tags bzw. die DiffServ-Felder von IP-Paketen, wenn keine VLAN-Tags vorhanden sind. Die Verzögerungszeiten (Jitter) bleiben mit weniger als zwei Millisekunden in einem Bereich, der vom menschlichen Gehör nicht wahrgenommen wird. Zur Steuerung des Zugriffs auf das Übertragungsmedium nutzt der 802.11e-Standard die Enhanced Distributed Coordination Function (EDCF).

Hinweis: Die Steuerung der Prioritäten ist nur möglich, wenn sowohl der WLAN-Client als auch der AP den 802.11e-Standard bzw. WMM unterstützen und die Anwendungen die Datenpakete mit den entsprechenden Prioritäten kennzeichnen.

Client-Modus

Wenn das Gerät als Client betrieben wird, können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces noch weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.



LANconfig: Wireless LAN / Allgemein / Physikalische WLAN-Einstellungen / Client-Modus

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Client-Einstellungen

- Client-Verbindung aufrecht erhalten

  Mit dieser Option hält die Client-Station die Verbindung zur Basisstation aufrecht, auch wenn von den angeschlossenen Geräten keine Datenpakete

gesendet werden. Ist diese Option ausgeschaltet, wird die Clientstation automatisch aus dem Funknetzwerk abgemeldet, wenn für eine bestimmte Zeit keine Pakete über die WLAN-Verbindung fließen.

- Durchsuchte Bänder

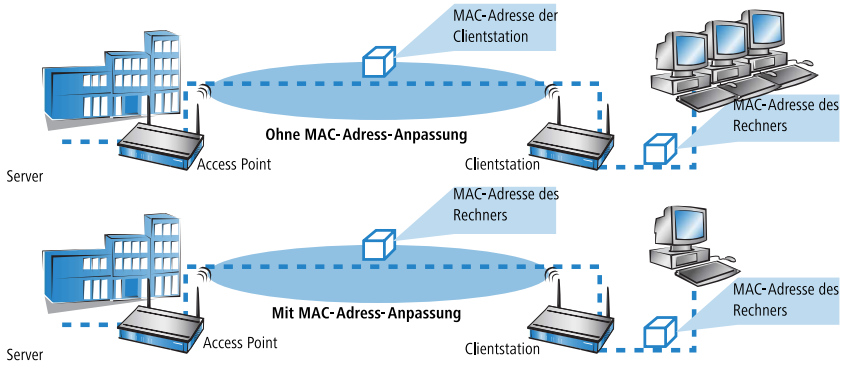
  Legen Sie hier fest, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

- Bevorzugte BSS-ID

  Wenn sich die Clientstation nur bei einem bestimmten AP einbuchen soll, können Sie hier die MAC-Adresse des WLAN-Moduls aus diesem AP eintragen.

- Adress-Anpassung

  Im Client-Modus ersetzt die Clientstation üblicherweise die MAC-Adressen in den Datenpaketen der an ihr angeschlossenen Geräte durch die eigene MAC-Adresse. Der AP auf der anderen Seite der Verbindung „sieht“ also immer nur die MAC-Adresse der Clientstation, nicht jedoch die MAC-Adresse der oder des angeschlossenen Rechners.



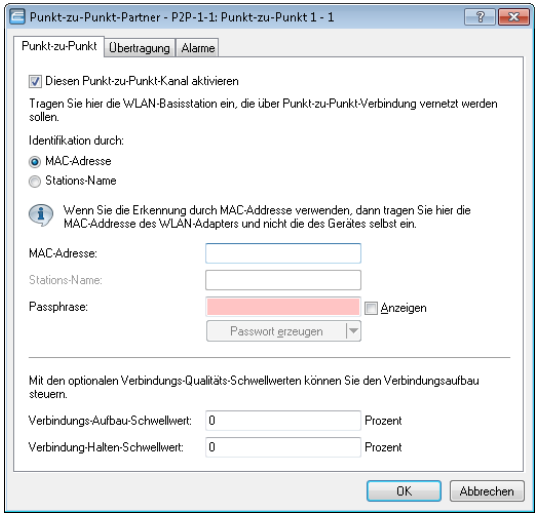
In manchen Installationen ist es jedoch gewünscht, dass die MAC-Adresse eines Rechners und nicht die der Clientstation an den AP übertragen wird. Mit der Option 'Adress-Anpassung' wird das Ersetzen der MAC-Adresse durch die Clientstation unterbunden, die Datenpakete werden mit der ori-

ginalen MAC-Adresse übertragen – der AP übernimmt im WLAN die MAC-Adresse des Clients.

Hinweis: Die Adress-Anpassung funktioniert nur, wenn an die Clientstation nur **ein** Rechner angeschlossen ist!

12.6.6 Die Punkt-zu-Punkt-Partner

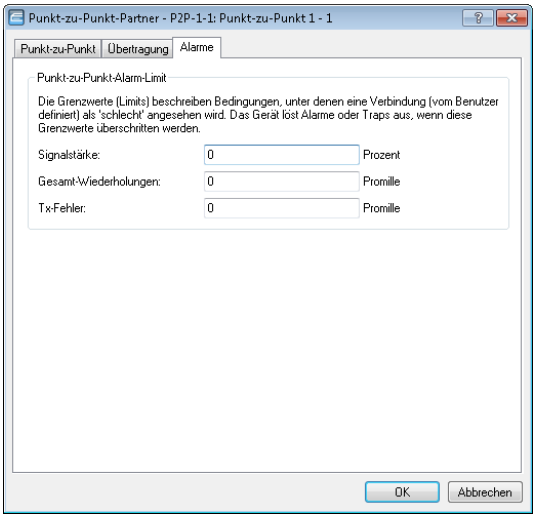
Für jedes WLAN-Modul sind bis zu 16 Punkt-zu-Punkt-Verbindungen aktivierbar. In LANconfig finden Sie diese Einstellungen unter **Wireless-LAN** > **Allgemein** > **Punkt-zu-Punkt** > **Punkt-zu-Punkt-Partner**



Für die Einrichtung einer Punkt-zu-Punkt-Verbindung gehen Sie wie folgt vor:

1. Markieren Sie die Option **Diesen Punkt-zu-Punkt-Kanal aktivieren**.
2. Wählen Sie, ob Sie die P2P-Gegenstelle anhand ihrer **MAC-Adresse** oder ihres **Stations-Namens** identifizieren.
3. Das entsprechende Textfeld wird aktiviert. Geben Sie die MAC-Adresse oder den Stations-Namen ein.

Hinweis: Wenn Sie die Erkennung durch MAC-Addresse verwenden, dann tragen Sie hier die MAC-Addresse des WLAN-Moduls und nicht die des Gerätes selbst ein.

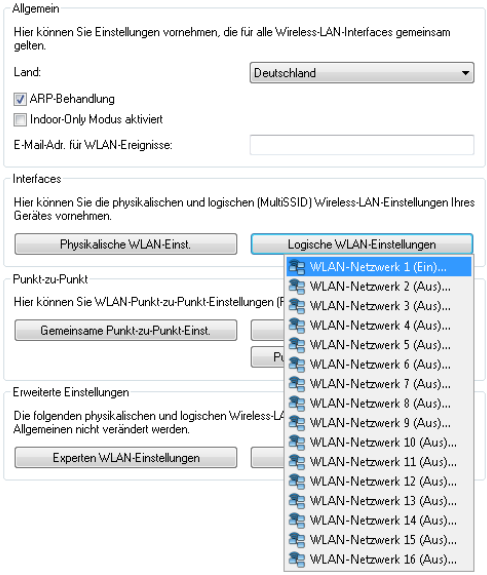


Auf dem Reiter **Alarm** sind Grenzwerte für **Signalstärke**, **Gesamtwiederholungen** und **Tx-Fehler** der Punkt-zu-Punkt-Verbindung definierbar. Bei deren Über-oder Unterschreitung löst der AP Alarme oder Traps aus.

Schließen Sie Ihre Eingaben mit einem Klick auf **OK** ab.

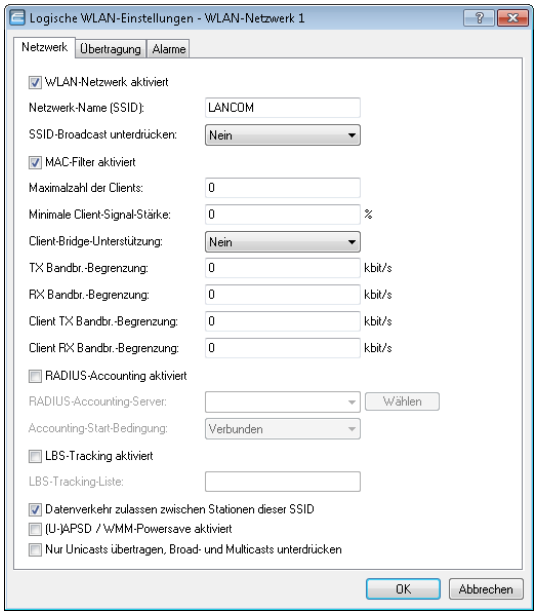
12.6.7 Die logischen WLAN-Schnittstellen

Jede physikalische WLAN-Schnittstelle kann bis zu 16 verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche APs benötigt werden.



Netzwerkeinstellungen

Die nachfolgenden Einstellungen nehmen Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** vor.



WLAN-Netzwerk aktiviert

Mit diesem Schalter aktivieren bzw. deaktivieren Sie das entsprechende logische WLAN.

Netzwerk-Name (SSID)

Bestimmen Sie für jedes benötigte logische Funknetzwerk eine eindeutige SSID (den Netzwerknamen). Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

SSID-Broadcast unterdrücken

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.
- **Verschärft**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.

Wichtig: Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

MAC-Filter aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **Stationen**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

Hinweis: Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase über LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase beachtet der AP daher immer die MAC-Filterliste, auch wenn Sie diese Option hier deaktivieren.

Maximale Client-Anzahl

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der AP ab.

Minimale Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren APs, da keine APs aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

Client-Bridge-Unterstützung

Aktivieren Sie diese Option für einen AP, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

Hinweis: Sie können den Client-Bridge-Modus ausschließlich zwischen zwei OpenBAT-Geräten verwenden.

Client-Bridge-Roaming-Unterstützung

Die Client-Bridge-Roaming-Unterstützung verbessert die Zuverlässigkeit und Latenz des Roaming-Vorganges. Sie ist in Situationen nützlich, in denen viele Geräte am LAN des Clients angebunden sind, insbesondere mit Downstream-Datenverkehr. Mit Downstream-Verkehr ist Datenverkehr gemeint, der von den APs durch den Client zu den angebundenen Geräten fließt. Das Aktivieren dieser Funktion auf den APs erlaubt den direkten Informationsaustausch zwischen den APs über die an den Client angebundenen Geräte. Das Aktivieren dieser Funktion auf dem Client entlastet zusätzlich den WLAN-Kanal nach dem Roaming, was die Roaming-Zeit reduziert. Wenn die Client-Bridge-Roaming-Unterstützung auf dem Client aktiviert ist, überprüft dieser bei jedem Roaming ob diese Verbesserung möglich ist. Ist keine Verbesserung möglich, greift der Client auf das Standard-Verhalten zurück.

TX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

RX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID (Limit in kBit/s). Der Wert `0` deaktiviert die Begrenzung.

Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

RADIUS-Accounting aktiviert

Aktivieren Sie die Option, um RADIUS-Accounting für diese SSID einzuschalten.

RADIUS-Accounting-Server

Geben Sie einen RADIUS-Accounting-Server für die betreffende SSID an. Die hier auswählbaren Server definieren Sie in der Tabelle **Wireless-LAN** > **Stationen** > **RADIUS-Accounting-Server**.

Accounting-Start-Bedingung

Im Normalfall sendet der WLAN-Stack eine RADIUS-Accounting-Start-Nachricht, sobald der WLAN-Client verbunden ist. Vielfach hat der WLAN-Client zu diesem Zeitpunkt noch keine IP-Adresse, weil sie u. U. vom DHCP-Server noch nicht zur Verfügung gestellt wurde. Das Attribut `Framed-IP-Address` innerhalb der RADIUS-Accounting-Nachricht kann somit nicht sinnvoll befüllt werden.

Verbunden

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client in den Status “Verbunden” wechselt. Diese Einstellung ist als Standardwert definiert.

Gültige IP-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IP-Adresse erhält (IPv4 oder IPv6).

Gültige IPv4-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv4-Adresse erhält.

Gültige IPv6-Adresse

Das Accounting beginnt mit dem Moment, in dem der WLAN-Client eine gültige IPv6-Adresse erhält.

Hinweis: APIPA-Adressen (`169.254.1.0` bis `169.254.254.255` sowie `fe80:`) werden nicht als gültige IP-Adressen anerkannt.

LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Hinweis: Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Datenverkehr zulassen zwischen Stationen dieser SSID

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

(U-)APSD / WMM-Powersave aktiviert

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen AP in den Energiesparmodus um. Erhält der AP nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert.

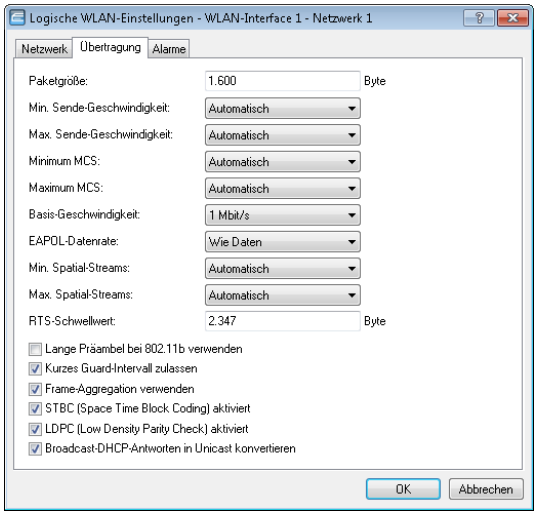
Nur Unicasts übertragen, Broad- und Multicasts unterdrücken

Multi- und Broadcast-Sendungen innerhalb einer WLAN-Funkzelle bedeuten eine Belastung für die Bandbreite dieser Funkzelle, zumal die WLAN-Clients mit diesen Sendungen oft nichts anfangen können. Der AP fängt durch ARP-Spoofing bereits einen Großteil der Multi- und Broadcast-Sendungen in die Funkzelle ab. Mit der Beschränkung auf Unicast-Sendungen filtert er z. B. überflüssige IPv4-Broadcasts wie Bonjour oder NetBIOS aus den Anfragen heraus.

Die Unterdrückung von Multi- und Broadcast-Sendungen ist zudem eine Forderung der HotSpot-2.0-Spezifikation.

Einstellungen für die Übertragung

Die Details für die Datenübertragung auf dem logischen Interface stellen Sie auf der Registerkarte **Übertragung** ein.



Paketgröße

Bei kleinen Datenpaketen ist die Gefahr für Übertragungsfehler geringer als bei großen Paketen, allerdings steigt auch der Anteil der Header-Informationen am Datenverkehr, die effektive Nutzlast sinkt also. Erhöhen Sie den voreingestellten Wert nur, wenn das Funknetzwerk überwiegend frei von Störungen ist und nur wenig Übertragungsfehler auftreten. Reduzieren Sie den Wert entsprechend, um die Übertragungsfehler zu vermeiden.

Minimale und maximale Geschwindigkeit

Der AP handelt mit den angeschlossenen WLAN-Clients die Geschwindigkeit für die Datenübertragung normalerweise fortlaufend dynamisch aus. Dabei passt der AP die Übertragungsgeschwindigkeit an die Empfangslage an. Alternativ können Sie hier die minimalen und maximalen Übertragungsgeschwindigkeiten fest vorgeben, wenn Sie die dynamische Geschwindigkeitsanpassung verhindern wollen.

Modulation Coding Scheme (MCS) (Nur verfügbar für 802.11n)

Eine bestimmte MCS-Nummer bezeichnet eine eindeutige Kombination aus Modulation der Einzelträger (BPSK, QPSK, 16QAM, 64QAM), Coding-Rate (d. h. Anteil der Fehlerkorrekturbits an den Rohdaten) und Anzahl der Spatial Streams. 802.11n verwendet diesen Begriff anstelle „Datenrate“

bei älteren WLAN-Standards, weil die Rate keine eindeutige Beschreibung mehr ist.

MCS-Index	*Datenströme*	*Modulation*	*Coding-Rate*	*Datendurchsatz (GI=0,4 µs, 40 MHz)*
0	1	BPSK	1/2	15
1	1	QPSK	1/2	30
2	1	QPSK	3/4	45
3	1	16QAM	1/2	60
4	1	16QAM	3/4	90
5	1	64QAM	1/2	120
6	1	64QAM	3/4	135
7	1	64QAM	5/6	150
8	2	BPSK	1/2	30
9	2	QPSK	1/2	60
10	2	QPSK	3/4	90
11	2	16QAM	1/2	120
12	2	16QAM	3/4	180
13	2	64QAM	1/2	240
14	2	64QAM	3/4	270
15	2	64QAM	5/6	300

Die Auswahl des MCS gibt also an, welche Modulationsparameter bei einem oder zwei Spatial-Datenströmen minimal bzw. maximal verwendet werden sollen. Innerhalb dieser Grenzen wird das passende MCS je nach den vorliegenden Bedingungen beim Verbindungsaufbau gewählt und während der Verbindung bei Bedarf angepasst. Damit wird auch der maximal erreichbare Datendurchsatz definiert, der in der letzten Spalte der Tabelle angegeben ist (hier für das kurze Guard-Intervall GI = 0,4 µs mit Nutzung des 40 MHz-Kanals).

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der AP die

Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

EAPOL-Datenrate (EAP over LAN)

WLAN-Clients nutzen EAPOL zur Anmeldung an APs über WPA und 802.1x. Dazu kapseln sie die EAP-Pakete zum Austausch der Authentifizierungs-Informationen in Ethernet-Frames, um die EAP-Kommunikation über eine Layer-2-Verbindung zu ermöglichen

In manchen Fällen ist es sinnvoll, die Datenrate für die Übertragung der EAPOL-Pakete niedriger zu wählen als die Datenrate für die Nutzdaten. Bei beweglichen WLAN-Clients kann z. B. eine zu hohe Datenrate der EAPOL-Pakete zu Paketverlusten führen und so den Anmeldevorgang deutlich verzögern. Durch die gezielte Auswahl der EAPOL-Datenrate verläuft dieser Vorgang stabiler.

Die Standard-Auswahl "Wie Daten" behandelt EAPOL-Pakete wie normale Datenpakete und wählt die für Datenpakete übliche Übertragungsrate bzw. aktiviert die für Datenpakete übliche Ratenadaption.

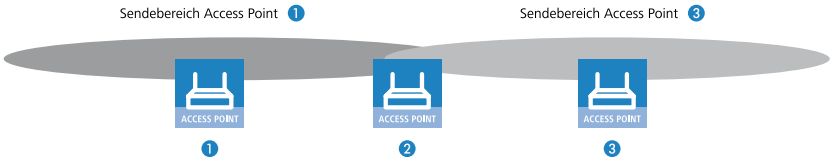
Anzahl Spatial-Streams (Nur verfügbar für 802.11n)

Mit der Funktion des Spatial-Multiplexing können mehrere separate Datenströme über separate Antennen übertragen werden, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

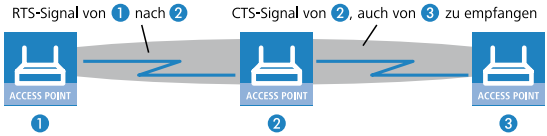
Hinweis: Mit der Einstellung 'Auto' werden alle Spatial-Streams genutzt, die von dem jeweiligen WLAN-Modul unterstützt werden.

RTS-Schwellwert

Mit dem RTS-Schwellwert wird das Phänomen der „Hidden-Station“ vermieden.



Dabei sind drei APs **1**, **2**, und **3** so positioniert, dass zwischen den beiden äußeren Geräten keine direkte Funkverbindung mehr möglich ist. Wenn nun **1** ein Paket an **2** sendet, bemerkt **3** diesen Vorgang nicht, da er außerhalb des Sendebereichs von **1** steht. **3** sendet also möglicherweise während der laufenden Übertragung von **1** ebenfalls ein Paket an **2**, denn **3** hält das Medium (in diesem Falle die Funkverbindung) für frei. Es kommt zur Kollision, keine der beiden Übertragungen von **1** oder **3** nach **2** ist erfolgreich. Um diese Kollisionen zu vermeiden, wird das RTS/CTS-Protokoll eingesetzt.



Dazu schickt **1** vor der eigentlichen Übertragung ein RTS-Paket an **2**, das **2** mit einem CTS beantwortet. Das von **2** ausgestrahlte CTS ist jetzt aber in „Hörweite“ von **3**, so dass **3** mit seinem Paket an **2** warten kann. Die RTS- und CTS-Signale beinhalten jeweils eine Zeitangabe, wie lange die folgende Übertragung dauern wird.

Eine Kollision bei den recht kurzen RTS-Paketen ist sehr unwahrscheinlich, die Verwendung von RTS/CTS erhöht aber dennoch den Overhead. Der Einsatz dieses Verfahrens lohnt sich daher nur für längere Datenpakete, bei denen Kollisionen wahrscheinlich sind. Mit dem RTS-Schwellwert wird eingestellt, ab welcher Paketlänge das RTS/CTS eingesetzt werden soll. Der passende Wert ist in der jeweiligen Umgebung im Versuch zu ermitteln.

Hinweis: Der RTS/CTS-Schwellwert muss auch in den WLAN-Clients entsprechend den Möglichkeiten des Treibers bzw. des Betriebssystems eingestellt werden.

Lange Präambel bei 802.11b

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die „lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

Kurzes Guard-Interval zulassen (Nur verfügbar für 802.11n)

Mit dieser Option wird die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval) reduziert. Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite wird das WLAN-System anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden (Nur verfügbar für 802.11n)

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Durch dieses Verfahren kann der Overhead der Pakete reduziert werden, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert (Nur verfügbar für 802.11n.)

STBC ist ein Kodierverfahren nach IEEE 802.11n. Das STBC kodiert einen Datenstrom zur Übertragung in Datenblöcke, so dass es in einem MIMO-System zu besseren Empfangsbedingungen kommt.

LDPC (Low Density Parity Check) aktiviert (Nur verfügbar für 802.11n.)

LDPC ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standard-Methode zur Fehlerkorrektur Convolution Coding (CC) und optional den effektiveren LDPC.

Broadcast-DHCP-Antworten in Unicast konvertieren

Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

Hinweis: Diese Funktion ist bereits integraler Bestandteil der Einstellung **Nur Unicasts übertragen, Broad und Multicasts unterdrücken** und muss dafür nicht explizit aktiviert werden.

Hard-Retries (Nur im WEBconfig)

Dieser Wert gibt an, wie oft die Hardware versuchen soll, Pakete zu verschicken, bevor sie als Tx-Fehler gemeldet werden. Kleinere Werte ermöglichen es so, dass ein nicht zu versendendes Paket den Sender weniger lange blockiert.

Soft-Retries (Nur mit WEBconfig)

Wenn ein Paket von der Hardware nicht verschickt werden konnte, wird mit der Anzahl der Soft-Retries festgelegt, wie oft der gesamte Sendeversuch wiederholt werden soll.

Die Gesamtzahl der Versuche ist also (Soft-Retries + 1) * Hard-Retries.

Der Vorteil von Soft-Retries auf Kosten von Hard-Retries ist, dass aufgrund des Raten-Adaptionalgorithmus die nächste Serie von Hard-Retries direkt mit einer niedrigeren Rate beginnt.

12.6.8 Konfigurierbare Datenraten je WLAN-Modul

Um in Anwendungsszenarien bestimmte Datenraten auszuschließen (z. B. bei ungünstigen Umgebungsbedingungen), ist es möglich, die Datenraten pro SSID oder P2P-Strecke genau nach den speziellen Anforderungen zu konfigurieren.

Wichtig: In den meisten Anwendungsfällen sind keine Änderungen an den Standard-Einstellungen notwendig. Stellen Sie sicher, dass nur WLAN-Experten diese Einstellungen ändern, da unsachgemäße Änderungen zu Problemen im WLAN-Netzwerk führen können.

Die Konfiguration von Datenraten je WLAN-Modul legt fest, welche Datenraten der AP zur Kommunikation mit Clients verwendet (Tx) und welche Datenraten der AP dem Client “ankündigt”, die dieser zur Kommunikation mit dem AP verwenden soll oder darf (Rx).

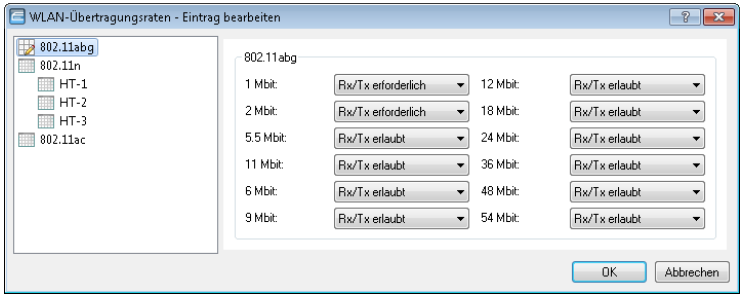
Die Ratenadaption richtet sich entsprechend nicht nur nach einer minimalen und einer maximalen Datenrate, sondern der AP verwendet auch deaktivierte Datenraten innerhalb dieser Grenzwerte nicht mehr.

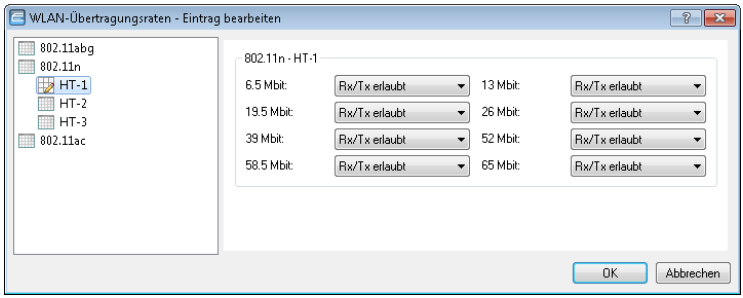
Hinweis: Die Konfiguration von Datenraten ist nur bei Stand-Alone-APs möglich. Für den Einsatz in WLC-Szenarien sind entsprechende Skripte notwendig, die der WLC an die APs ausrollt.

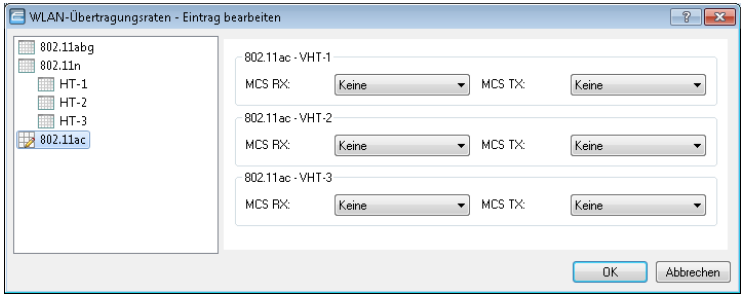
Konfiguration der Datenraten über LANconfig

Um die Datenraten mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** und öffnen Sie im Abschnitt **Erweiterte Einstellungen** den Dialog **WLAN-Übertragungsraten**. LANconfig listet die Einstellungen aller verfügbaren Schnittstellen auf. Um die Einstellung für eine Schnittstelle zu ändern, markieren Sie die entsprechende Schnittstelle und klicken Sie auf **Bearbeiten**.

Wählen Sie links den zu konfigurierenden Standard aus.







Die Konfiguration ist separat möglich für die Standards

- 802.11abg
- 802.11n
  - HT-1
  - HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Je nach Standard sind für jede Übertragungsrate je SSID und P2P-Strecke explizit die folgenden Einstellungen verfügbar:

Rx/Tx erforderlich

Der AP kündigt dem Client die Rate als “unterstützt” und “erforderlich” in Beacons und Probe Responses an und nutzt sie selber auch zur Kommu-

nikation mit dem Client. Unterstützt der Client die entsprechende Rate nicht, nimmt der AP ihn bei einer Verbindungsanfrage nicht an.

Rx/Tx erlaubt

Der AP kündigt dem Client die Rate als “unterstützt” an und nutzt sie selber auch zur Kommunikation mit dem Client. Der AP akzeptiert jedoch auch Anfragen von Clients, die die entsprechende Rate nicht unterstützen.

Rx erforderlich

Der AP kündigt dem Client die Rate als “unterstützt” und “erforderlich” an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Rx erlaubt

Der AP kündigt dem Client die Rate als “unterstützt” an, nutzt sie aber selber nicht zur Kommunikation mit dem Client.

Deaktiviert

Der AP kündigt diese Rate nicht an und verwendet sie nicht zur Kommunikation mit dem Client.

MCS-9/8/7

Bei 802.11ac-Modulen ist für die Datenraten lediglich pro Stream-Variante (1, 2 oder 3 Streams) die maximale MCS auswählbar.

Keine

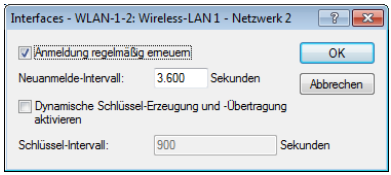
Bei 802.11ac-Modulen ist die jeweilige Stream-Variante für die entsprechende Datenrichtung deaktiviert.

12.6.9 IEEE 802.1x/EAP

Der internationale Industrie-Standard IEEE 802.1x und das Extensible **A**uthentication **P**rotocol (EAP) ermöglichen Basis-Stationen die Durchführung einer zuverlässigen und sicheren Zugangskontrolle. Die Zugangsdaten können zentral auf einem RADIUS-Server verwaltet und von der Basis-Station bei Bedarf von dort abgerufen werden.

Diese Technologie ermöglicht außerdem den gesicherten Versand und den regelmäßigen automatischen Wechsel von WEP Schlüsseln. Auf diese Weise verbessert IEEE 802.1x die Sicherungswirkung von WEP.

Ab Windows XP ist die IEEE-802.1x-Technologie bereits fest integriert. Für andere Betriebssysteme existiert Client-Software.



LANconfig: **Wireless-LAN** > **Allgemein** > **802.1X**

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **IEEE802.1x**

- Anmeldung regelmäßig erneuern

  Hier aktivieren Sie die regelmäßige Neuanmeldung. Wird eine Neuanmeldung gestartet, so bleibt der Benutzer während der Verhandlung weiterhin angemeldet. Ein typischer Standardwert für das Neuanmelde-Intervall ist 3.600 Sekunden.

- Neuanmelde-Intervall

  Intervall für die regelmäßige Neuanmeldung.

- Dynamische Schlüssel-Erzeugung und Übertragung aktivieren

  Hier aktivieren Sie die regelmäßige Erzeugung dynamischer WEP-Schlüssel und deren Übertragung.

- Schlüssel-Intervall

  Intervall für die regelmäßige Erzeugung der Schlüssel.

12.6.10 Spezielle Datenrate für EAPOL-Pakete

EAP over LAN (EAPOL) wird zur Anmeldung über WPA und/oder 802.1x von WLAN-Clients an APs verwendet. Dabei werden die EAP-Pakete zum Austausch der Authentisierungsinformationen in Ethernetframes gekapselt, um die EAP-Kommunikation über eine Layer-2 Verbindung zu ermöglichen.

In manchen Fällen ist es sinnvoll, die Datenrate für die Übertragung der EAPOL-Pakete niedriger zu wählen als die Datenrate für die Nutzdaten. Bei bewegten WLAN-Clients kann z. B. eine zu hohe Datenrate der EAPOL-Pakete zu Paketverlusten führen und so den Anmeldevorgang deutlich verzö-

gern. Durch die gezielte Auswahl der EAPOL-Datenrate kann dieser Vorgang stabilisiert werden.

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Übertragung

- **EAPOL-Rate**

  Legen Sie hier die Datenrate für die Übertragung der EAPOL-Pakete fest.

  Mögliche Werte:

  – Wie-Daten, Auswahl aus den angebotenen Geschwindigkeiten

  Default:

  – Wie-Daten

  Besondere Werte:

  – Wie-Daten überträgt die EAPOL-Daten mit der gleichen Datenrate wie die Nutzdaten.

12.6.11 Rausch-Offsets

Die Funkmodule der WLAN-Geräte können Rausch- und Signalpegel als absolute Werte (in dBm) angeben. Die Empfangsteile sind jedoch ab Werk nicht kalibriert. Um die Genauigkeit der Angaben für Rausch- und Signalpegel zu optimieren, können in der Rausch-Offset-Tabelle abhängig von Funkband (2,4/5 GHz), Kanal und WLAN-Schnittstelle Korrekturwerte (in dB) angegeben werden, die zu den von den Funkmodulen gelieferten Werten für Rausch- und Signalpegel addiert werden.

WEBconfig: HiLCOS-Menübaum / Setup / WLAN / Rausch-Offsets

- **Band**

  Frequenzband, für das der Rausch-Offset-Wert angegeben wird.

  Mögliche Werte:

  – 2,4 oder 5 GHz

  Default:

  – 2,4 GHz

- **Kanal**

Kanal, für den der Rausch-Offset-Wert angegeben wird.

Mögliche Werte:

– Gültige Kanalbezeichnung für das gewählte Frequenzband, maximal 5 Zeichen

Default:

– leer

▶ **Schnittstelle**

Physikalische WLAN-Schnittstelle, für die der Rausch-Offset-Wert angegeben wird.

Mögliche Werte:

– Auswahl aus der Liste der möglichen WLAN-Interfaces.

Default:

– WLAN-1

▶ **Wert**

Rausch-Offset-Wert in dB, der zu den vom Funkmodul übermittelten Werten addiert wird.

Mögliche Werte:

– Maximal 4 Ziffern.

Default:

– leer

Hinweis: Die Ermittlung der geeigneten Offset-Werte mit einem entsprechenden Meßaufbau obliegt dem Betreiber der WLAN-Geräte. Die Werte können durch produktionsbedingte Streuungen, Alterung und Umwelteinflüsse schwanken und müssen je nach Gerät einzeln ermittelt sowie ggf. regelmäßig überprüft werden, sofern der Bedarf für die exakten Signalpegel-Angaben dies rechtfertigt. Hirschmann liefert nur für einige Modelle Standard-Werte. Aufgrund der genannten Schwankungen übernimmt Hirschmann keine Gewähr für die Genauigkeit dieser Werte.

12.6.12 APSD – Automatic Power Save Delivery

Einleitung

Beim Automatic Power Save Delivery (APSD) handelt es sich um eine Erweiterung des Standards IEEE 802.11e. APSD wird in zwei Varianten angeboten:

- Unscheduled APSD (U-APSD)
- Scheduled APSD (S-APSD)

Die beiden Verfahren unterscheiden sich u.a. in der Nutzung der Übertragungskanäle. HirschmannAPs unterstützen U-APSD, auf dem auch das von der WiFi als WMM Power Save oder kurz WMMPS zertifizierte Verfahren basiert.

U-APSD ermöglicht für WLAN-Geräte eine deutliche Stromeinsparung. Ein besonders großer Bedarf für diese Funktion entsteht durch die immer stärkere Nutzung von WLAN-fähigen Telefonen (Voice over WLAN – VoWLAN).

Mit der Aktivierung des U-APSD für ein WLAN können die WLAN-Geräte im Gesprächsbetrieb in einen “Schlummer-Modus” wechseln, während sie auf das nächste Datenpaket warten. Die VoIP-Datenübertragung erfolgt in einem festen zeitlichen Raster – die WLAN-Geräte synchronisieren ihre aktiven Phasen mit diesem Zyklus, so dass sie rechtzeitig vor dem Empfang des nächsten Pakets wieder bereit sind. Der Stromverbrauch wird dadurch deutlich reduziert, die Gesprächszeit der Akkus wird merklich erhöht.

Das genaue Verhalten des Stromsparmodus wird zwischen AP und WLAN-Client ausgehandelt und wird dabei auf die spezifische Anwendung hin optimiert. APSD ist damit deutlich flexibler als das zuvor verwendete Stromsparverfahren, das in diesem Zusammenhang als “Legacy Power Save” bezeichnet wird.

Konfiguration

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Netzwerk

- APSD

  Aktiviert den Stromsparmodus APSD für dieses logische WLAN-Netzwerk.

  Mögliche Werte:

– Ein, Aus

Default:

– Aus

Hinweis: Bitte beachten Sie, dass zur Nutzung der Funktion APSD in einem logischen WLAN auf dem Gerät das QoS aktiviert sein muss. Die Mechanismen des QoS werden bei APSD verwendet, um den Strombedarf der Anwendungen zu optimieren.

Statistik

WEBconfig: HiLCOS-Menübaum / Status / WLAN E Netzwerke

▶ APSD

Zeigt an, ob APSD im jeweiligen WLAN (SSID) aktiv ist. APSD wird hier nur als aktiv angezeigt, wenn sowohl APSD in den Einstellungen des logischen WLANs als auch das globale QoS-Modul aktiviert sind.

WEBconfig: HiLCOS-Menübaum / Status / WLAN

▶ Stationstabelle

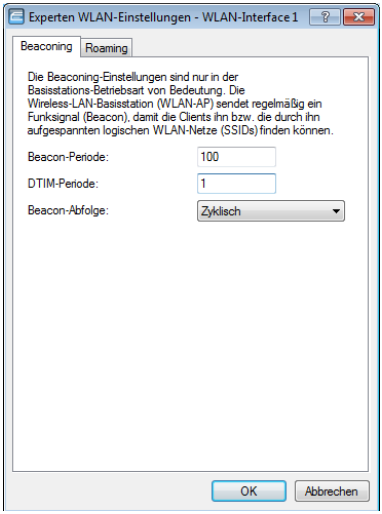
Zeigt in einer Bitmaske an, für welche Zugriffskategorien der eingebuchte WLAN-Client APSD nutzt:

– Voice (höchste Priorität)
– Video
– Best effort (einschließlich Datenverkehr von “Legacy Power Save”-Clients)
– Background (geringste Priorität).

12.6.13 Experten-WLAN-Einstellugnen

Die Beaconing-Tabelle

Die Einstellungen in der Beaconing-Tabelle beeinflussen, wie die im AP-Modus vom AP ausgestrahlten Beacons (Leuchtfeuer) versendet werden. Teilweise kann damit das Roaming-Verhalten von Clients beeinflusst werden, teilweise dient dies der Optimierung des MultiSSID-Betriebes für ältere WLAN-Clients.



LANconfig: Wireless LAN / Allgemein / Experten-WLAN-Einstellugnen / Beaconing

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Beaconing

- Beacon-Periode

  Dieser Wert gibt den zeitlichen Abstand in Kµs an, in dem Beacons verschickt werden (1 Kµs entspricht 1024 Mikrosekunden und stellt eine Recheneinheit des 802.11-Standard dar – 1 Kµs wird auch als Timer Unit TU bezeichnet). Niedrigere Werte ergebenen kleinere Beacon-Timeout-Zeiten auf dem Client und erlauben damit ein schnelleres Roaming beim AP-Ausfall, erhöhen aber den Overhead auf dem WLAN.

- DTIM-Periode

Dieser Wert gibt an, nach welcher Anzahl von Beacons die gesammelten Multicasts ausgesendet werden. Höhere Werte erlauben längere Sleep-Intervalle der Clients, verschlechtern aber die Latenzzeiten.

- Beacon-Abfolge

  Die Beacon-Abfolge bezeichnet die Reihenfolge, in der die Beacon zu den verschiedenen WLAN-Netzen versendet werden. Wenn z. B. drei logische WLAN-Netze aktiv sind und die Beacon-Periode 100 Kµs beträgt, so werden alle 100 Kµs die Beacons für die drei WLANs verschickt. Je nach Beacon-Abfolge werden die Beacons zu folgenden Zeitpunkten versendet:

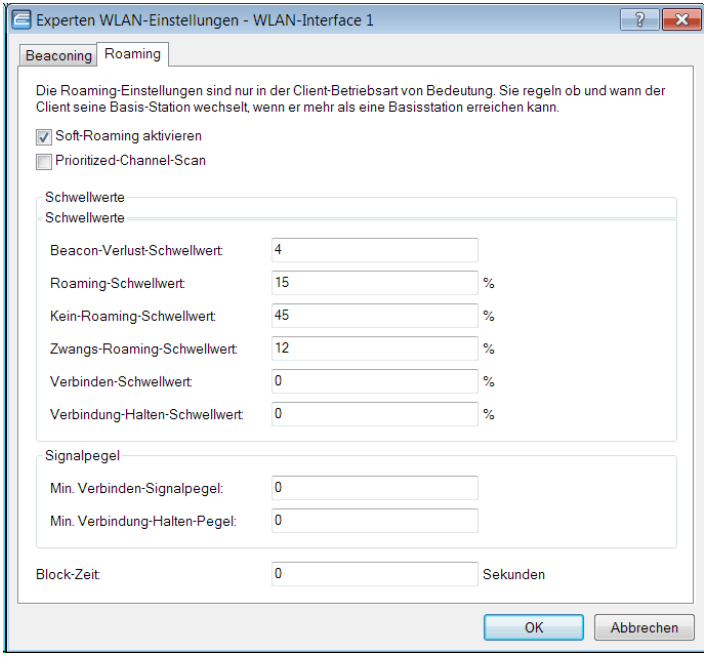
  – zyklisch: In diesem Modus beginnt der AP beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, gefolgt von WLAN-2 und WLAN-3. Beim zweiten Beacon-Versand (100 Kµs) wird zuerst WLAN-2 versendet, dann WLAN-3 und erst dann kommt wieder WLAN-1 an die Reihe. Beim dritten Beacon-Versand (200 Kµs) entsprechend WLAN-3, WLAN-1, WLAN-2 – dann beginnt die Reihe wieder von vorne.
  – gestaffelt: In diesem Modus werden die Beacons nicht gemeinsam zu einem Zeitpunkt verschickt, sondern auf die verfügbare Beacon-Periode aufgeteilt. Zum Start bei 0 Kµs wird nur WLAN-1 verschickt, nach 33,3 Kµs kommt WLAN-2, nach 66,6 Kµs WLAN-3 – mit Beginn einer neuen Beacon-Periode startet der Versand wieder mit WLAN-1.
  – einfach-Burst: In diesem Modus verschickt der AP die Beacons für die definierten WLAN-Netze immer in der gleichen Abfolge. Beim ersten Beacon-Versand (0 Kµs) mit WLAN-1, WLAN-2 und WLAN-3, beim zweiten Versand nach dem gleichen Muster und so weiter.
  – Default: zyklisch

  Ältere WLAN-Clients sind manchmal nicht in der Lage, die schnell aufeinander folgenden Beacons richtig zu verarbeiten, wie sie bei einem einfachen Burst auftreten. In der Folge erkennen diese Clients oft nur die ersten Beacons und können sich daher auch nur bei diesem einen Netz einbuchen.

  Die gestaffelte Aussendung der Beacons führt zum besten Ergebnis, erhöht aber die Prozessorlast für den AP. Die zyklische Aussendung stellt sich als guter Kompromiss dar, weil hier jedes Netz einmal als erstes ausgesendet wird.

Die Roaming-Tabelle

Zur genauen Steuerung, wie sich ein WLAN-Gerät in der Betriebsart 'Client' beim Roaming verhält, dienen verschiedene Schwellwerte in der Roaming Tabelle.



LANconfig: Wireless LAN / Allgemein / Experten-WLAN-Einstellugnen / Roaming

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Roaming

- Soft-Roaming

  Diese Option ermöglicht dem Client, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren AP durchzuführen (Soft-Roaming). Roaming aufgrund eines Verbindungsverlustes (Hard-Roaming) bleibt davon natürlich unbeeinflusst. Die eingestellten Roaming-Schwellwerte haben nur eine Funktion, wenn Soft-Roaming aktiviert ist.

- Prioritized-Channel-Scan

Die Prioritized-Channel-Scan-Funktion optimiert das Roaming durch das Einbeziehen vorheriger Roaming-Entscheidungen und eignet sich damit für Szenarios wiederkehrender Bewegungsabläufe des Clients im WLAN. Die Prioritized-Channel-Scan-Funktion ermittelt Kanäle, auf denen potentielle Roaming-Partner am wahrscheinlichsten zu finden sind. Das Ergebnis ist ein beschleunigtes Roaming und eine damit einhergehende reduzierte Handover-Zeit sowie ein reduzierter Paketverlust.

- Beacon-Verlust-Schwellwert

  Der Beacon-Empfangs-Schwellwert gibt an, wieviele Beacons des APs empfangsgestört sein dürfen, bevor ein eingebuchter Client eine erneute Suche beginnt.

  Je höher der eingestellte Wert ist, desto eher kann es unbemerkt zu einer Unterbrechung der Verbindung kommen, gefolgt von einem zeitverzögerten Wiederaufbau der Verbindung.

  Je kleiner der eingestellte Wert ist, desto eher kann eine möglicherweise folgende Unterbrechung erkannt werden, der Client kann frühzeitig mit dem Suchen nach einem alternativen AP beginnen.

  Hinweis: Zu kleine Werte können dazu führen, dass der Client unnötig oft einen Verbindungsverlust erkennt.

- Roaming-Schwellwert

  Dieser Schwellwert gibt an, um wieviel Prozent die Signalstärke eines anderen APs besser sein muss, damit der Client auf den anderen AP wechselt.

  Hinweis: In anderem Zusammenhang wird die Signalstärke teilweise in dB angegeben. In diesen Fällen gilt für die Umrechnung:

  64dB - 100%

  32dB - 50%

  0dB - 0%

- Kein-Roaming-Schwellwert

Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle AP als so gut betrachtet wird, dass auf keinen Fall auf einen anderen AP gewechselt wird.

- Zwangs-Roaming-Schwellwert

  Dieser Schwellwert gibt die Feldstärke in Prozent an, ab welcher der aktuelle AP als so schlecht betrachtet wird, dass auf jeden Fall auf einen anderen, besseren AP gewechselt wird.

- Verbinden-Schwellwert

  Dieser Schwellwert gibt die Feldstärke in Prozent an, die ein AP mindestens aufweisen muss, damit ein Client einen Versuch zum Einbuchen bei diesem AP startet.

- Verbindung-Halten-Schwellwert

  Dieser Schwellwert gibt die Feldstärke in Prozent an, die der aktuelle AP mindestens aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

- Min. Verbinden-Signalpegel

  Analog zum Verbinden-Schwellwert, Angabe jedoch als absolute Signalstärke.

- Min. Verbindung-Halten-Signalpegel

  Analog zum Verbindung-Halten-Schwellwert, Angabe jedoch als absolute Signalstärke.

- Blockzeit

  In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkten (gleiche SSID auf mehreren APs) können Sie hier einen Zeitraum definieren, in dem sich der WLAN-Client nicht mehr mit einem AP verbindet, nachdem die Anmeldung an diesem AP abgelehnt wurde (Association-Reject).

  Mögliche Werte sind 0 bis 4294967295 Sekunden.

  Der Standardwert ist 0 Sekunden. Die Anmeldung des Clients wird nicht blockiert.

12.6.14 Gruppenschlüssel pro VLAN

Im folgenden Abschnitt finden Sie Erläuterungen zur Verwaltung von Gruppenschlüsseln im VLAN.

Einleitung

In einer VLAN-Umgebung weist die zentrale Netzwerkverwaltung jedem virtuellen Netz in der Regel eine eindeutige VLAN-ID zu. Die Zugehörigkeit zu einem VLAN ergibt sich meist über den physikalischen Anschluss, der den Netzwerk-Client mit dem Netz verbindet.

Die zentrale, das Netz verwaltende Station (z. B. ein VLAN-fähiger Switch) weist ihren Ports intern bestimmte VLAN-IDs zu. Trifft nun ein Datenpaket an einem Port ein, geschieht die interne Weiterleitung ausschließlich an Ports mit korrespondierenden VLAN-IDs. Alle anderen Netzteilnehmer, die an Ports mit abweichenden oder ohne VLAN-IDs angeschlossen sind, erhalten diese Datenpakete nicht.

Bei mehreren vorhandenen VLANs mit differenziertem Dienstumfang erfolgt die Trennung der Datenkommunikation meistens über die Zuweisung zu unterschiedlichen logischen WLAN-Netzen (SSIDs). Mitarbeiter erhalten z. B. über eine spezielle SSID Zugriff auf das Firmennetzwerk und das Internet. Gäste hingegen erhalten über eine andere SSID eingeschränkten Zugriff auf das Internet.

Hirschmann APs verwalten darüber hinaus in VLAN-Netzwerk-Tabellen die Zuordnung von WLAN-Clients zu einzelnen VLANs. In umfangreichen Netzwerkumgebungen übernimmt meist ein RADIUS-Server die Rechteverwaltung und Zuordnung der Clients zu genutzten VLANs. Nach erfolgreicher Authentifizierung übergibt der RADIUS-Server die Daten zurück an den entsprechenden AP. Für die Dauer der Client-Anmeldung speichert er sie in seiner VLAN-Netzwerk-Tabelle.

Bei Bedarf erhalten die verschiedenen WLAN-Clients, die am gleichen AP angemeldet sind, unterschiedliche VLAN-IDs. Die geschieht durch die dynamischen VLAN-Netzwerk-Tabellen in den APs. Die VLAN-interne Kommunikation erfolgt abgesichert über einen bei der Anmeldung am AP ausgehandelten Sitzungsschlüssel. Somit ist die Datenübertragung der Clients in unterschiedlichen VLANs voneinander isoliert, obwohl jeder Client zur Kommunikation mit dem AP dasselbe logische WLAN-Netz (SSID) verwendet.

Meldet sich ein Client an einem AP eines WLAN-Netzes an, erhält er vom AP außerdem einen Gruppenschlüssel für den Empfang von Broad- oder Multicast-Nachrichten.

Broad- und Multicast-Nachrichten unterstützen kein VLAN-Tagging. Deshalb können WLAN-Clients, die sich in einem isolierten VLAN befinden, nicht vom Empfang dieser Nachrichten ausgeschlossen werden. Im Idealfall ignorieren die WLAN-Clients die Kommunikation über VLAN-fremde Broad- und Multicast-Nachrichten.

Da diese Nachrichten jedoch besonders zur Netzwerk-Konfiguration vermehrt zum Einsatz kommen, ergeben sich folgende Probleme:

- Netzwerkprotokolle wie "UPnP" und "Bonjour" nutzen diese Nachrichten, um neue Dienste im Netzwerk anzukündigen.

  Es ist also möglich, dass WLAN-Clients den Zugang zu Servern einrichten, auf die sie überhaupt nicht zugreifen können.

- Der Internetstandard IPv6 verwendet Multicast-Sendungen, um Routerinformationen an die Clients zu übermitteln.

  Die Gefahr besteht, dass VLAN-fremde WLAN-Clients diese Informationen übernehmen und sich damit den Zugriff auf das VLAN entziehen, für das sie eigentlich registriert sind.

Mit der zunehmenden Verbreitung von IPv6 werden auch diese Client-Probleme zunehmen.

Um diese Probleme zu vermeiden, kann der AP statt eines für alle WLAN-Clients gültigen Gruppenschlüssels jedem verwendeten VLAN einen separaten Gruppenschlüssel zuweisen. Er schickt somit seine Broad- und Multicast-Sendungen nicht mehr an alle vorhandenen WLAN-Clients, sondern ausschließlich an ein bestimmtes VLAN und an die dort registrierten Clients. Die WLAN-Clients anderer VLANs können diese Sendungen nun nicht mehr entschlüsseln.

Hinweis:

Der IEEE 802.11-Standard sieht die Verwaltung von 4 unterschiedlichen Schlüsseln vor. Ein Schlüssel ist dabei immer für die gesicherte Unicast-Kommunikation zwischen dem AP und einem WLAN-Client reserviert.

Es können prinzipiell also maximal 3 separate VLANs über eigene Gruppenschlüssel verwaltet werden. Die jeweiligen Gruppenschlüssel werden dabei entweder automatisch vom AP oder manuell vom Netzwerk-Administrator verwaltet. Während der Anmeldung des WLAN-Clients am Netzwerk überträgt der AP ihm den zugehörigen VLAN-Gruppenschlüssel zur Entschlüsselung aller für sein VLAN bestimmten Broad- und Multicast-Sendungen.

Damit ergeben sich 2 mögliche Szenarien:

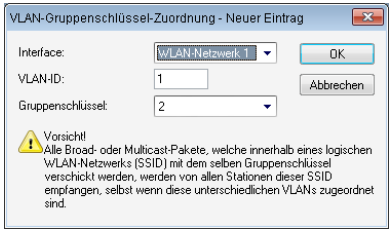
- Höchstens 3 VLANs sind im Bereich eines APs eingerichtet: Durch die 3 spezifischen VLAN-Gruppenschlüssel sind diese VLANs sicher voneinander getrennt.
- Mehr als 3 VLANs existieren im Bereich eines APs: Hierbei teilen sich mindestens 2 VLANs einen Gruppenschlüssel. Der Administrator muss die geteilten Gruppenschlüssel optimal auf die VLANs aufteilen.

Die Verwaltung der VLAN-Gruppenschlüssel erfolgt in 2 Tabellen:

- Die Konfigurations-Tabelle, in der die Zuordnung manuell durch den Administrator erfolgt.
- Die Status-Tabelle, in der die automatische Gruppenschlüssel-Zuordnung durch den AP abzulesen ist.

Verwaltung von VLAN-Gruppenschlüsseln

Wenn Sie vorhaben, verschiedene VLAN-IDs auf einem logischen WLAN-Netzwerk (SSID) zu verwenden, besteht die Möglichkeit den entsprechenden Gruppenschlüssel für Broad- und Multicast-Sendungen zuzuordnen. In LANconfig finden Sie diese Einstellung unter **Wireless-LAN** > **802.11i/WEP** > **Erweiterte Einstellungen** > **VLAN-Gruppenschlüssel-Zuordnung**



Die automatische Zuordnung der Gruppenschlüssel durchläuft folgende Schritte:

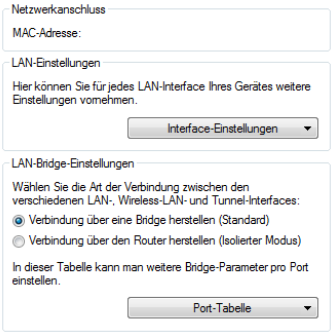
1. Wenn sich ein WLAN-Client anmeldet, überprüft der AP, ob dessen VLAN-ID bereits in der Statustabelle gelistet und entsprechend einem Gruppenschlüssel zugeordnet ist.
2. Falls nicht, überprüft der AP anhand der Konfigurationstabelle, ob eine manuelle Zuordnung besteht. In diesem Fall erstellt er einen entsprechend gemappten Eintrag in dieser Tabelle.
3. Falls auch keine manuelle Zuordnung besteht, fügt der AP einen neuen Eintrag hinzu und ordnet diesem Client den Gruppenschlüssel mit den wenigsten Teilnehmern zu.

Die Statustabelle mit den aktuellen automatischen VLAN-Gruppenschlüssel-Zuordnungen je SSID finden Sie unter **HiLCOS-Menübaum** > **Status** > **WLAN** > **VLAN-Gruppenschlüssel-Abbildung**

12.6.15 WLAN-Routing (Isolierter Modus)

In der Standardeinstellung wird der Datenverkehr zwischen LAN und WLAN „gebrückt“, also Layer-2-transparent übertragen. Dabei verläuft der Datenverkehr zwischen dem drahtgebundenen und den drahtlosen Netzwerken **nicht** über den IP-Router. Damit stehen auch die im IP-Router integrierten Funktionen Firewall und Quality-of-Service nicht für den Datenverkehr zwischen WLAN und LAN zur Verfügung. Um diese Möglichkeiten dennoch zu nutzen, werden die WLAN-Schnittstellen in den „isolierten Modus“ versetzt, der Datenverkehr wird gezielt über den IP-Router geleitet.

Hinweis: Damit der IP-Router Daten zwischen LAN und WLAN richtig übertragen kann, müssen die beiden Bereiche über unterschiedliche IP-Adresskreise verfügen. Weitere Informationen finden Sie im Bereich Advanced Routing and Forwarding (ARF).



LANconfig: Schnittstellen / LAN

WEBconfig: HiLCOS-Menübaum / Setup / LAN-Bridge / Isolierter-Modus

12.6.16 Alarm-Grenzwerte für WLAN Geräte

Typische Situationen, welche sich im WLAN-Umfeld meist für Probleme verantwortlich zeigen, sind ein Absinken der Signalstärke unter einen gewissen Grenzwert, der Prozentsatz der Anzahl an verlorenen Paketen einen gewissen Grenzwert überschreitet oder Pakete müssen sehr oft erneut versendet werden, was die effektiv zur Verfügung stehende Bandbreite stark reduziert.

Um diese Situationen zu erkennen und darauf zu reagieren bietet Hirschmann nun auf WLAN Geräten diverse Konfigurationsmöglichkeiten für Grenzwerte, die beim Über- beziehungsweise Unterschreiten einen Alarm auslösen.

Hinweis: Eine Verbindung wird nicht absolut als schlecht bewertet, die Bewertung hängt immer von den Parametern ab, die angegeben werden. Hierbei ist insbesondere zu beachten, dass zu hohe oder zu niedrige Grenzwerte eine Verbindung auch falsch bewerten können und unnötige Alarme in einer sehr großen Anzahl erzeugen können. Ein gewisses Mass an Paketverlusten und eine schwankende Signalstärke sind auch bei stabilen WLAN-Verbindungen zu erwarten.

Es können Grenzwerte für die einzelnen SSIDs und die Punkt-zu-Punkt-Verbindungen eines APs festgelegt werden. Diese werden zur Bewertung der Verbindung jedes Clients zu der entsprechenden SSID und bei der Verbindung zu einem entsprechenden P2P-Partner genutzt.

12.6.17 Übernahme der User-Priorität von IEEE 802.11e in VLAN-Tags

IEEE 802.11e ist ein Standard zur Erweiterung der WLAN-Standards um Quality-of-Service-Funktionen (QoS). Wenn ein AP diesen Standard nutzt, kann das Gerät den angebundenen WLAN-Clients eine bestimmte Priorität zuweisen (User-Priorität). Mit der Priorisierung der WLAN-Datenpakete kann der AP u. a. die Daten von Voice-over-IP-Clients bevorzugt übertragen. Auf der LAN-Seite sind die APs in vielen Fällen mit einem Switch verbunden, verschiedene LAN-Segmente sind oft durch VLANs getrennt. Das kabelgebundene LAN nutzt andere Mechanismen zur Priorisierung der Datenpakete.

Das folgende Anwendungsbeispiel verdeutlicht die Situation:

- Ein WLAN-Client (z. B. VoIP-Telefon) ist an einen AP angebunden, QoS ist auf dem WLAN aktiviert, die Daten zwischen Telefon und AP sind nicht VLAN-getaggt.
- Der AP ist auf der Ethernet-Seite mit einem VLAN-fähigen Switch verbunden, die Daten zwischen AP und Switch sind VLAN-getaggt.

Der AP als Schnittstelle zwischen kabelgebundenem LAN und drahtlosem WLAN setzt die unterschiedlichen Priorisierungsinformationen entsprechend um:

- Bei der Übertragung von Daten vom AP zum WLAN-Client (Senderichtung aus Sicht des APs) ermittelt das Gerät die Priorität eines empfangenen Paketes entweder aus dem VLAN-Tag oder aus dem ToS/DSCP-Feld des IP-Headers. Mit dieser Priorität sendet der AP die Pakete an den Client.
- Bei der Übertragung von Daten vom WLAN-Client zum AP (Empfangsrichtung aus Sicht des APs) enthält das Datenpaket jedoch kein VLAN-Tag. In dieser Richtung untersucht der AP außerdem nicht den IP-Header. Stattdessen entnimmt der AP die User-Priorität aus dem WLAN-Paket und setzt diese entsprechend in das VLAN-Tag der ausgehenden Datenpakete in Richtung Switch ein.

12.6.18 UUID-Info-Element für Hirschmann WLAN Access Points

Alle aktuellen Hirschmann APs sind Multi-SSID-fähig. D. h., sie können mehreren WLAN-Clients gleichzeitig unterschiedliche 'virtuelle' APs anbieten.

Bei Geräten mit zwei Funkmodulen (Dual Radio) beziehen sich darüber hinaus die BSSIDs der logischen Netzwerke zwar auf das entsprechende Funkmodul, die MAC-Adressen der beiden Funkmodule sind jedoch völlig unabhängig voneinander. Somit lassen sich logische Netzwerke mit unterschiedlicher BSSID nicht eindeutig einem Gerät zuordnen.

Zur Netzwerk-Überwachung und -Planung ist es jedoch sinnvoll, die logischen Netzwerke den entsprechenden Geräten (bzw. Funkmodulen) zuordnen zu können.

Hirschmann APs unterstützen unter anderem ein Aironet-kompatibles Info-Element, das den vom Administrator vergebenen Namen des Gerätes beinhaltet. Die Übertragung dieser Information ist jedoch optional, wobei viele Anwender sie deaktivieren, weil sie z. B. aus Sicherheitsgründen so wenig Informationen wie möglich über den AP im Netzwerk veröffentlichen möchten.

Bei der Überwachung des Netzwerkes taucht diese Information also entweder gar nicht auf, oder sie identifiziert das Gerät je nach Eingabe nicht zwingend als AP.

Darüber hinaus besitzen Hirschmann Access Points eine UUID (Universally Unique Identifier), die aus Geräte-Typ und Seriennummer errechnet wird und das Gerät eindeutig im Netzwerk identifizieren kann. Durch eine Verschlüsselung bei der UUID-Erzeugung ist jedoch ein Rückschluss auf Gerät oder Seriennummer nur mit hohem Aufwand (Brute-Force-Angriff über alle möglichen Geräte-Typen und Seriennummern) möglich.

Sie können die Übertragung der UUID je Funkmodul und logischem Netzwerk unabhängig voneinander ein- oder ausschalten.

12.6.19 Erweiterte WLAN-Parameter

- **ProbeRsp-Retries**

  WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Übertragung

  Dies ist die Anzahl der Hard-Retries für Probe-Responses, also Antworten, die ein AP als Antwort auf einen Probe-Request von einem Client schickt.

  Mögliche Werte:

  – 0 bis 15

  Default:

– 3

Default:

– Werte größer als 15 werden wie 15 behandelt.

▶ **Sperrzeit**

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Roaming

In der Betriebsart als WLAN-Client und bei mehreren gleichen WLAN-Zugangspunkte (gleiche SSID auf mehreren APs) können Sie hier einen Zeitraum zu definieren, in dem sich der WLAN-Client nicht mehr mit einem AP verbindet, nachdem die Anmeldung an diesem AP abgelehnt wurde (Association-Reject).

Mögliche Werte:

– 0 bis 4294967295 in Sekunden

Default:

– 0

12.6.20 Ratenadaptionsalgorithmus

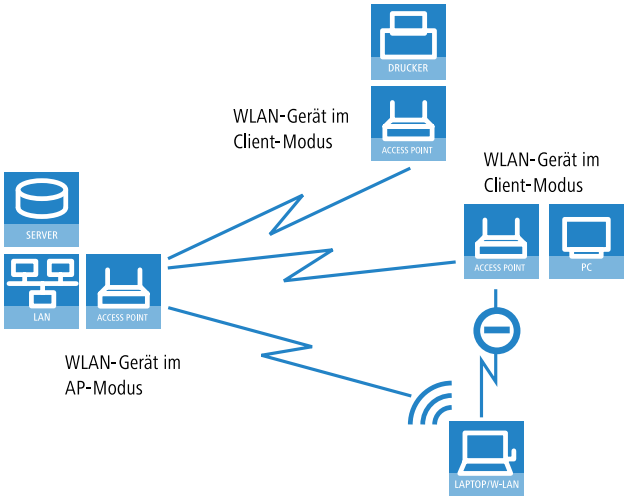
Eine WLAN-Verbindung nutzt, im Gegensatz zu einer Ethernet-Verbindung, variable Bitraten. Höhere Bitraten bieten einen besseren Durchsatz, setzen allerdings auch eine höhere Signalqualität beim Empfänger voraus. Dies ist Voraussetzung für eine fehlerlose Dekodierung. WLAN-Geräte passen die Bitrate an, wenn sich Eigenschaften des Mediums ändern oder eine erste Verbindung hergestellt wird. Dadurch wird sichergestellt, dass das Gerät die beste verfügbare Bitrate nutzt.

Der bekannte Minstrel-Algorithmus prüft im Gegensatz zum Standard-Algorithmus nicht ausschließlich die benachbarten Bitraten sondern alle Bitraten. Somit wird die optimale Bitrate schneller bestimmt.

12.7 Konfiguration des Client-Modus

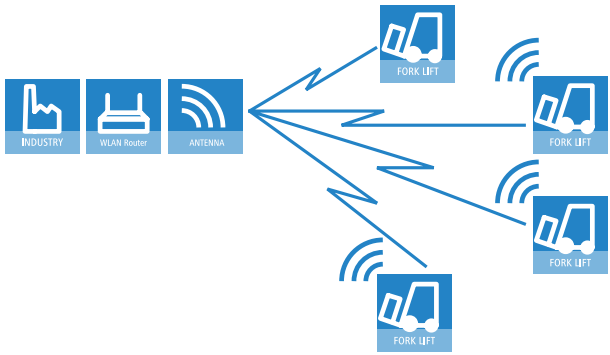
Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein Funk-LAN können Hirschmann-Geräte mit WLAN-Modul in den sogenannten

Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher Funk-LAN-Adapter verhalten und nicht wie ein Access Point (AP). Über den Client-Modus ist es also möglich, auch Geräte wie PCs oder Drucker, die ausschließlich über eine Ethernet-Schnittstelle verfügen, in ein Funk-LAN einzubinden.



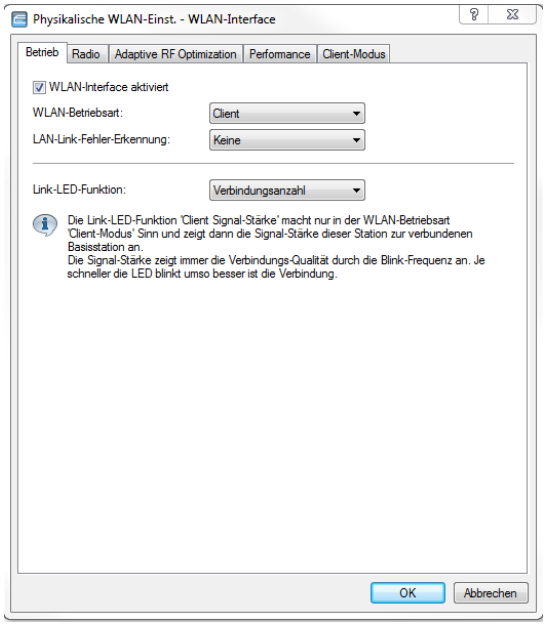
Hinweis: Bei einem WLAN-Gerät im AP-Modus können sich weitere WLAN-Clients anmelden, bei einem WLAN-Gerät im Client-Modus jedoch nicht.

In industriellen Anwendungen können die WLAN-Clients auch mobil eingesetzt werden, z. B. auf einem Gabelstapler, der über die drahtlose Verbindung ständig Kontakt zu seiner Leitstelle hält.



12.7.1 Client-Modus mit LANconfig aktivieren

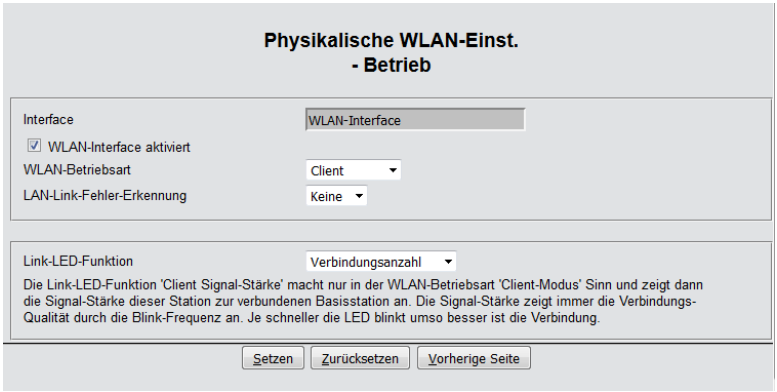
Um Ihr Gerät mittels LANconfig in den Client-Modus zu versetzen, wechseln Sie in die Ansicht **Wireless-LAN** > **Physikalische WLAN-Einst.** und wählen Sie im Reiter **Betrieb** die WLAN-Betriebsart **Client**. Bestätigen Sie Ihre Auswahl mit einem Klick auf die Schaltfläche **OK**.



12.7.2 Client-Modus mit WEBconfig aktivieren

Um Ihr Gerät mittels WEBconfig in den Client-Modus zu versetzen, wechseln Sie in das Menü **Konfiguration** > **Wireless-LAN**.

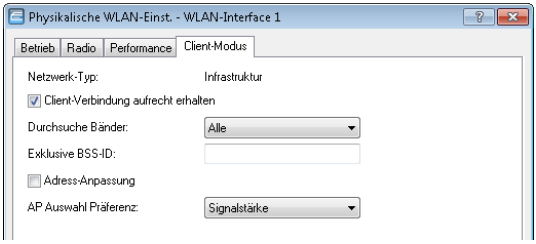
Wählen Sie im Abschnitt "Interfaces" die Wireless-LAN-Einstellung **Physikalische WLAN-Einst. - Betrieb** und stellen Sie die WLAN-Betriebsart auf **Client**. Bestätigen Sie Ihre Auswahl mit einem Klick auf die Schaltfläche **Setzen**.



12.7.3 Client-Einstellungen

Für HirschmannAPs im Client-Modus können auf der Registerkarte 'Client-Modus' bei den Einstellungen für die physikalischen Interfaces weitere Einstellungen bzgl. des Verhaltens als Client vorgenommen werden.

Hinweis: Die Konfiguration der Client-Einstellungen kann auch mit dem WLAN-Assistenten von LANconfig erfolgen.

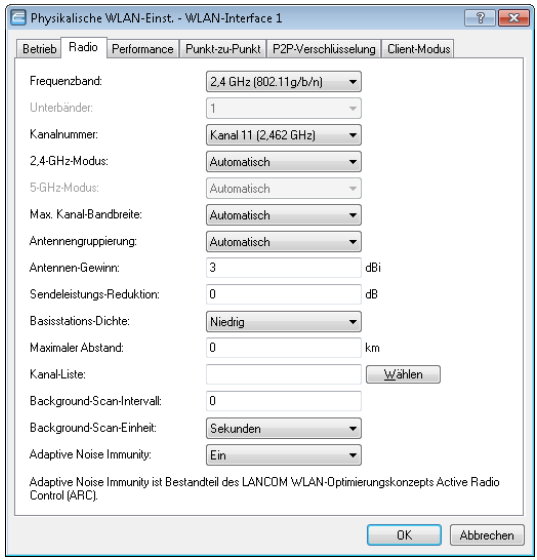


1. Zum Bearbeiten der Einstellungen für den Client-Modus wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Client-Modus'.
2. Stellen Sie unter 'Durchsuchte Bänder' ein, ob die Clientstation nur das 2,4 GHz-, nur das 5 GHz-Band oder alle verfügbaren Bänder absuchen soll, um eine Basisstation zu finden.

12.7.4 Radio-Einstellungen

Damit der WLAN-Client eine Verbindung zu einem AP aufbauen kann, muss er geeignete Frequenzbänder bzw. Kanäle verwenden.

1. Zum Bearbeiten der Radio-Einstellungen wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



2. Stellen Sie das Frequenz-Band, die Kanäle und den 2,4 GHz- bzw. 5 GHz-Modus passend zu den Einstellungen des APs ein.

Hinweis: Je nach Modell entfällt die Auswahl des Frequenzbandes und der Kanäle, z. B. wenn das Gerät nur ein Frequenzband unterstützt.

Greenfield-Modus für Access Points mit IEEE 802.11n

Bei APs nach dem Standard IEEE 802.11n haben Sie in den physikalischen WLAN-Einstellungen die Möglichkeit, die Datenübertragung nach den Standards IEEE 802.11a/b/g/n gezielt zu erlauben oder einzuschränken.

Neben der Auswahl der einzelnen Standards a/b/g/n und verschiedenen gemischten Betriebsarten erlauben die APs auch die Auswahl des Greenfield-Modus. Wenn Sie in den physikalischen WLAN-Einstellungen einer WLAN-Schnittstelle den Greenfield-Modus aktivieren, können sich nur WLAN-Clients in die zugehörigen logischen WLANs (SSIDs) einbuchen, die ihrerseits den Standard IEEE 802.11n unterstützen. Andere WLAN-Clients, die ausschließlich nach den Standards IEEE 802.11a/b/g arbeiten, können sich nicht in diese WLANs einwählen.

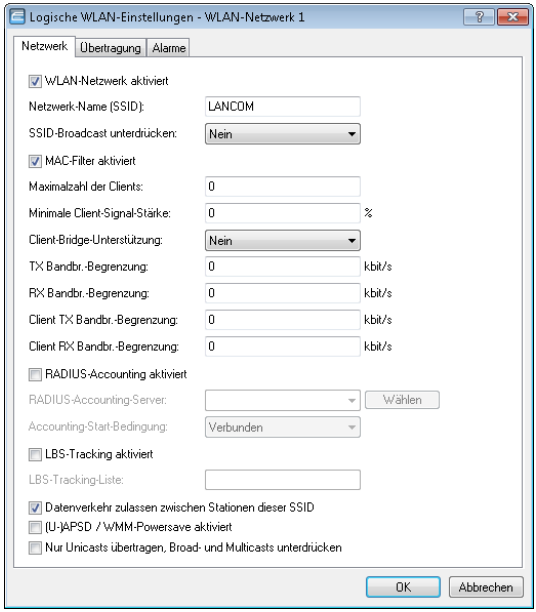
Der Standard IEEE 802.11n erlaubt nur Verschlüsselungen nach WPA2/AES und unverschlüsselte Verbindungen. WEP- und TKIP-basierte Verschlüsselungen sind in IEEE 802.11n nicht erlaubt. Bitte beachten Sie je nach Einstellungen der physikalischen und logischen WLAN-Einstellungen die folgenden Einschränkungen:

- Wenn Sie in den physikalischen Einstellungen einen gemischten Modus mit Unterstützung für den Standard IEEE 802.11n aktivieren und einzelne WLAN-Clients in einem logischen Netzwerk nur WEP-Verschüsselung erlauben, reduziert der AP die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit WEP nicht erlaubt sind.
- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs neben AES auch andere Sitzungsschlüssel nach TKIP erlauben, verwendet der AP für dieses WLAN ausschließlich den Sitzungsschlüssel nach AES, weil TKIP nach IEEE 802.11n nicht erlaubt ist.
- Wenn Sie in den Verschlüsselungseinstellungen eines logischen WLANs ausschließlich Sitzungsschlüssel nach TKIP erlauben, reduziert der AP die Übertragungsrate auf den Standard 802.11a/b/g, weil die höheren Übertragungsraten nach IEEE 802.11n in Kombination mit TKIP nicht erlaubt sind.

12.7.5 SSID des verfügbaren Netzwerks einstellen

In den WLAN-Clients muss die SSID des Netzwerks eingetragen werden, zu dem sich die Clientstationen verbinden soll.

1. Zum Eintragen der SSID wechseln Sie unter LANconfig nach **Wireless-LAN** > **Allgemein**. Nach einem Klick auf **Logische WLAN-Einstellungen** wählen Sie das **erste** WLAN-Interface aus.

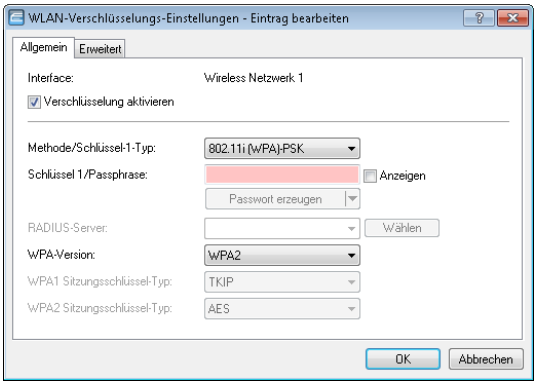


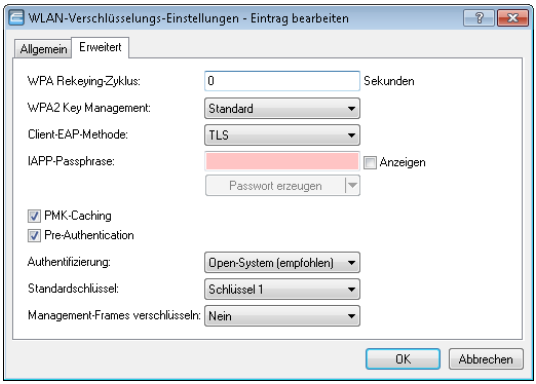
2. Aktivieren Sie auf der Registerkarte **Netzwerk** das WLAN-Netzwerk und tragen Sie die SSID des Netzwerks ein, bei dem sich die Clientstation einbuchen soll.

12.7.6 Verschlüsselungseinstellungen

Für den Zugriff auf ein WLAN müssen in der Clientstation die entsprechenden Verschlüsselungsmethoden und Schlüssel eingestellt werden.

1. Zum Eintragen der Schlüssel wechseln Sie unter LANconfig nach **Wireless LAN** > **Verschlüsselung**. Nach dem Klick auf **WLAN-Verschlüsselungs-Einstellungen** markieren Sie in der Liste der logischen WLAN-Einstellungen das **erste** WLAN-Interface und klicken auf **Bearbeiten**.





2. Aktivieren Sie die Verschlüsselung und passen Sie die Verschlüsselungsmethode an die Einstellungen des APs an.
3. Hirschmann APs in der Betriebsart als WLAN-Client können sich über EAP/802.1X bei einem anderen AP authentifizieren. Wählen Sie dazu hier die gewünschte Client-EAP-Methode aus. Beachten Sie, dass die gewählte Client-EAP-Methode zu den Einstellungen des APs passen muss, bei dem sich das Gerät einbuchen will.

Hinweis: Je nach gewählter EAP-Methode müssen im Gerät die entsprechenden Zertifikate hinterlegt werden:

- Für TTLS und PEAP nur das EAP/TLS-Root-Zertifikat, als Schlüssel wird dabei die Kombination Benutzername:Kennwort eingetragen.
- Für TLS zusätzlich das EAP/TLS-Gerätezertifikat samt privatem Schlüssel.

Hinweis: Bei der Verwendung von WPA bzw. 802.1X sind evtl. weitere Einstellungen im RADIUS-Server notwendig.

12.7.7 PMK-Caching im WLAN-Client-Modus

Beim Verbindungsaufbau eines WLAN-Clients zu einem AP handeln die beiden Gegenstellen im Rahmen der 802.1x-Authentifizierung einen gemeinsamen Schlüssel für die nachfolgende Verschlüsselung aus, den Pairwise Master Key (PMK). Bei Anwendungen mit bewegten WLAN-Clients (Notebooks in größeren Büro-Umgebungen, bewegte Objekte mit WLAN-Anbindung im Industriebereich) wechseln die WLAN-Clients häufig den AP, bei dem sie sich in einem WLAN-Netz anmelden. Die WLAN-Clients roamen also zwischen verschiedenen, aber in der Regel immer den gleichen APs hin und her.

APs speichern üblicherweise einen ausgehandelten PMK für eine bestimmte Zeit. Auch ein WLAN-Gerät in der Betriebsart als WLAN-Client speichert den PMK. Sobald ein WLAN-Client einen Anmeldevorgang bei einem AP startet, zu dem zuvor schon einer Verbindung bestand, kann der WLAN-Client direkt den vorhandenen PMK zur Prüfung an den AP übermitteln. Die beiden Gegenstellen überspringen so die Phase der PMK-Aushandlung während des Verbindungsaufbaus, WLAN-Client und AP stellen die Verbindung deutlich schneller her.

Der WLAN-Client speichert den ausgehandelten PMK für die unter dem Parameter "Vorgabe-Lebenszeit" eingestellte Dauer.

12.7.8 Prä-Authentifizierung im WLAN-Client-Modus

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2/802.1x unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1x-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1x-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Hinweis: Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.

- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem *PMK-Caching*.

Hinweis: Client-seitig ist die Anzahl gleichzeitiger Prä-Authentifizierungen auf vier begrenzt, um in Netzwerk-Umgebungen mit vielen APs die Netzlast für den zentralen RADIUS-Server gering zu halten.

12.7.9 Mehrere WLAN-Profile im Client-Modus

Einleitung

Zur Anbindung von einzelnen Geräten mit einer Ethernet-Schnittstelle in ein WLAN können APs in den sogenannten Client-Modus versetzt werden, in dem sie sich wie ein herkömmlicher WLAN-Client verhalten und nicht wie ein AP.

WLAN-Clients wie Notebooks können in der Regel über das Betriebssystem oder über die gerätespezifische Software verschiedene Profile speichern und verwalten, um je nach Umgebung auf verschiedene APs zuzugreifen (z. B. für ein WLAN im Unternehmen und für ein weiteres WLAN im Home-Office). In diesen Profilen sind u. a. die SSID des entsprechenden WLANs und die benötigten Schlüssel gespeichert. Der WLAN-Client wählt dann automatisch

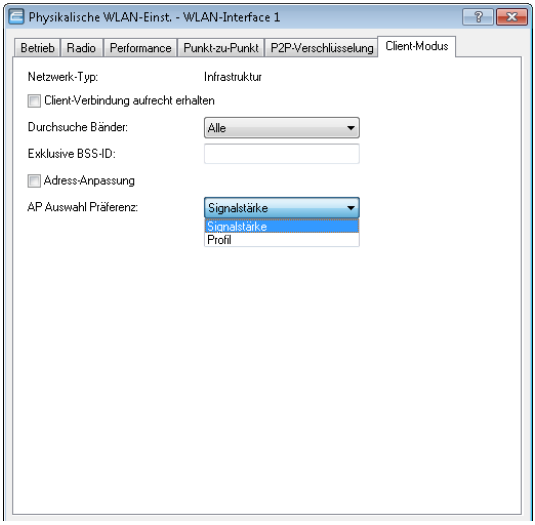
aus den verfügbaren WLANs das passende Profil für das stärkste oder das bevorzugte WLAN.

Hirschmann APs können bis zu 816 verschiedene WLAN-Profile für die Verwendung im Client-Modus speichern. Für die Profile werden im Client-Modus die Netzwerk- sowie Übertragungsparameter für die logischen WLANs sowie die Verschlüsselungseinstellungen verwendet.

Hinweis: Bitte beachten Sie, dass Sie ein WLAN-Modul im Client-Modus sich zu jeder Zeit nur mit einem AP verbinden kann, auch wenn mehrere WLAN-Profile definiert sind.

Konfiguration

Neben den Netzwerk-, Übertragungs- und Verschlüsselungsparametern kann für jedes WLAN-Modul separat definiert werden, nach welchem Kriterium das zu verwendende Client-Profil ausgewählt werden soll.



LANconfig: WLAN / Allgemein / Physikalische WLAN-Einstellungen / Client-Modus

WEBconfig: HiLCOS-Menübaum / Setup / Schnittstellen / WLAN / Client-Einstellungen / WLAN-1

▶ **AP Auswahl Präferenz**

Wählen Sie hier aus, wie diese Schnittstelle verwendet werden soll.

Mögliche Werte:

- Signalstärke: Wählt das Profil, dessen WLAN aktuell das stärkste Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald diese ein stärkeres Signal bietet.
- Profil: Wählt aus den verfügbaren WLANs das zu verwendende Profil in der Reihenfolge der definierten Einträge (WLAN-Index, z. B. WLAN-1, WLAN-1-2 etc.), auch wenn ein anderes WLAN ein stärkeres Signal bietet. In dieser Einstellung wechselt das WLAN-Modul im Client-Modus automatisch in ein anderes WLAN, sobald ein WLAN mit einem niedrigeren WLAN-Index erkannt wird (unabhängig von der Signalstärke dieses WLANs).

Default:

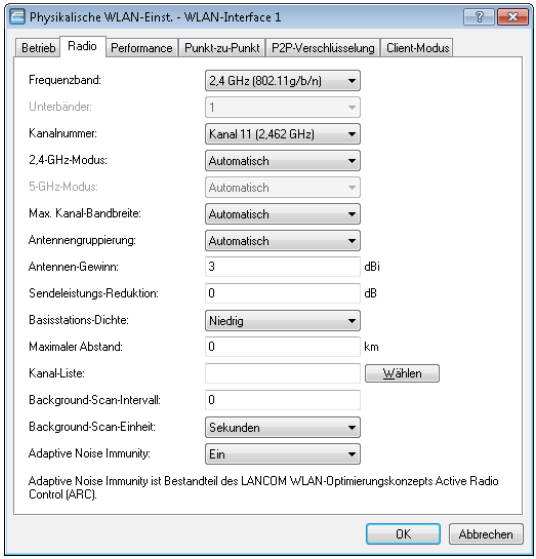
- Signalstärke.

12.7.10 Roaming

Mit Roaming bezeichnet man den Übergang eines WLAN-Clients zu einem anderen AP, wenn er keine Verbindung zum bisherigen AP mehr aufrecht erhalten kann. Um das Roaming zu ermöglichen, muss sich mindestens ein weiterer AP in der Reichweite des Clients befinden, der ein Netzwerk mit der gleichen SSID und den passenden Radio- und Verschlüsselungs-Einstellungen anbietet.

Normalerweise würde der WLAN-Client sich nur dann bei einem anderen AP einbuchen, wenn er die Verbindung zu dem bisherigen AP vollständig verloren hat (Hard-Roaming). Das Soft-Roaming ermöglicht dem Client hingegen, anhand verfügbarer Scan-Informationen ein Roaming zu einem stärkeren AP durchzuführen. Mit der Funktion des Background-Scanning kann das Gerät im Client-Modus schon vor Verbindungsverlust Informationen über andere verfügbare APs sammeln. Die Umschaltung auf einen anderen AP erfolgt dann nicht erst, wenn die bisherige Verbindung vollständig verloren wurde, sondern wenn ein anderer AP in Reichweite über ein stärkeres Signal verfügt.

1. Zum Aktivieren des Soft-Roaming wechseln Sie unter WEBconfig oder Telnet in den Bereich Setup > Schnittstellen > WLAN > Roaming und wählen dort das physikalische WLAN-Interface.
2. Schalten Sie das Soft-Roaming ein und stellen Sie ggf. die weiteren Parameter wie die Schwellwerte und Signalpegel ein.
3. Zur Konfiguration des Background-Scanning wechseln Sie unter LANconfig bei den physikalischen WLAN-Einstellungen für das gewünschte WLAN-Interface auf die Registerkarte 'Radio'.



4. Tragen Sie als Background-Scan-Intervall die Zeit ein, in welcher das Gerät zyklisch die aktuell ungenutzten Frequenzen des aktiven Bandes nach erreichbaren APs absucht. Um ein schnelles Roaming zu erzielen, wird die Scan-Zeit auf z. B. 260 Sekunden (2,4 GHz) bzw. 720 Sekunden (5 GHz) eingestellt.

ARF-Netzwerk für IAPP

APs nutzen das IAPP-Protokoll, um sich über die Roaming-Vorgänge der eingebuchten WLAN-Clients zu informieren. Die APs senden dazu regelmäßig bestimmte Multicast-Nachrichten aus (Announces), mit deren Hilfe die Geräte die BSSIDs und IP-Adressen der anderen APs lernen. Bei einem Roaming-Vorgang informiert der WLAN-Client den neuen AP darüber, bei welchem AP

er bisher eingebucht war. Der neue AP kann mit den aus den IAPP-Announces gelernten Informationen den bisherigen AP informieren, der den WLAN-Client umgehend aus seiner Tabelle der eingebuchten Clients entfernen kann.

Wenn in einem AP mehrere ARF-Netzwerke definiert sind, werden die IAPP-Announces in alle ARF-Netze ausgesendet. Um diese Multicasts auf ein bestimmtes ARF-Netz zu reduzieren, kann gezielt ein IAPP-IP-Netzwerk definiert werden.

WEBconfig: HiLCOS-Menübaum / Setup / WLAN

- **IAPP-IP-Netzwerk**

  Wählen Sie hier aus, welches ARF-Netzwerk als IAPP-IP-Netzwerk verwendet werden soll.

  Mögliche Werte:

  – Auswahl aus der Liste der im Gerät definierten ARF-Netzwerke, maximal 16 alphanumerische Zeichen.

  Default:

  – leer

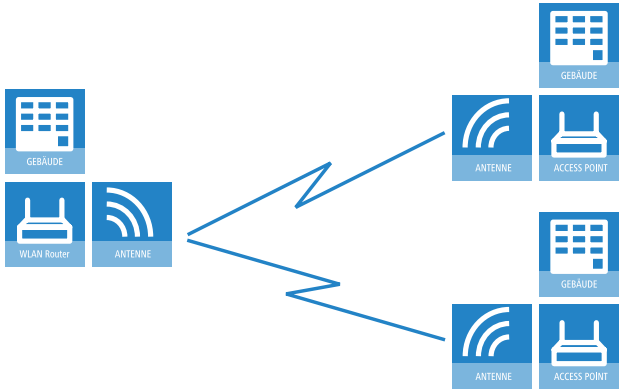
  Besondere Werte:

  – leer: Wenn kein IAPP-IP-Netzwerk definiert ist, werden die IAPP-Announces in alle definierten ARF-Netze versendet.

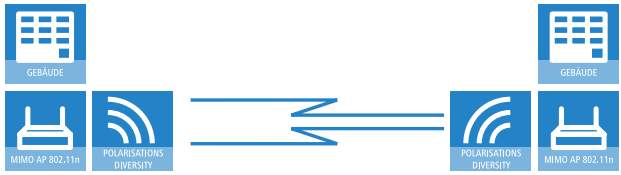
12.8 Aufbau von Punkt-zu-Punkt-Verbindungen

12.8.1 Konfiguration der Punkt-zu-Punkt-Verbindungen

Hirschmann APs können nicht nur als zentrale Station in einem Funknetzwerk arbeiten, sie können im Punkt-zu-Punkt-Betrieb auch Funkstrecken über größere Distanzen bilden. So können z. B. zwei Netzwerke über mehrere Kilometer hinweg sicher verbunden werden – ohne direkte Verkabelungen oder teure Standleitungen.



Bei der Verwendung von APs und entsprechend polarisierten Antennen nach IEEE 802.11n können gleichzeitig zwei Funkbeziehungen zwischen den Endpunkten einer P2P-Verbindung aufgebaut werden. Damit können deutliche höhere Datenraten erzielt oder größere Entfernungen überwunden werden als beim Einsatz der anderen Standards.



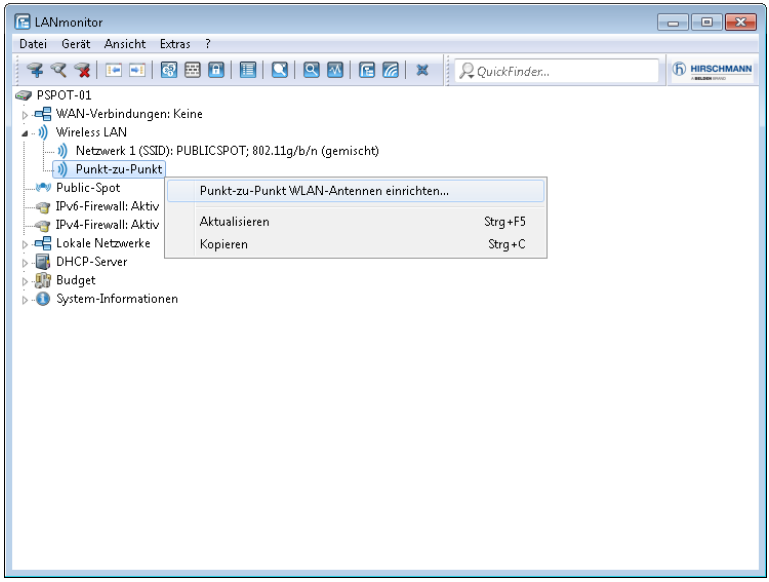
Dieses Kapitel stellt die Grundlagen zur Auslegung von Point-to-Point-Strecken vor und gibt Hinweise zur Ausrichtung der Antennen.

Hinweis: Informationen über die verwendeten Frequenzbereiche finden Sie im Anhang des ~Titles. Hinweise zur Konfiguration der APs finden Sie in der entsprechenden Geräte-Dokumentation bzw. im HiLCOS-Referenzhandbuch.

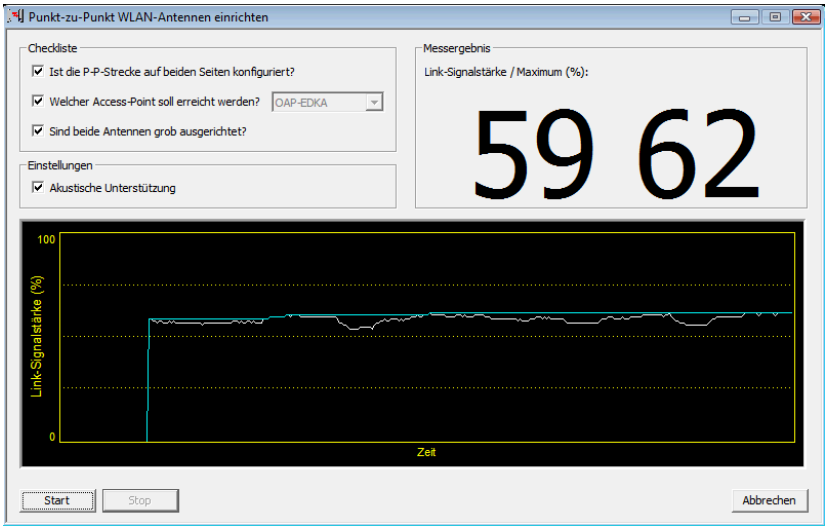
12.8.2 Einrichten von Punkt-zu-Punkt-Verbindungen mit dem LANmonitor

Um die Antennen für Punkt-zu-Punkt-Verbindungen möglichst gut ausrichten zu können, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden. Der LANmonitor bietet dabei neben der optischen Anzeige der Link-Signalstärke auch eine akustische Unterstützung.

Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'



Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

Zur genaueren Ausrichtung kann eine akustische Unterstützung aktiviert werden. Mit dieser Option wir abhängig von der aktuellen Link-Signalstärke ein Ton über den PC ausgegeben. Die maximale Link-Signalstärke wird mit einem Dauerton signalisiert. Fällt die Link-Signalstärke unter das Maximum, wird der Abstand zum bisher erreichten Maximum durch Tonintervalle angezeigt. Je kürzer die Intervalle, um so näher liegt die Link-Signalstärke am Maximum.

12.8.3 Geometrische Auslegung von Outdoor-Funknetz-Strecken

Geometrische Auslegung von Outdoor-Funknetz-Strecken

Bei der Auslegung der Funkstrecken sind im Wesentlichen folgende Fragen zu beantworten:

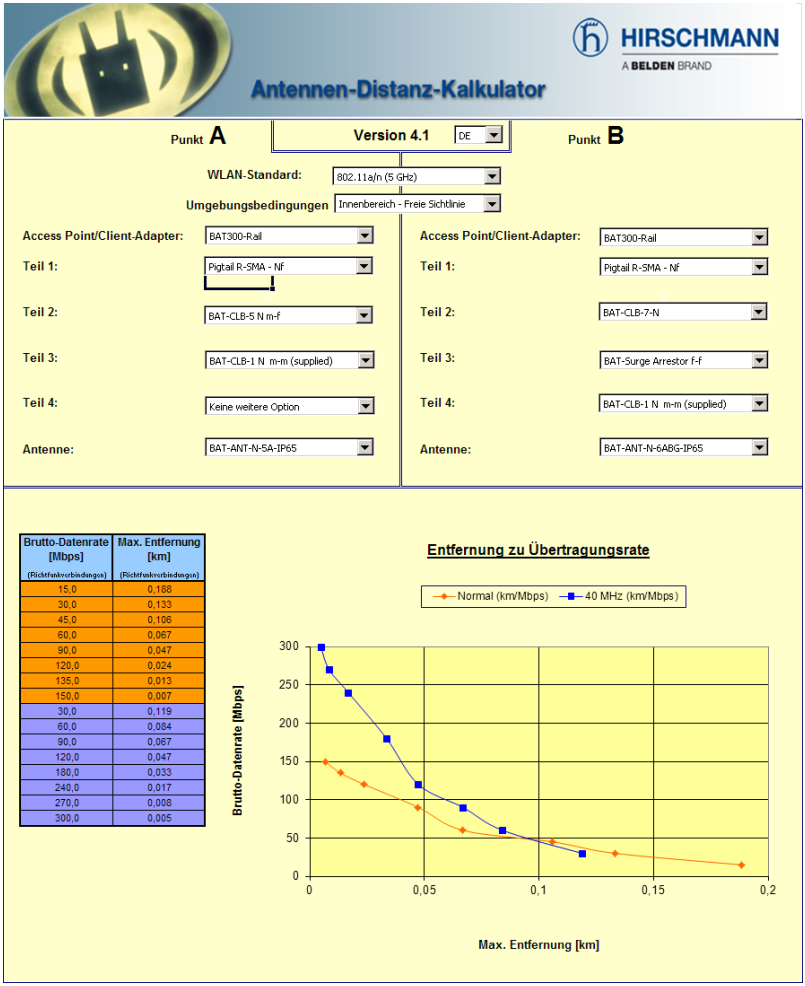
- Welche Antennen müssen für die gewünschte Anwendung eingesetzt werden?
- Wie müssen die Antennen positioniert werden, um eine einwandfreie Verbindung herzustellen?
- Welche Leistungen müssen die eingesetzten Antennen aufweisen, um einen ausreichenden Datendurchsatz innerhalb der gesetzlichen Grenzen zu gewährleisten?

Auswahl der Antennen mit dem Hirschmann Antennen-Kalkulator

Zur Berechnung der Ausgangsleistungen in den APs und für eine erste Abschätzung der erreichbaren Distanzen und Datenraten können Sie den Hirschmann Antennen-Kalkulator verwenden, den Sie zum Download auf unserer Webseite unter *www.hirschmann.com* finden.

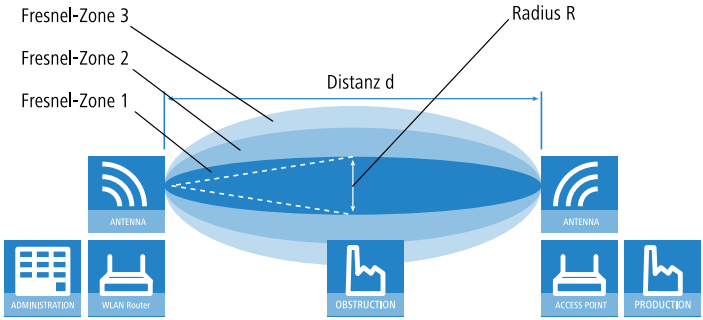
Nach Auswahl der verwendeten Komponenten (APs, Antennen, Blitzschutz und Kabel) berechnet der Kalkulator neben Datenraten und Distanzen auch den Antennen-Gewinn, der in den APs eingestellt werden muss.

Hinweis: Bitte beachten Sie, dass bei der Verwendung von 5 GHz-Antennen je nach Einsatzland zusätzliche Techniken wie die dynamische Frequenzwahl (Dynamic Frequency Selection – DFS) vorgeschrieben sein können. Der Betreiber der WLAN-Anlage ist für die Einhaltung der jeweils geltenden Vorschriften verantwortlich.



Positionierung der Antennen

Die Antennen strahlen ihre Leistung nicht linear, sondern in einem modellabhängigen Winkel ab. Durch die kugelförmige Ausbreitung der Wellen kommt es in bestimmten Abständen von der direkten Verbindung zwischen Sender und Empfänger zur Verstärkung oder zu Auslöschungen der effektiven Leistung. Die Bereiche, in denen sich die Wellen verstärken oder auslöschen, werden als Fresnel-Zonen bezeichnet.



Um die von der Antenne abgestrahlte Leistung möglichst vollständig auf die empfangende Antenne abzubilden, muss die Fresnel-Zone 1 frei bleiben. Jedes störende Element, das in diese Zone hineinragt, beeinträchtigt die effektiv übertragene Leistung deutlich. Dabei schirmt das Objekt nicht nur einen Teil der Fresnel-Zone ab, sondern führt durch Reflexionen zusätzlich zu einer deutlichen Reduzierung der empfangenen Strahlung.

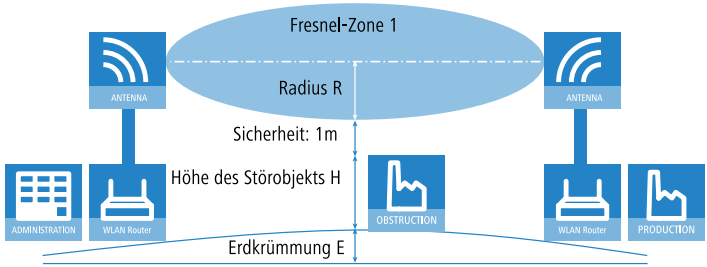
Der Radius (R) der Fresnel-Zone 1 berechnet sich bei gegebener Wellenlänge der Strahlung (λ) und der Distanz zwischen Sender und Empfänger (d) nach folgender Formel:

$R = 0{,}5 * \sqrt{(\lambda * d)}$

Die Wellenlänge beträgt im 2,4 GHz-Band ca. 0,125 m, im 5 GHz-Band ca. 0,05 m.

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 4 km ergibt sich im 2,4 GHz-Band der Radius der Fresnel-Zone 1 zu **11 m**, im 5 GHz-Band nur zu **7 m**.

Damit die Fresnel-Zone 1 frei und ungestört ist, müssen die Antennen das höchste Störobjekt um diesen Radius überragen. Die gesamte erforderliche Masthöhe (M) der Antennen ergibt sich nach folgendem Bild zu:



M = R + 1m + H + E (Erdkrümmung)

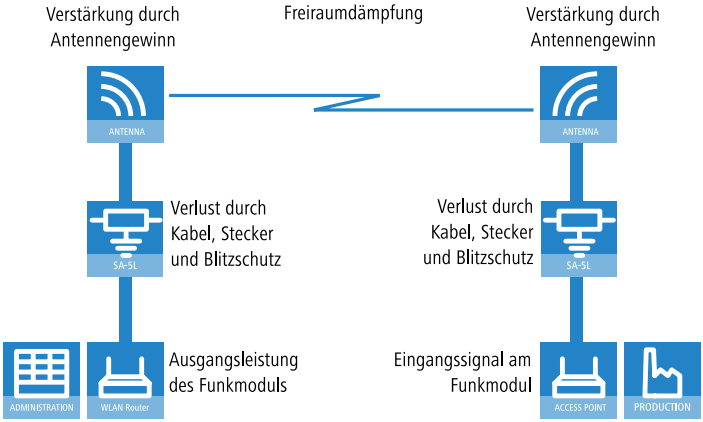
Die Höhe der Erdkrümmung (E) ergibt sich bei einer Distanz (d) zu E = d² * 0,0147 – bei einer Distanz von 8 km also immerhin schon fast 1m!

Beispiel: Bei einer Distanz zwischen den beiden Antennen von 8 km ergibt sich im 2,4 GHz-Band die Masthöhe über dem höchsten Störobjekt von ca. **13 m**, im 5 GHz-Band zu **9 m**.

Antennen-Leistungen

Die Leistungen der eingesetzten Antennen müssen so ausgelegt sein, dass eine ausreichende Datenübertragungsrate erreicht wird. Auf der anderen Seite dürfen die länderspezifischen gesetzlichen Vorgaben für die maximal abgestrahlten Leistungen nicht überschritten werden.

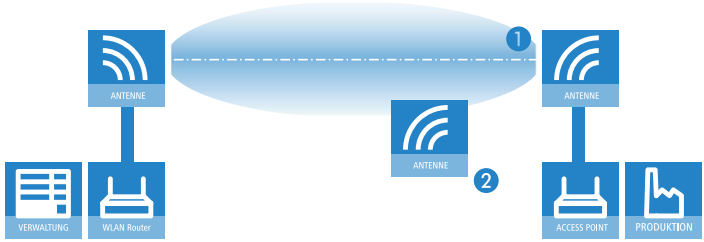
Die Berechnung der effektiven Leistungen führt dabei vom Funkmodul im sendenden AP bis zum Funkmodul im empfangenden AP. Dazwischen liegen dämpfende Elemente wie die Kabel, Steckverbindungen oder einfach die übertragende Luft und verstärkende Elemente wie die externen Antennen.



Ausrichten der Antennen für den P2P-Betrieb

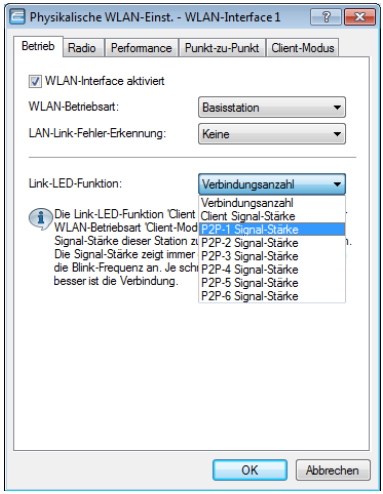
Hinweis: Der Schutz der verwendeten Komponenten vor den Folgen von Blitzeinschlag oder anderen elektrostatischen Vorgängen ist einer der wichtigsten Aspekte bei der Auslegung und Installation von WLAN-Systemen im Outdoor-Einsatz. Bitte beachten Sie die entsprechenden Hinweise zum → 'Blitz- und Überspannungsschutz', da Hirschmann ansonsten keine Garantie für Schäden an den Komponenten übernehmen kann. Informationen zur Installation von WLAN-Systemen im Outdoor-Einsatz finden Sie im 'Hirschmann Outdoor Wireless Guide'.

Beim Aufbau von P2P-Strecken kommt der genauen Ausrichtung der Antennen eine große Bedeutung zu. Je besser die empfangende Antenne in der „Ideallinie“ der sendenden Antenne liegt, desto besser ist die tatsächliche Leistung und damit die nutzbare Bandbreite **1**. Liegt die empfangende Antenne jedoch deutlich neben dem idealen Bereich, sind erhebliche Leistungsverluste zu erwarten **2**.

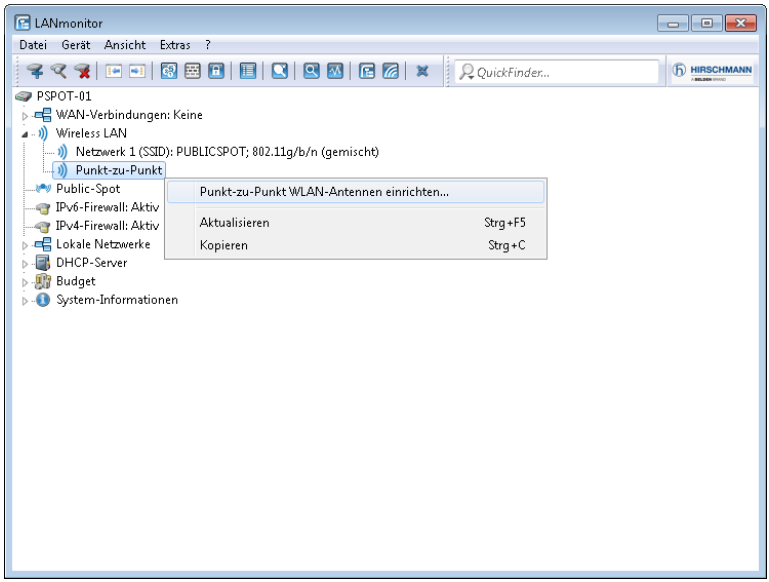


Um die Antennen möglichst gut ausrichten zu können, kann die aktuelle Signalqualität von P2P-Verbindungen über die LEDs des Gerätes oder im LANmonitor angezeigt werden.

Die Anzeige der Signalqualität über die LEDs muss für die physikalische WLAN-Schnittstelle aktiviert werden (LANconfig: **Wireless LAN** / **Allgemein** / **Physikalische WLAN-Einstellungen** / **Betrieb**). Je schneller die LED blinkt, umso besser ist die Verbindung (eine Blinkfrequenz von 1 Hz steht für eine Signalqualität von 10 dB, eine Verdoppelung der Frequenz zeigt die jeweils doppelte Signalstärke).



Im LANmonitor kann die Anzeige der Verbindungsqualität über das Kontext-Menü geöffnet werden. Ein Klick mit der rechten Maustaste auf den Eintrag 'Punkt-zu-Punkt' erlaubt den Aufruf 'Punkt-zu-Punkt WLAN-Antennen einrichten ...'



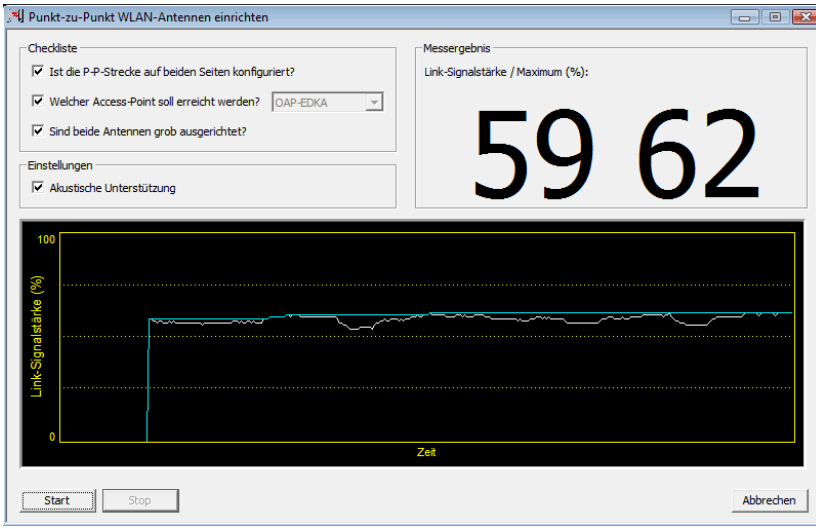
Hinweis: Der Eintrag 'Punkt-zu-Punkt' ist im LANmonitor nur sichtbar, wenn in dem überwachten Gerät mindestens eine Basisstation als Gegenstelle für eine P2P-Verbindung eingerichtet ist (LANconfig: **Wireless LAN** / **Allgemein** / **Physikalische WLAN-Einstellungen** / **Punkt-zu-Punkt**).

Im Dialog zur Einrichtung der Punkt-zu-Punkt-Verbindung fragt der LANmonitor die Voraussetzungen für den P2P-Verbindungsaufbau ab:

- Ist die P2P-Strecke auf beiden Seiten konfiguriert (gegenüberliegende Basisstation mit MAC-Adresse oder Stations-Namen definiert)?
- Ist die Punkt-zu-Punkt-Betriebsart aktiviert?
- Welcher AP soll überwacht werden? Hier können alle im jeweiligen Gerät als P2P-Gegenstelle eingetragenen Basis-Stationen ausgewählt werden.
- Sind beide Antennen grob ausgerichtet? Die Verbindung über die P2P-Strecke sollte schon grundsätzlich funktionieren, bevor die Einrichtung mit Hilfe des LANmonitors gestartet wird.

Der P2P-Dialog zeigt nach dem Start der Signalüberwachung jeweils die absoluten Werte für die aktuelle Signalstärke sowie den Maximalwert seit dem

Start der Messung. Zusätzlich wird der zeitliche Verlauf mit dem Maximalwert in einem Diagramm angezeigt.



Bewegen Sie zunächst nur eine der beiden Antennen, bis Sie den Maximalwert erreicht haben. Stellen Sie dann die erste Antenne fest und bewegen Sie auch die zweite Antenne in die Position, bei der Sie die höchste Signalqualität erzielen.

Vermessung von Funkstrecken

Nach der Planung und Einrichtung kann die Funkstrecke vermessen werden, um den tatsächlichen Datendurchsatz zu bestimmen.

Weitere Informationen zu den verwendeten Tools und zum Mess-Aufbau finden Sie im *WLAN Outdoor Guide* als Download unter *e-catalog.beldensolutions.com*.

Punkt-zu-Punkt-Betriebsart aktivieren

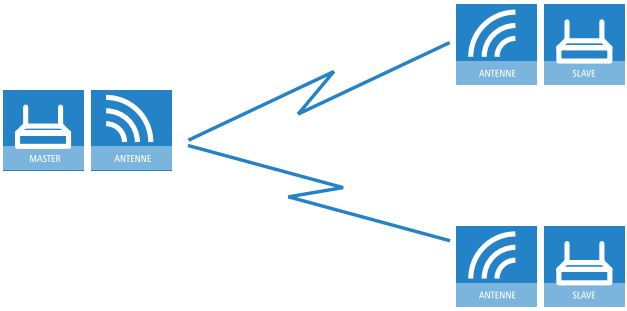
Das Verhalten eines APs beim Datenaustausch mit anderen APs wird in der „Punkt-zu-Punkt-Betriebsart“ festgelegt:

- **Aus:** Der AP kann nur mit mobilen Clients kommunizieren

- **An:** Der AP kann mit anderen Basis-Stationen und mit mobilen Clients kommunizieren
- **Exklusiv:** Der AP kann nur mit anderen Basis-Stationen kommunizieren

Bei der automatischen Suche nach einem freien WLAN-Kanal kann es im 5 GHz-Band zu gleichzeitigen Sendeversuchen mehrerer APs kommen, die sich in der Folge gegenseitig nicht finden. Diese Pattsituation kann mit dem geeigneten „Kanalwahlverfahren“ verhindert werden:

- **Master:** Dieser AP übernimmt die Führung bei der Auswahl eines freien WLAN-Kanals.
- **Slave:** Alle anderen APs suchen solange nach dem freien Kanal, bis sie einen sendenden Master gefunden haben.



Es ist daher empfehlenswert, im 5 GHz-Band jeweils einen zentralen AP als 'Master' und alle anderen Punkt-zu-Punkt-Partner als 'Slave' zu konfigurieren. Auch im 2,4 GHz-Band bei aktivierter automatischer Kanalsuche erleichtert diese Einstellung den Aufbau von Punkt-zu-Punkt-Verbindungen.

Hinweis: Für die Verschlüsselung von Punkt-zu-Punkt-Verbindungen mit 802.11i/WPA ist die korrekte Konfiguration der Kanalwahlverfahren zwingend erforderlich (ein Master als Authentication Server und ein Slave als Client).

Hinweis: Die automatische Kanalwahl für P2P-Verbindungen im 5 GHz-Bereich ist nur aktiv, wenn das ausgewählte Länderprofil DFS unterstützt.

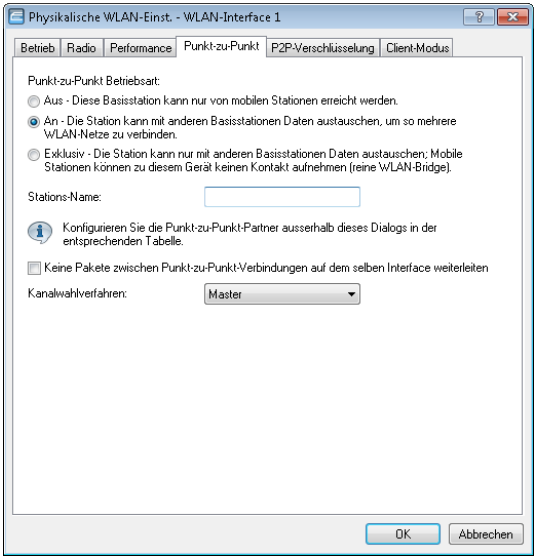
Konfiguration von P2P-Verbindungen

Bei der Konfiguration von Punkt-zu-Punkt-Verbindungen (P2P-Verbindungen) geben Sie neben der Punkt-zu-Punkt-Betriebsart und dem Kanalwahlverfahren wahlweise die MAC-Adressen oder die Stationsnamen der Gegenstellen an. Die Konfiguration kann in LANconfig entweder über den Setup-Assistenten **WLAN konfigurieren** oder manuell über den Konfigurationsdialog erfolgen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie manuell eine verschlüsselte oder unverschlüsselte P2P-Basis-Konfiguration erstellen.

Hinweis: Parallel zu einer P2P-Verbindung spannen die betreffenden APs automatisch je eine fixe SSID ***** P2P INFO ***** auf. Diese SSID dient als reines Verwaltungsnetz für den Verbindungaufbau und die Erreichbarkeitsprüfung ('Alive') eines Punkt-zu-Punkt-Partners. Den WLAN-Clients ist es nicht möglich, sich mit solch einem Netz zu verbinden.

1. Öffnen Sie den Konfigurationsdialog für das Gerät, das als P2P-Master bzw. P2P-Slave agieren soll, und wechseln Sie auf die Seite **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.**.
2. Wählen Sie das WLAN-Interface aus, welches Sie ausschließlich für die P2P-Verbindung benutzen wollen, und wechseln Sie auf die Registerkarte **Punkt-zu-Punkt**.



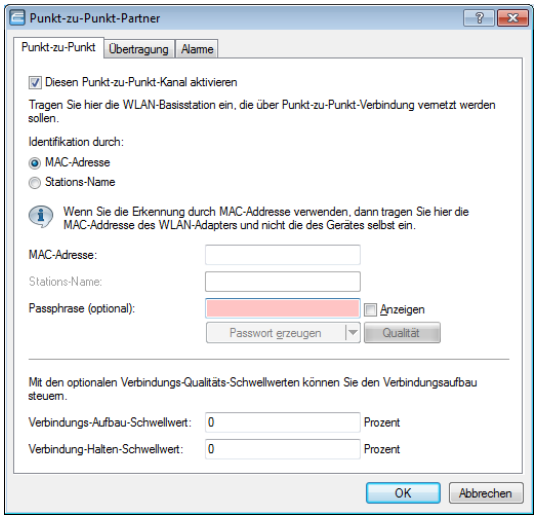
3. Aktivieren Sie die gewünschte **Punkt-zu-Punkt Betriebsart**, z. B. **An**.
4. Setzen Sie das **Kanalwahlverfahren** auf **Master** bzw. **Slave**.
5. Optional: Sofern die Gegenstelle die physikalische Schnittstelle nicht über die MAC-Adresse, sondern einen Alias-Namen identifizieren soll, geben Sie im Eingabefeld **Stations-Name** eine entsprechende Bezeichnung ein, z. B. P2P_MASTER bzw. P2P_SLAVE.
6. Optional: Passen Sie auf der Registerkarte **Verschlüsselung** bei Bedarf die Einstellungen für die IEEE 802.11i-Verschlüsselung der P2P-Verbindung an.

   Mit IEEE 802.11i lässt sich die Sicherheit von Punkt-zu-Punkt-Verbindungen im WLAN deutlich verbessern. Alle Vorteile von 802.11i wie die einfache Konfiguration und die starke Verschlüsselung mit AES stehen damit im P2P-Betrieb ebenso zur Verfügung wie die verbesserte Sicherheit der Passphrases durch LANCOM Enhanced Passphrase Security (LEPS).

   Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der physikalischen WLAN-Interfaces, siehe *WLAN-Verschlüsselungs-Einstellungen* auf Seite 1101. Standardmäßig ist die P2P-Verschlüsselung aktiviert und mit sinnvollen Werten vorbelegt.

Hinweis: In HiLCOS-Versionen vor 8.90 sind die Einstellungen zur Verschlüsselung an die Einstellungen für das erste logische WLAN-Netz im verwendeten physikalischen WLAN-Interface gekoppelt (also WLAN-1, wenn Sie das erste WLAN-Modul für die P2P-Verbindung nutzen; WLAN-2, wenn Sie das zweite WLAN-Modul bei einem AP mit zwei WLAN-Modulen nutzen). In diesem Fall finden Sie die Einstellungen unter **Wireless-LAN** > **802.11i/WEP** > **WPA- / Einzel-WEP-Einstellungen**.

7. Schließen Sie den Dialog mit **OK** und wählen Sie im Konfigurationdialog auf der gleichen Seite unter **Punkt-zu-Punkt-Partner** eine logische P2P-Verbindung aus, z. B. **P2P-1-1**.



8. Aktivieren Sie auf der Registerkarte **Punkt-zu-Punkt** den gewählten P2P-Kanal und geben Sie an, ob Ihr Gerät die Gegenstelle über eine **MAC-Adresse** oder einen **Stations-Name**n identifiziert. Je nach Auswahl tragen Sie anschließend im gleichnamigen Eingabefeld entweder die MAC-Adresse des physikalischen WLAN-Interfaces, das die Gegenstelle für die P2P-Verbindung benutzt, oder deren Stations-Namen ein.
   Sie finden die WLAN-MAC-Adresse auf einem Aufkleber, der unterhalb des jeweiligen Antennenanschlusses am Gehäuse des Gerätes angebracht ist. Verwenden Sie nur die als "WLAN-MAC" oder "MAC-ID" gekennzeichnete Zeichenkette. Bei den anderen ggf. angegebenen Adressen handelt

es sich nicht um die WLAN-MAC-Adresse, sondern um die LAN-MAC-Adresse!

Alternativ finden Sie die MAC-Adresse auch im Status-Menü unter **WLAN** > **Interfaces** > **MAC-Adresse**.

9. Geben Sie unter **Passphrase** ein gemeinsames Kennwort aus mindestens 8 Zeichen an (empfohlen: 32 Zeichen), mit dem Sie die P2P-Verbindung zusätzlich verschlüsseln. Die P2P-Verschlüsselung muss dafür aktiviert sein (siehe oben).
   In der Einstellung als P2P-Master wird die hier eingetragene Passphrase verwendet, um die Zugangsberechtigung der Slaves zu prüfen. In der Einstellung als P2P-Slave überträgt der AP diese Informationen an die Gegenseite, um sich dort anzumelden.
10. Optional: Wechsel Sie auf die Registerkarte **Übertragung**, um die Grenzwerte und Einstellung für die Paketübertragung vorzunehmen.

    Die Einstellungsmöglichkeiten sind weitgehend identisch mit denen der logischen WLAN-Netze, siehe *Einstellungen für die Übertragung* auf Seite 1132). Standardmäßig sind sämtliche Parameter auf Optimierung und Automatik ausgerichtet.

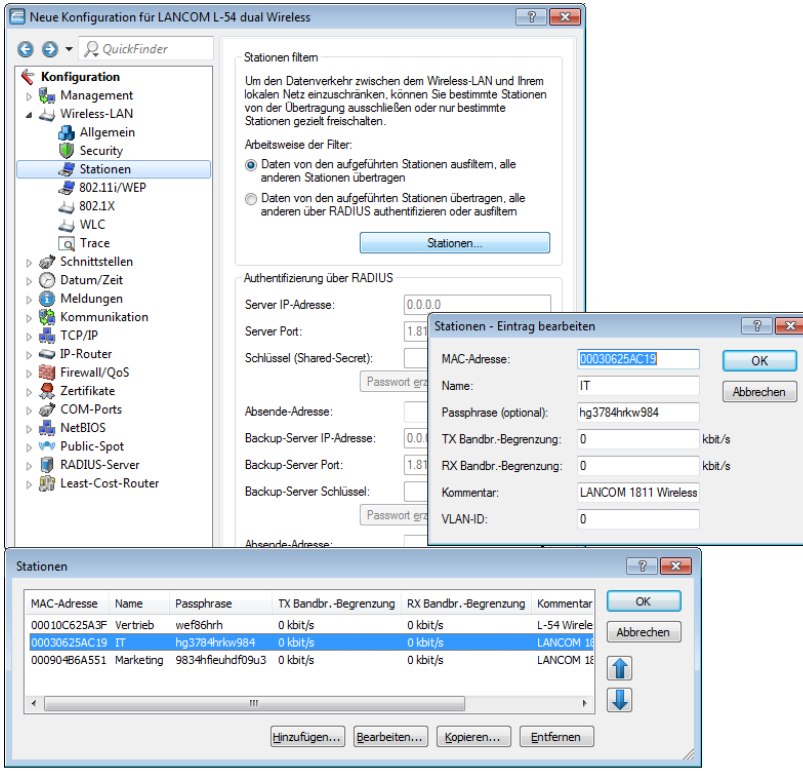
11. Schließen Sie den Dialog mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
12. Nehmen Sie die äquivalenten Konfigurationsschritte für die Gegenstelle (Slave bzw. Master) vor.

LEPS für P2P-Verbindungen

Einen weiteren Sicherheitsgewinn erzielen Sie durch die zusätzliche Verwendung der LANCOM Enhanced Passphrase Security (LEPS), also der Verknüpfung der MAC-Adresse mit der Passphrase.

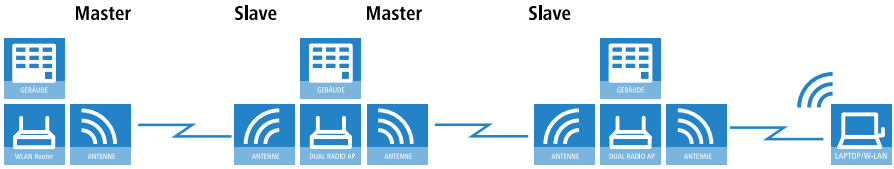
Mit LEPS können einzelne Punkt-zu-Punkt-Strecken (P2P) mit einer individuellen Passphrase abgesichert werden. Wenn bei einer P2P-Installation ein AP entwendet wird und dadurch Passphrase und MAC-Adresse bekannt werden, sind alle anderen per LEPS abgesicherten WLAN-Strecken weiterhin sicher.

Bei der Konfiguration mit LANconfig geben Sie die Passphrases der im WLAN zugelassenen Stationen (MAC-Adressen) im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte 'Stationen' unter der Schaltfläche **Stationen** ein.



Access Points im Relais-Betrieb

APs mit zwei Funkmodulen können Funkbrücken über mehrere Stationen hinweg aufbauen. Dabei wird jeweils ein WLAN-Modul als 'Master', das zweite als 'Slave' konfiguriert.



Hinweis: Mit dem Einsatz von Relais-Stationen mit jeweils zwei WLAN-Modulen wird gleichzeitig das Problem der „hidden station“ reduziert.

12.9 Zentrales WLAN-Management

Der weit verbreitete Einsatz von APs hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Bei allen Vorzügen der WLAN-Strukturen bleiben einige offene Aspekte:

- Alle APs benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der APs erfordert gerade bei größeren WLAN-Strukturen mit entsprechenden Sicherheitsmechanismen eine hohe Qualifikation und Erfahrung der Verantwortlichen und bindet erhebliche Ressourcen in den IT-Abteilungen.
- Die manuelle Anpassung der Konfigurationen in den APs bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- APs an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können. Außerdem können ggf. unbemerkt fremde APs mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

Mit einem zentralen WLAN-Management werden diese Probleme gelöst. Die Konfiguration der APs wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC). Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus. Da die vom WLC zugewiesene Konfiguration in den APs optional **nicht** im Flash, sondern im RAM abgelegt wird, können in besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im „autarken Weiterbetrieb“ wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

12.9.1 Stationstabelle (ACL-Tabelle)

Mit Hilfe der Stationstabelle legen Sie fest, welche WLAN-Clients sich in den WLANs anmelden können, die der WLC zentral verwaltet. Außerdem können sie den einzelnen WLAN-Clients auf diesem Wege sehr komfortabel eine Passphrase zur Authentifizierung und eine VLAN-ID zuweisen.

Zur Nutzung der Stationstabelle muss grundsätzlich der RADIUS-Server im WLC aktiviert sein. Alternativ kann auch eine Weiterleitung zu einem anderen RADIUS-Server konfiguriert werden.

Für jedes logische WLAN-Netzwerk, in dem die WLAN-Clients über RADIUS geprüft werden sollen, muss die MAC-Prüfung aktiviert werden.

12.9.2 Zertifikats-Backup aus dem Gerät herunterladen

1. Wählen Sie **Dateimanagement** / **Zertifikat oder Datei herunterladen**.
2. Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA und bestätigen Sie mit **Download starten**:
   - PKCS12-Container mit CA-Backup
   - PKCS12-Container mit RA-Backup

Die Backup-Datei wird damit auf Ihren Datenträger gespeichert. Die Passphrase wird erst beim Einspielen in einen WLC wieder benötigt.

12.10 Bandbreitenbegrenzung im WLAN

Zur besseren Verteilung der Bandbreite bei mehreren Teilnehmern im WLAN können die verfügbaren Bandbreiten begrenzt werden. Diese Bandbreitenbegrenzung bietet sich z. B. an für Wireless ISPs, die Ihren Kunden nur eine definierte Bandbreite zur Verfügung stellen wollen.

Hinweis: Im Gegensatz zu Bandbreitenmanagement mit Hilfe von QoS (Quality of Service) wird mit diesem Verfahren keine Mindest-Bandbreite eingeräumt, sondern eine exakt definierte Maximal-Bandbreite. Auch wenn durch den geringen Traffic anderer Netzteilnehmer eigentlich mehr Bandbreite verfügbar wäre, wird dem Benutzer hier immer nur die vorgegebene Bandbreite bereitgestellt.

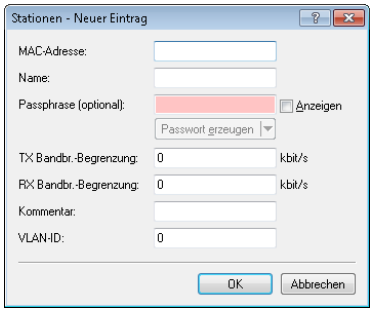
Die Einstellungen unterscheiden den Betrieb eines Gerätes als AP oder im Client-Modus.

12.10.1 Einstellung als Access Point

In der Betriebsart als AP können die maximal zulässigen Bandbreiten in Tx- und RX-Richtung für die WLAN-Clients festgelegt werden, die sich beim AP einbuchen. Dazu werden in der MAC-Zugangs-Liste die Werte für die maximale Tx- und Rx-Bandbreite in kBit/s eingetragen. Ein Wert von '0' signalisiert, dass in dieser Übertragungsrichtung keine Beschränkung der Bandbreite vorgesehen ist. Aus dem hier eingetragenen Wert und dem ggf. vom Client übermittelten Wert wird die tatsächlich bereitgestellte Bandbreite ermittelt.

Hinweis: Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für „Daten senden“ und Tx für „Daten empfangen“.

Die maximalen Bandbreiten für die angeschlossenen Clients werden im LANconfig im Konfigurationsbereich 'Wireless-LAN' auf der Registerkarte 'Stationen' in der MAC-Zugangs-Liste eingetragen.



- Kommentar

  Kommentar zu diesem Eintrag.

- VLAN-ID

  VLAN-ID für den WLAN-Client.

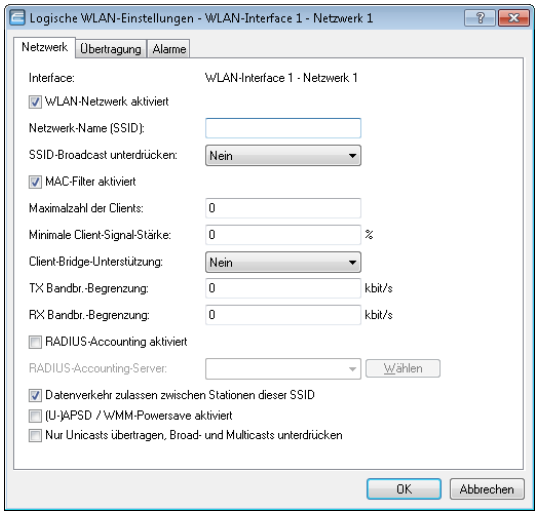
  - Mögliche Werte: 0 bis 4094
  - Besondere Werte: 0 schaltet die Verwendung von VLAN-Tagging aus.

12.10.2 Einstellung als Client

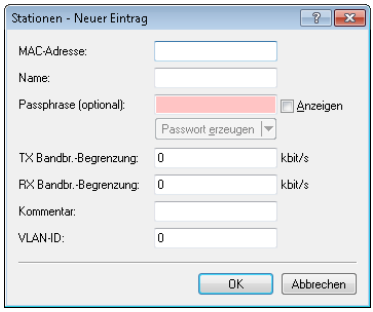
Wird das Gerät selbst als WLAN-Client betrieben, kann das Gerät beim Einbuchen beim AP seine maximalen Bandbreiten übermitteln. Der AP bildet dann mit ggf. eigenen Limits für diesen Client die tatsächlichen maximalen Bandbreiten.

Hinweis: Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als Client steht Tx für „Daten senden“ und Rx für „Daten empfangen“.

Die maximalen Bandbreiten für ein Gerät im Client-Modus werden im LANconfig unter **Wireless-LAN** > **Allgemein** mit einem Klick auf **Logische WLAN-Einstellungen** und Auswahl der entsprechenden logischen WLAN-Schnittstelle auf der Registerkarte **Netzwerk** eingetragen.



Im WLC finden Sie die Bandbreitenbegrenzung der einzelnen Stationen unter **WLAN-Controller** > **Stationen** nach einem Klick auf **Stationen**.



12.10.3 Bandbreitenbeschränkung der LAN-Schnittstellen

Einleitung

Bei einem Gerät mit integriertem WLAN-Modul können Sie ein Bandbreitenlimit für einzelne LAN-Schnittstellen definieren. Die Tabelle der LAN-Schnittstellen bietet zur Konfiguration der Bandbreitenbeschränkung die entsprechenden Parameter.

12.11 Automatische Anpassung der Übertragungsrate für Multicast- und Broadcast-Sendungen

Während bei Unicast-Sendungen AP und Client die optimale Übertragungsgeschwindigkeit miteinander aushandeln können, findet systembedingt bei Multicast- und Broadcast-Sendungen die Kommunikation nur in eine Richtung statt: Vom AP zum Client. Die Clients können dem AP nicht zurückmelden, mit welcher maximalen Übertragungsgeschwindigkeit sie tatsächlich kommunizieren können.

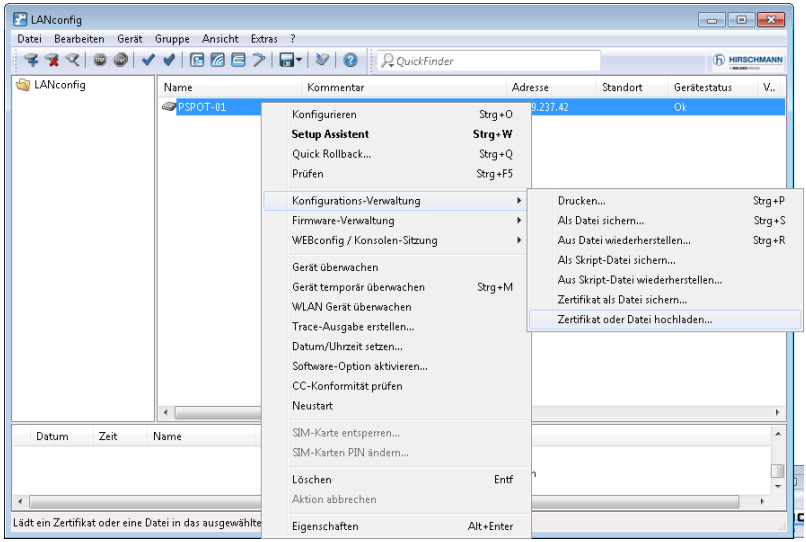
Der AP hat zwei Möglichkeiten, die Übertragungsgeschwindigkeit für Multicast- und Broadcast-Sendungen festzulegen:

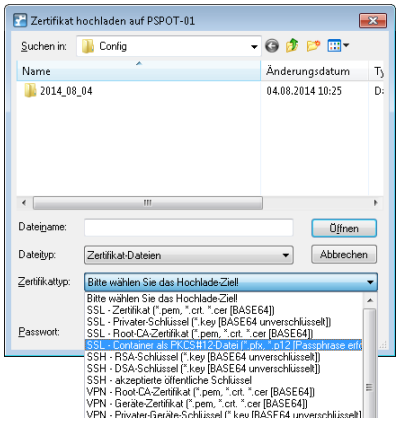
- **Feste Bitrate**: Die Übertragungsrate ist so bemessen, dass der langsamste Client im WLAN auch unter ungünstigen Bedingungen die Sendungen fehlerfrei und verständlich erhalten kann. Das kann dazu führen, dass der AP selbst dann mit einer geringeren Übertragungsrate sendet, wenn Umgebungsbedingungen und Clients eigentlich eine höhere Rate erlauben würden. Doch damit würde der AP das WLAN unnötig ausbremsen.
- **Automatische Bitrate**: Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

12.12 Mehrstufige Zertifikate für Public Spots

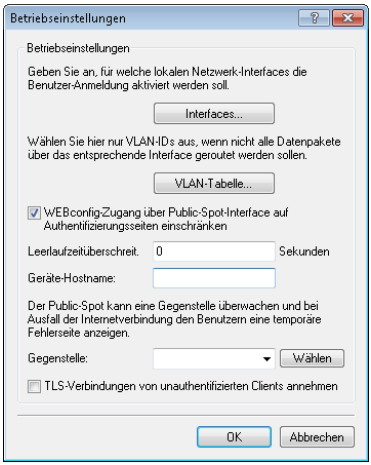
SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das Gerät geladen werden. Diese Zertifikatsketten können für die Public Spot-Authentifizierungsseiten über den im Gerät implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im Public Spot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei Public Spot-Authentifizierungen zu vermeiden.

Das Zertifikat laden Sie über LANconfig im Dateimanagement mit den einzelnen Dateien des Root-CA-Zertifikats oder als PKCS#12-Container in das Gerät:



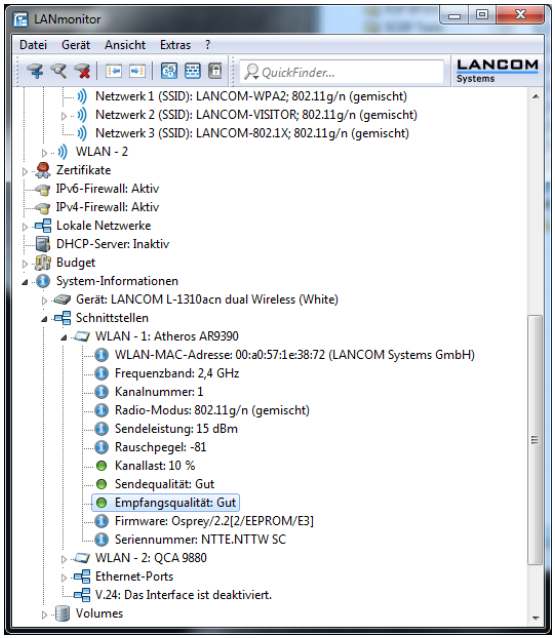


Da Zertifikate üblicherweise auf DNS-Namen ausgestellt werden, muss der Public Spot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (einzugeben unter **Public-Spot** > **Server** > **Betriebseinstellungen** bei **Geräte-Hostname**). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des Public Spots aufgelöst werden.

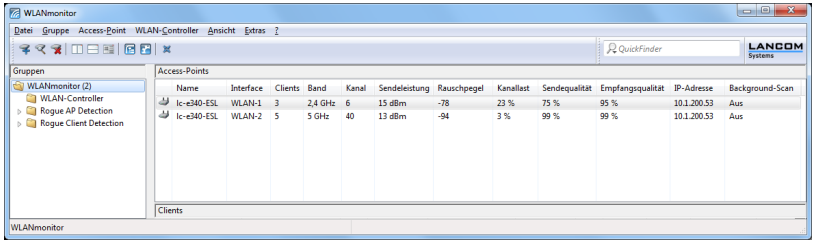


12.13 LANCOM "Wireless Quality Indicators" (WQI)

LANmonitor bietet Ihnen die Möglichkeit, die Signalqualität der einzelnen Schnittstellen anhand von **Wireless Quality Indicators** anzuzeigen. Diese Darstellung von Empfangs- und Sendequalität (RX und TX) dient der schnellen Identifizierung der Signalqualität. Öffnen Sie zum Anzeigen dieser Informationen im LANmonitor den Bereich **System-Informationen** des Gerätes. Unter **Schnittstellen** werden Ihnen die Indikatoren angezeigt.



Der WLANmonitor zeigt Ihnen die **Wireless Quality Indicators** ebenfalls an. Klicken Sie hierfür auf den Gruppen-Hauptordner.

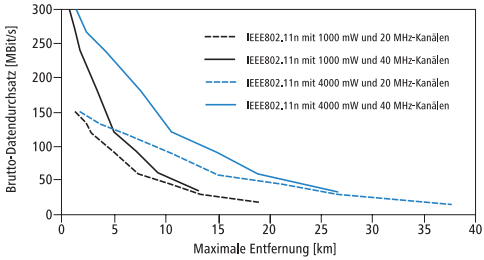


12.14 BFWA – mehr Sendeleistung für mehr Reichweite

BFWA steht für breitbandige, ortsfeste Funkstrecken, mit denen beispielsweise von einem Netzknoten ausgehend Verbindungen mit dem Internet für die

angeschlossenen Teilnehmer zur Verfügung gestellt werden können. Die Frequenzen wurden im Rahmen einer Allgemeinzuteilung von der Bundesnetzagentur bereitgestellt. BFWA funkt im 5,8 GHz-Bereich. Die maximal zulässige Sendeleistung beim Betrieb von BFWA-Funkstrecken liegt bei 4000 mW EIRP (Equivalent Isotropic Radiated Power).

In dieser hohen zulässigen Sendeleistung liegt der Vorteil von BFWA. Denn ohne BFWA ist die zulässige maximale Sendeleistung für Outdoor WLAN-Richtfunksysteme im 5 GHz-Band auf 1000 mW beschränkt. Durch die Vervierfachung der zulässigen Strahlungsleistung können mit denselben Richtfunksystemen deutlich größere Distanzen überbrückt werden.



OpenBAT APs auf Basis von 802.11n sowie alle aktuellen OpenBAT 54 Mbit/s APs unterstützen BFWA ab der HiLCOS-Version 7.70. Bei älteren APs ist die Unterstützung abhängig vom Chipsatz (AR-5414 Chipsatz). Der Hirschmann-Support informiert Sie bei diesen Modellen über eine mögliche Unterstützung von BFWA.

12.15 WLAN Band Steering

Der Standard IEEE 802.11 enthält kaum Kriterien, nach denen ein WLAN-Client den AP für eine Verbindung auswählen sollte. Zwar gibt es allgemeine Richtlinien, wonach z. B. ein AP mit höherem RSSI-Wert (d. h. der empfangenen Signalstärke) zu bevorzugen ist. Doch in der Praxis beachten WLAN-Clients weder die oben angesprochenen Definitionen noch die allgemeinen Richtlinien konsequent. Wird eine SSID in sowohl 2,4 GHz als auch 5 GHz ausgestrahlt, besteht im Normalfall keine Möglichkeit auf die Entscheidung des Clients, welches Frequenzband er bevorzugt, Einfluss zu nehmen.

Die gezielte Zuweisung von WLAN-Clients, das sog. "Client Steering", basiert auf dem Prinzip, dass viele Clients die verfügbaren APs durch einen aktiven Scan-Vorgang ermitteln. Aktives Scannen bedeutet hier, dass ein Client Test-Anforderungspakete (Probe Requests) versendet, welche die Netzwerkkennung enthalten, zu der ein Client eine Verbindung aufbauen soll. APs mit der entsprechenden Kennung versenden daraufhin eine Test-Antwort und ermöglichen es dem Client auf diese Weise, eine Liste mit verfügbaren APs zu erstellen. Die Tatsache, dass die weitaus meisten WLAN-Clients sich nur mit solchen APs verbinden, von denen sie eine Test-Antwort (Probe Response) erhalten haben, kann zur Steuerung des Auswahlverhaltens (und somit zur gezielten Zuweisung) eingesetzt werden.

Für die gezielte Zuweisung gibt es mehrere, zum Teil sehr fortgeschrittene Kriterien. Eines dieser Kriterien betrifft die verwendeten Funkfrequenzbereiche, in denen Clients kommunizieren. So erwartet man von modernen Dual-Band-WLAN-Clients immer häufiger, dass diese den 5-GHz-Frequenzbereich gegenüber dem inzwischen überfüllten 2,4-GHz-Bereich bevorzugen. Weist man einem WLAN-Client ganz gezielt ein bestimmtes Frequenzband bzw. einen bestimmten Frequenzbereich zu, spricht man von Band Steering.

Die Liste mit den ermittelten (bzw. "gesehenen") Clients enthält alle Clients, von denen der AP ein Test-Anforderungspaket empfangen hat. Zusammen mit der Funkfrequenz, auf der der WLAN-Client die Test-Anforderung gesendet hat, bildet diese Liste eine der Entscheidungsgrundlagen für den AP, die betreffende Anforderung zu beantworten oder nicht.

Weitere Kriterien für eine solche Entscheidungsfindung hängen mit den gemeldeten Kennungen der Clients und der Konfiguration der Geräte zusammen: So kann es z. B. vorkommen, dass auf dem bevorzugten Frequenzband weniger SSIDs gemeldet werden als auf dem weniger bevorzugten. Ebenso kann eine zu geringe Sendestärke beim Melden der SSIDs dazu führen, dass der Client auf dem bevorzugten Frequenzband keine Test-Antwort erhält. Für den letzteren Fall sollte man sicherstellen, dass der AP Test-Antworten auf dem weniger bevorzugten Frequenzband nicht durch den Steuerungsmechanismus unterdrückt. Die dafür verantwortliche, minimale Signalstärke können Sie über die folgenden Wege einstellen:

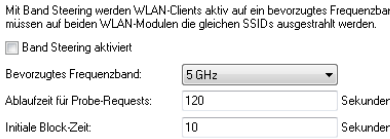
- **LANconfig: Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **Netzwerk** > **Minimale Client-Signal-Stärke**
- **WEBconfig: Setup** > **Schnittstellen** > **WLAN** > **Netzwerk** > **Minimal-Stations-Staerke**

Sie können das Band-Steering des APs im LANconfig unter **Wireless-LAN** > **Band Steering** aktivieren und verwalten.

Hinweis: WLAN Band Steering ist Bestandteil von *LANCOM Active Radio Control (ARC)*

12.15.1 Band Steering konfigurieren

Dieser Dialog bietet Ihnen die Möglichkeit, die Einstellungen für das Band Steering in LANconfig vorzunehmen.



Unter **Wireless-LAN** > **Band Steering** stehen Ihnen folgende Funktionen zur Verfügung:

Band Steering aktiviert

Aktiviert oder deaktiviert diese Funktion.

Bevorzugtes Frequenzband

Gibt das Frequenzband vor, auf welches das Gerät WLAN-Clients leitet. Mögliche Werte sind:

- **2,4GHz**: Das Gerät leitet Clients auf das Frequenzband 2,4GHz.
- **5GHz**: Das Gerät leitet Clients auf das Frequenzband 5GHz.

Ablaufzeit für Probe-Requests

Der Zeitraum, während dessen der AP den WLAN-Client auf das bevorzugte Frequenzband leitet. Der Standardwert lautet 120 Sekunden.

Initiale Block-Zeit

Geht ein AP mit einem 5GHz-DFS-Funkmodul und aktiviertem Band Steering erstmalig oder nach einem Neustart in Betrieb, kann er während des DFS-Scans keine Dual-Band-fähigen WLAN-Clients erkennen. Als Folge kann der AP einen vorhandenen WLAN-Client nicht auf ein ggf.

bevorzugtes 5GHz-Band leiten. Stattdessen würde das 2,4GHz-Funkmodul die Anfrage des Clients beantworten und ihn auf das 2,4GHz-Band leiten.

Durch die Eingabe einer initialen Block-Zeit beantwortet das auf 2,4GHz konfigurierte Funkmodul des APs Anfragen eines WLAN-Clients um die entsprechend angegebene Zeit später. Der Default-Wert ist 10 Sekunden.

Durch die verzögerte Antwort auf 2,4GHz-Probe-Responses veranlasst der AP zusätzlich einen WLAN-Client, der ggf. den 5GHz-Scan überspringt, weil er bereits einen AP auf 2,4GHz erwartet, erneut auf 5GHz zu scannen.

Hinweis: Das Einbuchen eines reinen 2,4GHz-WLAN-Clients erfolgt ebenfalls erst nach der eingestellten Verzögerungszeit. Wenn keine 5GHz-WLAN-Clients im Netzwerk vorhanden sind, sollte die Verzögerungszeit 0 Sekunden betragen.

12.16 Dynamic Frequency Selection (DFS)

Beim für 5GHz-WLANs geforderten DFS-Verfahren (Dynamic Frequency Selection) wählt das Gerät automatisch eine freie Frequenz, z. B. um Radaranlagen nicht zu stören. Die Signale von Wetter-Radarstationen waren jedoch manchmal nicht sicher zu erkennen.

Die europäische Kommission forderte daher in Ergänzung zu den Standards ETSI EN 301 893 V1.3.1 und ETSI EN 301 893 V1.4.1, im Unterband 2 des 5GHz-Bandes drei Kanäle (120, 124 und 128) auszusparen und solange nicht für die automatische Kanalwahl zu verwenden, bis Verfahren zur Erkennung der Wetter-Radar-Signaturen zur Verfügung stehen. Man bezeichnete die Version EN 301 893 V1.3 und EN 301 893 V1.4 kurz als "DFS-2"

Mitte 2010 trat die neue Version ETSI EN 301 893 V1.5.1 in Kraft, die einige Veränderungen für die Nutzung von WLAN-Frequenzen in den Bereichen 5,25 - 5,35 GHz und 5,47 - 5,725 GHz mit sich brachte. Die neue Version 1.5.1 regelte das DFS-Verfahren für diese Frequenzbereiche, um Radarstationen vor dem Einfluss durch WLAN-Systeme zu schützen. Bei der Erkennung von bestimmten Mustern in den empfangenen Funksignalen können seitdem WLAN-Systeme mit Hilfe von DFS die Radarstationen erkennen und einen automatischen Wechsel der verwendeten Kanäle durchführen. Im Unterschied

zu den bisherigen Regelungen bezeichnete man die aktualisierte DFS-Version nach EN 301 893-V1.5 kurz als "DFS-3".

Generell bestimmen die Werte Pulsrate, Pulsbreite und Anzahl der Pulse ein Pulsmuster. Die bisherigen DFS-Verfahren gaben vor, nur feste Radarmuster zu prüfen, die durch definierte Kombinationen verschiedener Pulsraten und Pulsbreiten im WLAN-Gerät hinterlegt waren. Nach DFS3 konnte das Gerät nun auch Muster aus wechselnden Pulsraten und Pulsbreiten als Radarmuster erkennen. Außerdem konnten innerhalb eines Radarsignals zwei oder drei unterschiedliche Pulsraten verwendet werden.

Am 01.01.2013 endete die Gültigkeit der Version ETSI EN 301 893 V1.5.1 (DFS-3). Danach galt die neue Version ETSI EN 301 893 V1.6.1 (kurz "DFS-4"), die auch kürzere Radarimpulse erkennt.

Am 31.12.2014 endete die Gültigkeit der Version ETSI EN 301 893 V1.6.1 (DFS-4). Danach gilt die neue Version ETSI EN 301 893 V1.7.1, die einige Änderungen bzgl. der Signalstärke mit sich brachte.

Hinweis: Für die Erkennung von Wetterradaren (Kanäle 120, 124 und 128 im Frequenzbereich 5,6 - 5,65 MHz) gelten besondere Nutzungsbedingungen. Die DFS-Implementierung im HiLCOS unterstützt die verschärften Erkennungsbedingungen nicht. Deshalb werden diese drei Kanäle von neueren HiLCOS-Versionen ausgespart.

Arbeitsweise

Nach dem Einschalten oder Booten wählt das Gerät aus den (z. B. aufgrund der Ländereinstellungen) verfügbaren Kanälen einen zufälligen Kanal aus und prüft, ob es auf diesem Kanal ein Radarsignal findet und ob auf diesem Kanal schon ein anderes WLAN arbeitet. Diesen Scan-Vorgang wiederholt es solange, bis es einen radarfreien Kanal mit möglichst wenig anderen Netzwerken findet. Anschließend wird der gewählte Kanal erneut für 60 Sekunden beobachtet, um evtl. auftretende Radarsignale sicher auszuschließen. Die Datenübertragung kann daher durch diesen Scan-Vorgang und die erneute Suche eines freien Kanals für 60 Sekunden unterbrochen werden.

Um diese Pausen in der Datenübertragung bei jedem Kanalwechsel zu verhindern, verlegt ein Gerät den Scanvorgang **vor** die Auswahl eines konkreten Kanals. Die Informationen über die gescannten Kanäle werden in einer internen Datenbank gespeichert:

- Wurde auf dem Kanal ein Radarsignal gefunden?
- Wieviele andere Netzwerke wurden auf dem Kanal gefunden?

Mit Hilfe dieser Datenbank wählt der AP einen Kanal aus einer Liste der radarfreien Kanäle mit der geringsten Anzahl an anderen Netzwerken aus (das ist der Betriebskanal). Nach der Auswahl eines Kanals kann die Datenübertragung dann sofort ohne weitere Wartezeit beginnen.

- Die “Blacklist” dieser Datenbank speichert die Kanäle, die aufgrund der gefundenen Radarsignale geblockt werden. Diese Einträge verschwinden nach jeweils 30 Minuten aus der Liste, um die Informationen ständig auf dem aktuellen Stand zu halten.
- Die “Whitelist” der Datenbank speichert die Kanäle, auf denen kein Radarsignal gefunden wurde. Diese Einträge bleiben für die nächsten 24 Stunden gültig, können aber zwischenzeitlich beim Auftreten eines Radarsignals durch einen Eintrag in der Blacklist überschrieben werden.

Standardmäßig nutzt der AP dauerhaft den Kanal, der beim ersten Scan als Betriebskanal gewählt wurde. Die Verbindungen können beliebig lange auf dem vom DFS-Algorithmus gewählten Kanal bestehen bleiben, bis entweder ein Radarsignal erkannt wird oder die Funkzelle neu gestartet wird (z. B. bedingt durch Umkonfigurieren des Geräts, Firmware-Upload oder einen Neustart).

Ein erneuter 60-Sekunden-Scanvorgang ist unter den folgenden Voraussetzungen notwendig:

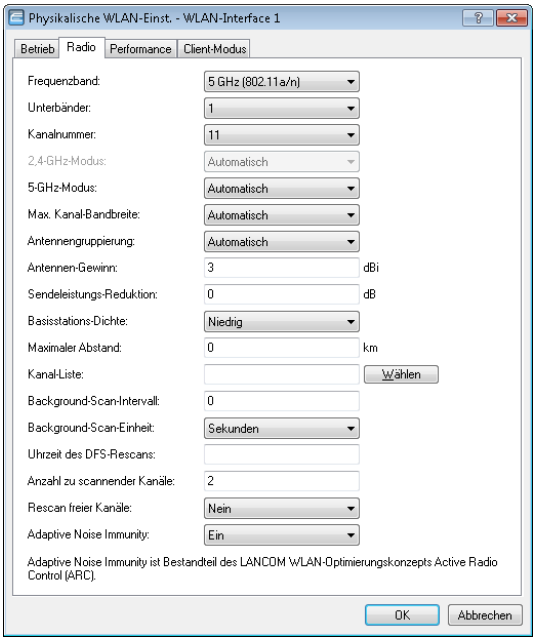
- Das Gerät wird eingeschaltet oder kalt gestartet. In diesem Fall ist die Datenbank leer, das Gerät kann nicht aus der Whitelist die bevorzugten Kanäle auswählen. Es ist ein Scanvorgang erforderlich.
- Innerhalb der ersten 24 Stunden nach dem Scanvorgang wird ein Kanalwechsel notwendig durch ein Radarsignal in der Reichweite des APs. In diesem Fall verfügt der AP über Alternativen in der Whitelist – er kann also den eingebuchten WLAN-Clients bzw. den P2P-Partnern den neuen Betriebskanal mitteilen und dann auf diesen Kanal wechseln. Die Dauer für diesen Vorgang liegt im Sekundenbereich, der Wechsel kann als unterbrechungsfrei angesehen werden.
- Das Gerät ist seit 24 Stunden in Betrieb, erst dann wird ein neuer Kanalscan notwendig. Die Einträge in der Whitelist sind aus der Datenbank “herausgealtert”, der AP hat keinen alternativen Kanal, den er direkt als Betriebskanal nutzen könnte. In diesem Fall muss die Datenbank durch einen

Scanvorgang neu gefüllt werden, es kommt zu einer einminütigen Unterbrechung des WLAN-Betriebs.

Hinweis: Grundsätzlich ist der Betreiber des WLANs zuständig für die Einhaltung der ETSI-Regelungen. Hirschmann empfiehlt daher den zeitnahen Umstieg auf eine Firmware-Version mit aktueller DFS-Unterstützung.

12.16.1 DFS-Konfiguration

In LANconfig konfigurieren Sie die DFS-Einstellungen unter **Wireless-LAN** > **Allgemein** durch einen Klick auf **Physikalische WLAN-Einst.** und Auswahl des Reiters **Radio**.



Uhrzeit des DFS-Rescans

Dieser Eintrag bestimmt, um welche Uhrzeit (0-24 Uhr) das Gerät die DFS-Datenbank löscht und einen DFS-Rescan durchführt. Ohne Eintrag führt das Gerät erst dann einen DFS-Rescan durch, wenn kein freier Kanal

mehr verfügbar ist. Das ist dann der Fall, wenn die beim initialen DFS-Scan ermittelte Kanalzahl die minimale Anzahl der freien Kanäle unterschreitet.

Tipp: Für die Definition der Uhrzeit lassen sich Möglichkeiten der cron-Befehle nutzen: Der Eintrag '1,6,13' startet den Rescan immer um 1 Uhr, 6 Uhr und 13 Uhr. Der Eintrag '0-23/4' startet alle vier Stunden einen Rescan in der Zeit zwischen 0 und 23 Uhr.

Anzahl zu scannender Kanäle

Dieser Eintrag bestimmt die minimale Anzahl an freien Kanälen, die ein DFS-Scan erreichen muss. Der Standardwert '2' bedeutet, dass das Gerät solange einen DFS-Scan durchführt, bis es 2 freie Kanäle erkennt. Im Falle eines nötigen Kanalwechsels, z. B. auf Grund eines aktivierten Radarmusters, steht der zweite Kanal sofort für einen Wechsel zur Verfügung.

Der Wert '0' deaktiviert die Beschränkung. Die physikalische WLAN-Schnittstelle führt einen DFS-Scan auf sämtlichen zur Verfügung stehenden Kanälen aus.

Rescan freier Kanäle

Diese Auswahl bestimmt, ob die physikalische WLAN-Schnittstelle nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle löscht oder für weitere DFS-Rescans zwischenspeichert.

- **Ja**: Die physikalische WLAN-Schnittstelle löscht nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, damit diese bei einem erneuten DFS-Rescan wieder zur Verfügung stehen.
- **Nein**: Das Gerät speichert nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, so dass das Gerät diese Kanäle bei einem erneuten DFS-Rescan sofort überspringt (Default).

12.17 STBC/LDPC

12.17.1 Low Density Parity Check (LDPC)

Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

12.17.2 Space Time Block Coding (STBC)

Die Funktion 'STBC' (Space Time Block Coding) variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen.

12.18 Spectral Scan

Neben der Anbindung von Rechnern an das Internet nutzen professionelle Anwender das Wireless Local Area Network (WLAN) immer häufiger auch für geschäftsrelevante Prozesse. Als Beispiele seien hier der Zugriff auf Patientenakten, die Online-Überwachung einer Produktion oder die (idealerweise verzögerungsfreie) Übertragung von Video- und Audiodaten genannt. Die Zuverlässigkeit und die Leistungsfähigkeit eines WLAN-Systems nehmen daher kontinuierlich an Bedeutung zu.

Aufgrund der zunehmenden Nutzung und Bedeutung von WLAN für die Datenübertragung ergeben sich immer häufiger Situationen, in denen Geräte oder Systeme anderer Nutzer die WLAN-Frequenzbereiche zeitgleich nutzen. Dies können z. B. Mikrowellenherde, kabellose Telefone, Bluetooth-Geräte oder Video-Transmitter sein, wobei deren Signale sowohl kontinuierlich wie intermittierend auftreten können. Durch die zeitgleiche Nutzung eines Frequenzbandes bzw. Frequenzbereiches ergeben sich Interferenzen, die die Zuverlässigkeit und Leistungsfähigkeit eines WLANs stören oder beeinträchtigen können. Solche Störungen können zum Verlust von Datenpaketen oder zum Abbruch von Verbindungen führen. Ist die Überlagerung zu stark, kann es sogar zum vollständigen Ausfall des WLANs kommen.

Es ist daher zunehmend von Bedeutung, den aktuell verwendeten Frequenzbereich durch eine gezielte Analyse zu überprüfen. Dies dient einerseits dem Zweck, Interferenzen oder andere Störfaktoren zu erkennen und bei Bedarf Gegenmaßnahmen einzuleiten. Andererseits lässt sich so auch sicherstellen, dass das WLAN ordnungsgemäß und störungsfrei funktioniert.

Eine gezielte Analyse bietet die Möglichkeit, folgende Faktoren zu klären bzw. näher zu bestimmen:

- Ordnungsgemäßer und störungsfreier Betrieb des WLANs
- Vorhandensein einer Interferenz bzw. eines Störsignals
- Anzeige oder Nennung der gestörten Bänder
- Stärke des Störsignals
- Regelmäßigkeit bzw. Häufigkeit des Störsignals
- Art und ggf. Herkunft des Störsignals

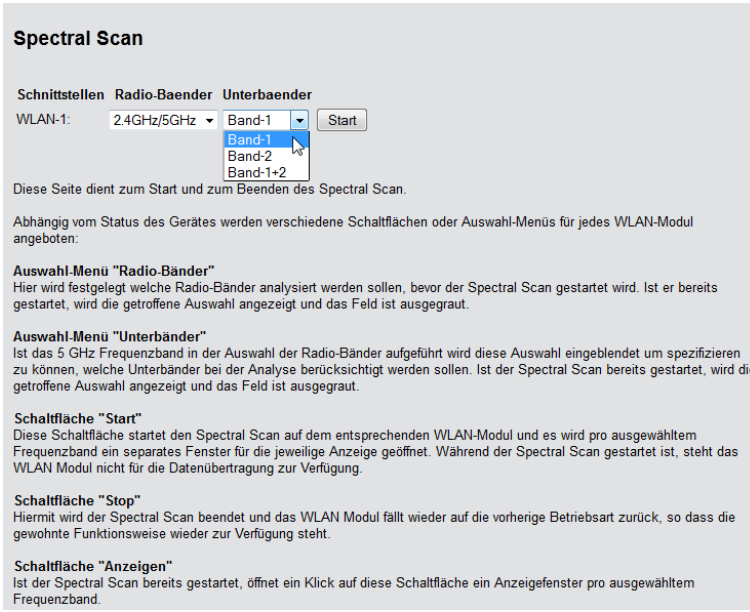
Die Untersuchung des für WLAN in Frage kommenden Frequenzbereiches findet auf der spektralen Ebene statt. Entsprechend hierzu werden die Ergebnisse grafisch wiedergeben, d. h. in Form von Echtzeit-Diagrammen oder Echtzeit-Übersichten, auf denen man Frequenzen und Störungen erkennen und ggf. ablesen kann. Hierbei ist zu bedenken, dass grafische Auswertungen eines spektralen Bereiches naturgemäß einen Interpretationsspielraum offen lassen und in manchen Fällen keine ganz eindeutigen Resultate ermöglichen. Ein Szenario wie das folgende wäre daher nicht ungewöhnlich: Sie stellen fest, dass Ihre aktuell verwendete Frequenz durch ein Signal gestört wird, das kontinuierlich auftritt und gleichbleibend stark ist. Sie können jedoch nicht eindeutig feststellen oder gar "ablesen", aus welchem Raum oder Gebäude das Signal kommt und welche Art von Gerät der Verursacher des Störsignals ist.

Hinweis: Spectral Scan ist Bestandteil von *LANCOM Active Radio Control (ARC)*

12.18.1 Funktionen des Software-Moduls

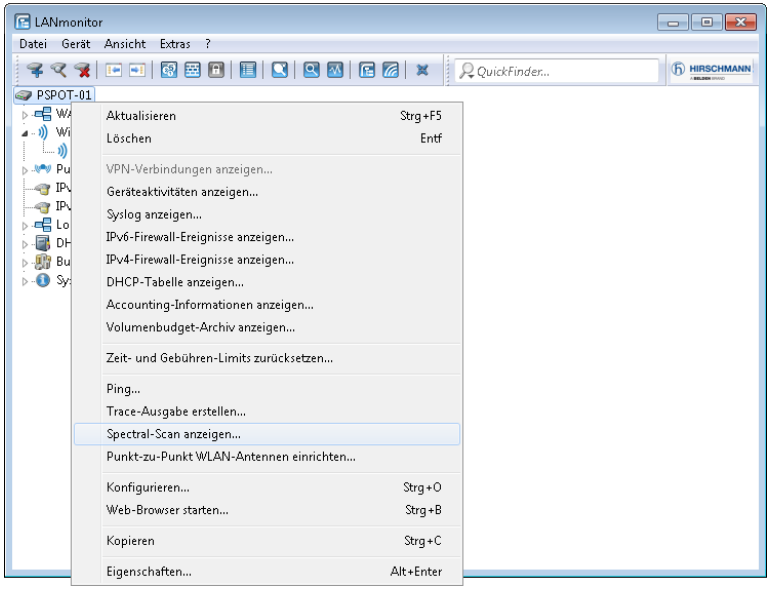
Das Software-Modul "Spectral Scan" bietet Ihnen die Möglichkeit, eine Spektralanalyse direkt am AP durchzuführen. Sie müssen sich also keine zusätzliche Soft- oder Hardware anschaffen, sondern können auf die integrierte Funktionalität zurückgreifen, um die in Frage kommenden Frequenzbereiche und -bänder zu untersuchen. Somit können Sie sich jederzeit einen grafischen Überblick über das Frequenzverhalten in Ihrem WLAN verschaffen, sei es nun zur Vorbeugung oder zur Aufdeckung von Störungen.

Ein Klick unter WEBconfig auf den Menüpunkt**Extras** > **Spectral Scan** öffnet den nachstehend abgebildeten Dialog:



Sie können den Spectral Scan auch aus dem LANmonitor heraus starten. Klicken Sie dazu das entsprechende Gerät in der Liste mit der rechten

Maustaste an und wählen Sie im Kontextdialog den Punkt **Spectral Scan anzeigen**.



Hinweis: Wenn das WLAN-Modul deaktiviert ist (**Setup** > **Schnittstellen** > **WLAN** > **Betriebs-Einstellungen**), erscheint ein entsprechender Hinweis, und der Spectral Scan lässt sich nicht starten. Konfigurieren Sie den AP für die Betriebsart "Basisstation" oder stellen Sie sicher, dass ein WLC den AP konfiguriert.

Hier stehen Ihnen folgende Einträge, Schaltflächen und Auswahl-Menüs zur Verfügung:

- **Schnittstellen**: Zeigt das ausgewählte, zu untersuchende WLAN-Modul an.
- **Radio-Baender**: Mit diesem Auswahl-Menü legen Sie fest, welches Frequenzband bzw. welche Frequenzbänder Sie untersuchen möchten. Wenn der Spectral Scan auf diesem Modul bereits gestartet ist, ist das betreffende Feld ausgegraut.
- **Unterbänder**: Dieses Auswahl-Menü ist nur aktiv, wenn Sie bei **Radio-Baender** entweder '5GHz' oder '2.4GHz/5Ghz' ausgewählt haben. Sie

können dann festlegen, welche Unterbänder des 5GHz-Bandes bei der Analyse berücksichtigt werden sollen.

- **Start**: Ein Klick auf diese Schaltfläche startet die Analyse (den "Spectral Scan") auf dem entsprechenden WLAN-Modul. Dabei öffnet sich ein separates Fenster pro ausgewähltem Frequenzband.
- **Stop**: Mit dieser Schaltfläche beenden Sie die Analyse. Das WLAN-Modul kehrt dann in die vorherige Betriebsart zurück und steht wieder mit der gewohnten Funktionalität zur Verfügung.

  Hinweis: Diese Schaltfläche erscheint erst nach dem Start des Moduls.

- **Anzeigen**: Sofern der Spectral Scan bereits gestartet ist, öffnen Sie mit einem Klick auf diese Schaltfläche ein Anzeigefenster pro ausgewähltem Frequenzband. Durch mehrfaches Betätigen der Schaltfläche können Sie mehrere Fenster öffnen.

Hinweis: Während des Analysevorgangs überträgt das untersuchte WLAN-Modul keine Daten und sendet keine SSID.

Hinweis: Weitere Informationen über die angezeigten Diagramme entnehmen Sie dem Abschnitt *Analyse-Fenster Spectral Scan*.

12.18.2 Analyse-Fenster Spectral Scan

Hinweis: Die Anzeige des Spectral Scans erfolgt in einer Browser-Anwendung. Damit sie ordnungsgemäß funktioniert, muss Ihr Browser Websockets in der aktuellen Version das HTML5-Element `<canvas>` unterstützen. Der in LANmonitor integrierte Browser erfüllt alle Anforderungen.

Im separaten Analyse-Fenster des Spectral Scan haben Sie unterschiedliche Möglichkeiten, die jeweiligen Frequenzen bzw. Frequenzbereiche nebst möglichen Störungen darzustellen. Hierfür stehen Ihnen am oberen Rand des Fensters die folgenden Schaltflächen zur Verfügung:

- **Current**: Zeigt oder verbirgt die Kurve der aktuell gemessenen Werte.

- **Maximum**: Zeigt oder verbirgt die Maximalwerte des laufenden Spektrum-Scans, bezogen auf den aktuell eingestellten History-Bereich.
- **Average**: Zeigt oder verbirgt die Durchschnittswerte des laufenden Spektrum-Scan, bezogen auf den aktuell eingestellten History-Bereich.
- **History**: Zeigt oder verbirgt die zuletzt gemessenen Werte.
- **Number of history values**: Bestimmt die Anzahl der angezeigten, zuletzt gemessenen Ergebnisse. Sie können sich mindestens die letzten 5 und maximal die letzten 50 Messpunkte je Frequenz anzeigen lassen.
- **Last Channel**: Zeigt oder verbirgt den zuletzt benutzten Kanal.
- **Frequency**: Wechselt die Anzeige auf der x-Achse zwischen WLAN-Kanal und Frequenz.

Das Fenster enthält zwei grafische Darstellungen, die Ihnen die Messergebnisse unterschiedlich präsentieren. Das obere Diagramm zeigt auf der y-Achse die Signalstärke in dBm, auf der x-Achse entweder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz. Das untere Diagramm enthält den zeitlichen Verlauf der Analyse in Form eines Wasserfall-Diagramms, wobei die y-Achse die Zeit darstellt, während die x-Achse wieder den jeweiligen WLAN-Kanal oder die entsprechende Frequenz zeigt. Diese Formen der Darstellung können sowohl andauernde als auch zeitlich variierende Störungen in den Frequenzen anschaulich machen, so dass Sie entsprechende Maßnahmen zur Verbesserung der Verbindung durchführen können (z. B. Wechsel des Kanals oder Identifizierung und Beseitigung der Störquelle). So weisen z. B. bestimmte Störquellen wie Mikrowellen-Geräte, DECT-Telefone (die im 2,4 GHz Frequenzbereich arbeiten) oder Audio-Video-Transmitter ganz typische Sendemuster auf, die in beiden Diagrammen deutlich hervortreten.

Am unteren Rand des Fensters sehen Sie einen mit **Time Slider** bezeichneten Schieberegler. Mit diesem können Sie für das Wasserfall-Diagramm den zu analysierenden Zeitraum der betreffenden Frequenz erweitern oder begrenzen. Alternativ können Sie über das Eingabefeld rechts neben dem Schieberegler auswählen, wie viele Messergebnisse Sie sich im Wasserfall-Diagramm anzeigen lassen möchten. Die Web-Applikation kann über den Time-Slider bis zu 300 Messwerte im Wasserfall-Diagramm zur Anzeige bringen, wobei sie insgesamt die Messwerte von maximal 24 Stunden zwischenspeichern kann.

Nachstehend sehen Sie einige exemplarische Analyse-Ergebnisse, die jeweils andere Einstellungen auf unterschiedliche Weise grafisch aufbereiten:

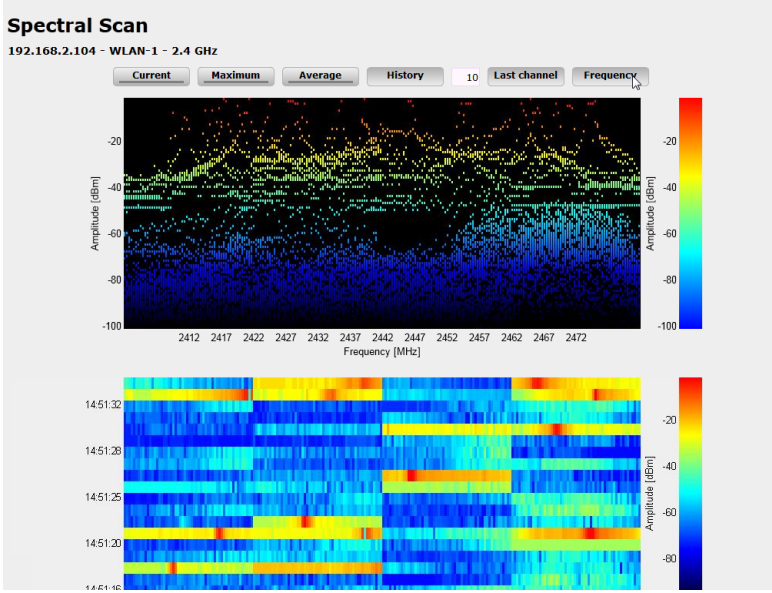


Abbildung 2: Spectral Scan, Frequenz-Anzeige der letzten 10 History-Werte

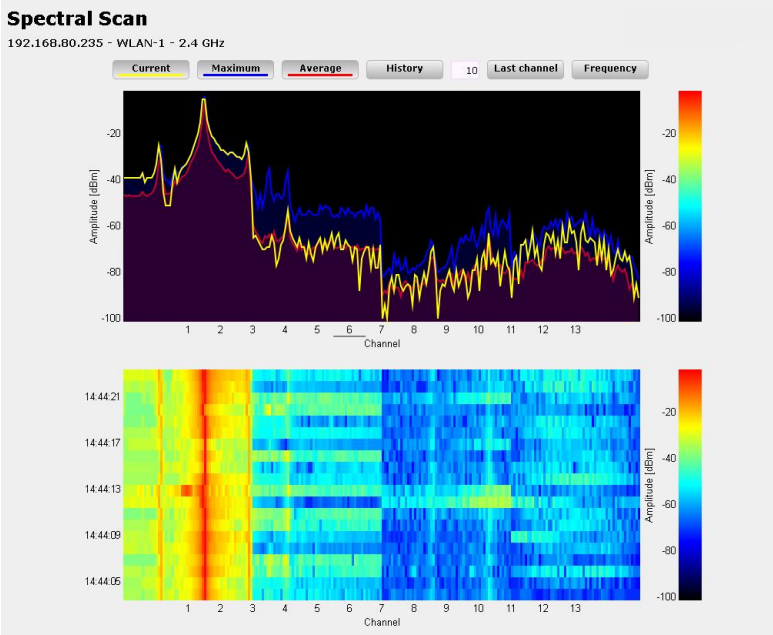


Abbildung 3: Spectral Scan, Kanal-Anzeige **Current**, **Maximum**, **Average**, Störung durch Funk-Kamera

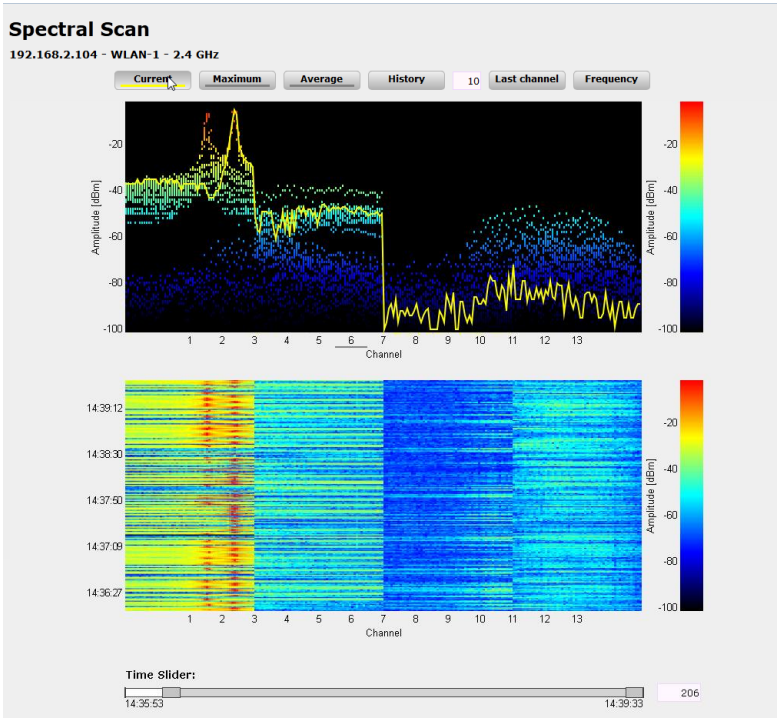


Abbildung 4: Spectral Scan, Kanal-Anzeige **Current**, letzte 10 History-Werte und "Time Slider", Störung durch Baby-Phone

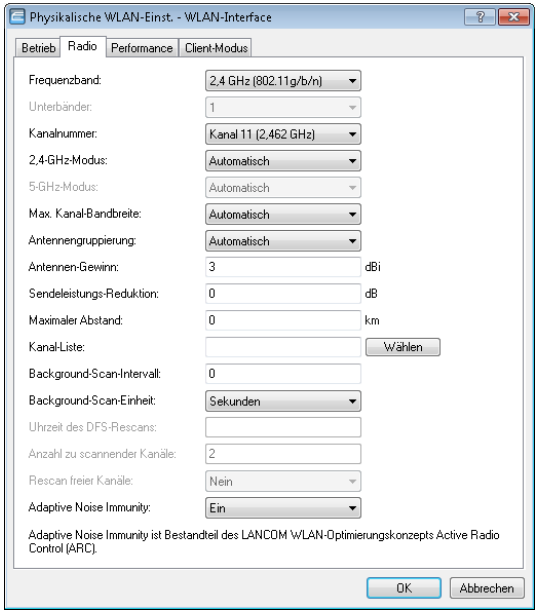
12.19 Adaptive Noise Immunity zur Abschwächung von Interferenzen im WLAN

Innerhalb eines WLANs kann es aus unterschiedlichen Gründen zu Störungen durch Interferenzen kommen. Einerseits stören Geräte wie Mikrowellenherde oder Funktelefone die Datenübertragung, andererseits können die Netzgeräte selber durch Aussendung von Störfrequenzen die Kommunikation behindern. Die Art dieser Störungen ist jeweils charakteristisch. Bei der adaptiven Rausch-Immunität (Adaptive Noise Immunity, ANI) ermittelt der AP anhand verschiedener Fehlerzustände die für die aktuelle Situation beste Kompensation der Störungen. Durch die automatische Erhöhung der Rausch-Immunität wird die

Funkzelle gezielt verkleinert, sodass sich die Auswirkungen der Interferenzen auf die Datenübertragung verringern.

Die aktuellen Werte sowie die Aufzeichnung der vergangenen Aktionen finden Sie im WEBconfig unter **Status** > **WLAN** > **Rausch-Immunität**.

Die adaptive Rausch-Immunität aktivieren Sie in LANconfig unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Physikalische WLAN-Einstellungen** > **Radio**.



Aktivieren Sie die Adaptive Noise Immunity, indem Sie im Auswahlfeld **Adaptive-Noise-Immunity** den Wert "Ein" auswählen.

Hinweis: Adaptive Noise Immunity ist Bestandteil von *LANCOM Active Radio Control (ARC)*

12.20 Opportunistic Key Caching (OKC)

Authentifizierung von WLAN-Clients über EAP und 802.1x ist mittlerweile Standard in Unternehmens-Netzwerken, und auch beim öffentlichen Internet-Zugang findet es im Rahmen der Hotspot 2.0-Spezifikation immer mehr Verbreitung. Der Nachteil der Authentifizierung über 802.1x ist, dass die Zeit von Anmeldung bis zur Verbindung durch den Austausch von bis zu zwölf Datenpaketen zwischen WLAN-Client und AP sich merklich verlängert. Für die meisten Anwendungen, bei denen es nur um den Austausch von Daten geht, mag das nicht ins Gewicht fallen. Zeitkritische Anwendungen wie z. B. Voice-over-IP sind jedoch davon abhängig, dass die Neuanmeldung in einer benachbarten WLAN-Funkzelle die Kommunikation nicht beeinträchtigt.

Um dem entgegenzuwirken, haben sich bestimmte Authentifizierungsstrategien wie PMK-Caching und Pre-Authentifizierung etabliert, wobei auch durch Pre-Authentifizierung nicht alle Probleme behoben sind. Einerseits ist nicht sichergestellt, wie der WLAN-Client erkennt, ob der AP Pre-Authentifizierung beherrscht. Andererseits führt Pre-Authentifizierung zu einer erheblichen Belastung des RADIUS-Servers, der die Authentifizierungen von allen Clients und allen APs im WLAN-Netzwerk verarbeiten muss.

Das opportunistische Schlüssel-Caching verlagert die Schlüsselverwaltung auf einen WLC oder zentralen Switch, der alle APs im Netzwerk verwaltet. Meldet sich ein Client bei einem AP an, übernimmt der nachgeschaltete WLC als Authenticator die Schlüsselverwaltung und sendet dem AP den PMK, den schließlich der Client erhält. Wechselt der Client die Funkzelle, errechnet er aus diesem PMK und der MAC-Adresse des neuen APs eine PMKID und sendet die an den neuen AP in der Erwartung, dass der OKC aktiviert hat (deshalb "opportunistisch"). Kann der AP mit der PMKID nichts anfangen, handelt er mit dem Client eine normale 802.1x-Authentifizierung aus.

Ein OpenBAT-AP kann auch OKC durchführen, falls der WLC vorübergehend nicht erreichbar ist. In diesem Fall speichert er den PMK und sendet ihn an den WLC, sobald er wieder verfügbar ist. Der schickt den PMK anschließend an alle APs im Netzwerk, so dass der Client sich beim Wechsel der Funkzelle dort über OKC anmelden kann.

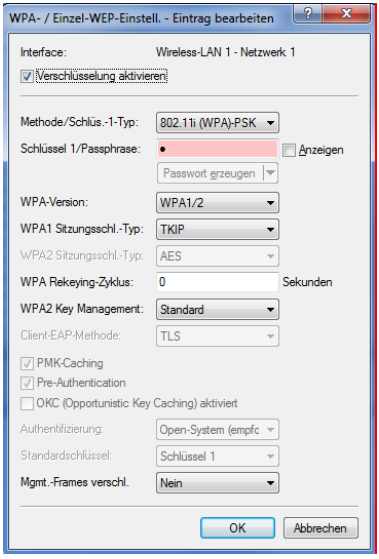
Für die Nutzung der OKC-Funktion ist eine Aktivierung von OKC sowohl auf den APs als auch auf der Client-Seite nötig. Informationen über die Aktivierung auf einem AP in der WLAN-Betriebsart **Client** oder **Basisstation** finden Sie

unter *Tutorial: OKC auf Access Point-/Client-Seite aktivieren* auf Seite 1218. Sofern Sie Ihre APs über einen WLC verwalten (WLAN-Betriebsart **Managed**), finden Sie hierzu weitere Informationen unter *Logische WLAN-Netzwerke* auf Seite 1290.

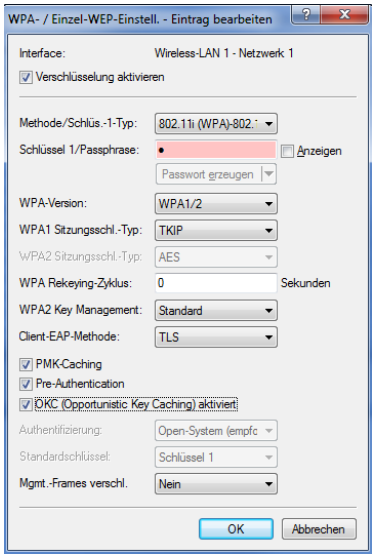
12.20.1 Tutorial: OKC auf Access Point-/Client-Seite aktivieren

Sie verfügen über einen OpenBAT im Access Point-/Client-Modus. Im Folgenden finden Sie die Konfiguration für einen OpenBAT mit einem WLAN-Modul mit einem aktivierten logischen WLAN-Netzwerk beschrieben. Für einen OpenBAT mit 2 WLAN-Modulen führen Sie die folgenden Schritte für beide WLAN-Module analog durch.

1. Wechseln Sie in die Ansicht **Wireless-LAN** > **802.11i/WEP** > **WPA- / Einzel-WEP-Einstell.**



2. Wählen Sie **Wireless-LAN 1 Netzwerk 1** und klicken Sie **Bearbeiten...**.
3. Wählen Sie als **Methode/Schlüs.-1-Typ 802.11i (WPA)-802.1x**.
4. Aktivieren Sie die Option **OKC (Opportunistic Key Caching) aktiviert**.



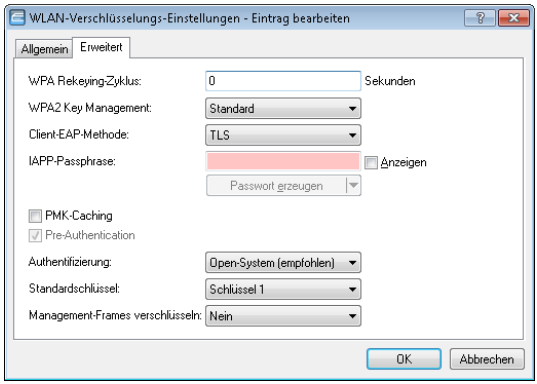
Sie haben OKC aktiviert.

Hinweis: Wenn OKC aktiviert ist, wird **Pre-Authentication** auch bei aktiviertem Kontrollkästchen automatisch deaktiviert.

12.20.2 Verschlüsseltes OKC über IAPP

Durch eine definierte IAPP-Passphrase (PMK-IAPP-Secret) auf einem AP ist es möglich, den PMK (Pairwise Master Key) verschlüsselt zu den anderen APs zu übertragen und dort zu speichern.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **802.11i/WEP** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.



12.21 Fast Roaming

Zusammen mit der Authentifizierung nach dem Standard IEEE 802.1X und dem Schlüsselmanagement nach dem Standard IEEE 802.11i bieten moderne WLAN-Installationen ein hohes Maß an Sicherheit und Vertraulichkeit der übertragenen Daten. Allerdings erfordern diese Standards die Übertragung zusätzlicher Datenpakete während der Verbindungsverhandlung sowie zusätzliche Rechenleistung auf Client- und Serverseite.

Aktuelle WLAN-Geräte besitzen Hardware-Beschleuniger, mit denen die Ver- und Entschlüsselung der Nutzerdaten während einer Verbindung in Echtzeit ohne spürbare Verzögerung oder auffällige Netzlast erfolgt. Auch die clientseitige Erstellung von Schlüsseln stellt mittlerweile durch die ausreichende Rechenleistung keine bemerkenswerte Beeinträchtigung dar.

Die Verzögerungen bei Verbindungen über EAP/802.1X oder WPA beruhen deshalb hauptsächlich auf der Zeit, die Client und Server zum Aushandeln der Sicherheitsprotokolle bei der Anmeldung benötigen.

Der ursprüngliche IEEE 802.11 benötigte zum Aufbau einer Datenverbindung zwischen WLAN-Client und AP lediglich bis zu sechs Datenpakete. Die Standard-Erweiterung IEEE 802.11i besserte Schwachstellen bei der WEP-Verschlüsselungs aus, verlängerte dabei jedoch den Anmeldeprozess je nach Authentifizierungsmethode um ein Vielfaches.

Diese verlängerte Anmeldezeit des WLAN-Clients am AP ist für nicht zeitkritische Anwendung ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem AP zum nächsten (wie es z. B. bei Voice-over-IP-Anwendungen oder in industriellen Echtzeit-Umgebungen notwendig ist), ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel.

Methoden wie Pairwise Master Key Caching (PMK Caching), Pre-Authentication, Opportunistic Key Caching (OKC) sowie der Einsatz von zentralen WLCs zur Schlüsselverwaltung verbessern die Zeit für die Schlüsselaushandlung zwischen WLAN-Client und AP bei der Anmeldung. Allerdings reicht das immer noch nicht aus, die vergleichsweise lange Zeit für die Schlüsselverhandlung zwischen WLAN-Client und AP auf ein brauchbares Maß zu begrenzen.

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim AP zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim AP. Beim Roaming von einem AP zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen AP reservieren. Die dafür notwendigen zusätzlichen Management-Frames erhöhen die Anmeldezeit jedoch wieder deutlich.

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem AP zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am AP wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Wie beim Opportunistic Key Caching (OKC) existiert eine zentrale Schlüssel-Verwaltung, sinnvollerweise in Form eines WLCs, der die angeschlossenen APs mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der AP 802.11r beherrscht.

Die vom WLC verwalteten APs senden als Kennung das sogenannte "Mobility Domain Information Element (MDIE)" aus, das den WLAN-Clients im Empfangsbereich u. a. mitteilt, welcher "Mobility Group" der AP angehört. Anhand dieser Gruppenkennung erkennt der WLAN-Client, ob er derselben Domain angehört und sich somit ohne Verzögerung anmelden kann. Diese Mobility Domain hat der WLAN-Client während der ersten Anmeldung an einem AP mitgeteilt bekommen.

Die Domain-Kennung sowie spezielle, bei der Erstanmeldung generierte und an alle verwalteten APs übertragenen Schlüssel verringern die Verhandlungsschritte bei der Neuanmeldung bei einem AP auf die angestrebten vier bis sechs Schritte.

Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen AP einen neuen PMK aushandeln. Dieser ist auch auf dem AP gültig, mit dem sich der WLAN-Client im Anschluss verbinden möchte.

Zusätzlich ermöglicht IEEE 802.11r in Form eines "resource requests" die Reservierung von zusätzlicher Bandbreite auf dem neuen AP, ohne dass weitere Datenpakete wie bei IEEE 802.11e die Anmeldung unnötig verlängern.

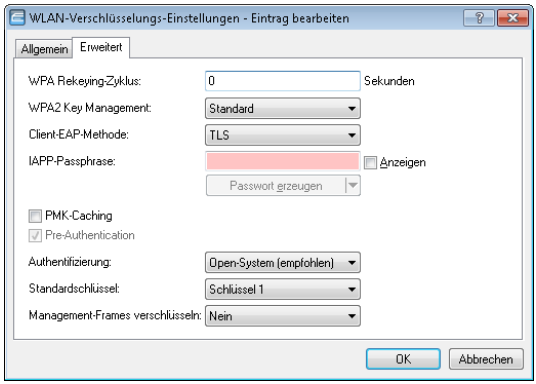
Hinweis: Ältere WLAN-Clients haben möglicherweise Probleme damit, eine Verbindung zu einer SSID mit aktiviertem 802.11r aufzubauen. Daher ist hier der Einsatz zweier SSIDs ratsam: eine SSID für ältere Clients ohne 802.11r-Unterstützung und eine weitere SSID mit aktiviertem 802.11r für Clients mit 802.11r-Unterstützung.

Das Fast-Roaming lässt sich in LANconfig einstellen unter **Wireless-LAN** > **802.11i/WEP** > **WPA-/Einzel-WEP-Einstellungen**.

12.21.1 Fast Roaming über IAPP

Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können APs mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **WLAN** > **Verschlüsselung** nach einem Klick auf **WLAN-Verschlüsselungs-Einstellungen**. Öffnen Sie den Konfigurationsdialog der entsprechenden Schnittstelle und wechseln Sie auf den Reiter **Erweitert**.



Hinweis: Beachten Sie bitte, dass es für die Verwendung von IEEE 802.11r erforderlich ist, in den Verschlüsselungs-Einstellungen unter **WPA2 Key Management** die Option “Fast Roaming” auszuwählen.

12.22 Wireless-IDS

Die Einführung von WLAN in industrielle Netze eröffnet eine neue Klasse von Bedrohungen der Netzsicherheit. Radiosignale durchdringen Wände und reichen eventuell weiter, als gewollt ist. Dies eröffnet unautorisierten Anwendern neue Möglichkeiten, das Netz zu stören.

Hirschmann ist sich dieser Bedrohungen bewusst und unterstützt Anwender mit seinem Angriffserkennungssystem (Wireless-IDS) darin, solche Angriffe zu erkennen und abzuwenden. Die typischen Angriffe auf ein WLAN-Netz erzeugen charakteristische Muster.

12.22.1 Wireless-IDS-Zähler

APs bieten durch das Angrifsserkennungssystem Wireless-IDS die Möglichkeit, potentielle Angriffe zu erkennen und Warnungen an eine Netzmanagement-Software zu senden, sobald ein Zähler für ein vorgegebenes Ereignis den Grenzwert/Intervall überschreitet. Wird ein Zähler auf "0" gestellt, deaktiviert dies die Erkennung des jeweiligen Angriffes.

Die voreingestellten Grenzwerte sind Richtwerte, die für Ihren Anwendungsfall ungeeignet sein können. Die Grenzwerte für Ihren Anwendungsfall hängen von den Umgebungsbedingungen Ihres APs ab. Führen Sie daher zuerst eine Referenzmessung mittels eines Testlaufs des Wireless-IDS am Einsatzort Ihres WLANs durch.

Zusätzliche Referenzwerte erhalten Sie durch Mitschnitte mittels eines kostenfreien Programms wie beispielsweise Wireshark. Für das Abhören des Funkverkehrs und das Speichern sowie das Verarbeiten der daraus gewonnenen Daten benötigen Sie in vielen Ländern die Erlaubnis der Regulierungsbehörde. Das unerlaubte Mitschneiden und das unerlaubte Speichern der Daten sowie deren Weitergabe steht in vielen Ländern unter Strafe.

Frame-Zähler	**Werkseinstellung Grenzwert**	**Werkseinstellung Zeitintervall (1 Intervall entspricht 1 Sekunde)**
EAPOL Start	250	10
Broadcast-Probe	500	10
Broadcast-Disassociation	2	1
Broadcast-Deauthentication	2	1
Deauthentication	250	10
Association-Request	250	10
Reassociation-Request	250	10
Authentication-Request	250	10
Disassociation-Request	250	10
Out-Of-Window	200	5
BA-Session	100	5
Null-Data (Null-Data-DoS-Angriff)	500	5
Data (Null-Data-PS-Angriff)	200	5
Listen-Interval-Difference	5	entfällt

Frame-Zähler	Werkseinstellung Grenzwert	Werkseinstellung Zeitintervall (1 Intervall entspricht 1 Sekunde)
PS-Poll	100	5
Multi-Stream-Data	100	5
No-Ack-MS-Data	100	5

12.22.2 Wireless-IDS Angriffstypen

Angriffe auf ein WLAN lassen sich wie folgt klassifizieren:

- nach dem Ziel des Angriffs (AP oder Client)
- wie viele Ziele der Angriff beinhaltet (eines oder mehrere)
- nach Angriffsart

Manche Angriffe lassen sich kaum verhindern, da sie Mechanismen ausnutzen, die in ihrer Ausgestaltung den Aufbau eines WLANs erst ermöglichen. Zu den Angriffen, die sich kaum verhindern lassen, gehört z. B. das Stören des Funkverkehrs mit einer Störquelle.

Angriffsarten:

- Denial-of-Service-Angriffe (DoS) haben das Ziel einen Dienst stillzulegen.
- Man-in-the-Middle-Angriffe (MitM) haben das Ziel, sich zwischen 2 Netzteilnehmer zu setzen. Dadurch kann der Angreifer unter bestimmten Voraussetzungen den Funkverkehr beider betroffener Teilnehmer abhören und ausgetauschte Daten manipulieren.
- SSID-Angriffe (SSID) haben das Ziel, eine unterdrückte SSID herauszufinden. Eine unterdrückte SSID dient der Sicherheit durch Verschleiern.

Name des Angriffes	*Ziel des Angriffes(AP, Client, Sonstige)*	*Anzahl Ziele (einer oder mehrere)*	*Angriffsarten*
EAPOL Start	Sonstige (Infrastruktur)	einer	DoS
Broadcast-Probe	AP	einer	DoS
Broadcast-Disassociation	Client	mehrere	DoS, MitM, SSID
Broadcast-Deauthentication	Client	mehrere	DoS, MitM, SSID
Deauthentication	Client	einer	DoS, SSID

Name des Angriffes	*Ziel des Angriffes(AP, Client, Sonstige)*	*Anzahl Ziele (einer oder mehrere)*	*Angriffsarten*
Association-Request	Client	einer	DoS
Reassociation-Request	Client	einer	DoS
Authentication-Request	Client	einer	DoS
Disassociation-Request	Client	einer	DoS
Block-Ack-DoS-Angriff	AP, Client	einer	DoS
Null-Data-DoS-Angriff	AP	einer	DoS
Null-Data-PS-Angriff	Client	einer	DoS
PS-Poll-Angriff	Client	einer	DoS
Spatial-Multiplexing-PS-Angriff	Client	einer	DoS

Tabelle 25: Angriffstypen auf WLAN

EAPOL Start (Extensible Authentication Protocol over LAN)

Wenn ein AP ein EAPOL-Start-Frame empfängt, startet er den Identifikationsprozess und weist intern Ressourcen für den neuen Client zu. Gehen nun ausreichend EAPOL-Start-Frames auf einem AP ein, erschöpft dies die internen Ressourcen des APs oder eines RADIUS-Servers.

Broadcast-Probe

Ein Angreifer sendet kontinuierlich Probe Requests ans Netz. Probe Requests sind von Clients verwendete Frames, die – etwas vereinfacht – fragen: "Ist hier ein WLAN?". Der AP antwortet mit Probe-Response-Frames, die antworten: "Ja, hier ist ein WLAN mit [SSID]". Dieser Mechanismus dient dazu, WLAN-Dienste in WLAN-Netzen ausfindig zu machen. Wenn der Angreifer genügend Probe Requests sendet, ist der AP mit diesen Frames ausgelastet, und der Funkkanal wird mit Probe Responses geflutet.

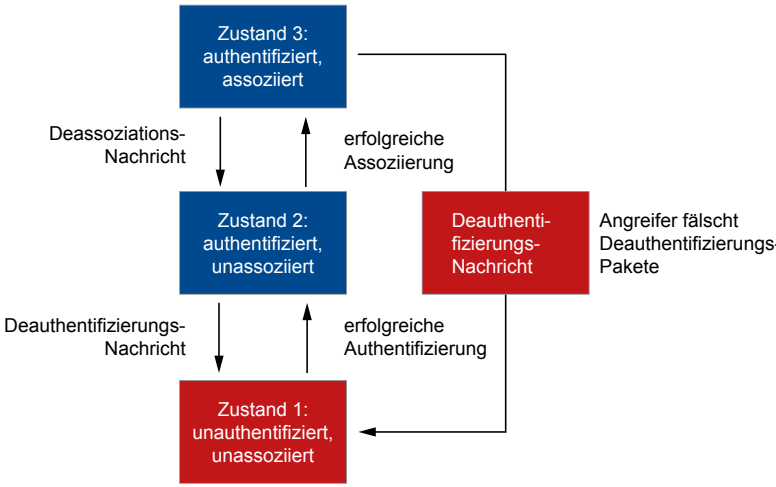


Abbildung 5: Verhalten eines Clients bei Deauthentifizierung

Association-Request

Ein Angreifer sendet kontinuierlich Assoziierungs-Frames zum AP. Dies überlastet die Assoziierungs-Tabelle des APs.

Reassociation-Request

Ein Angreifer sendet kontinuierlich Reassoziierungs-Frames zum AP mit dem Ziel, die Assoziierungs-Tabelle des APs zu überlasten. Reassozierungs-Frames in großer Zahl können auch ein Indiz für angegriffene Clients sein, die sich erneut mit dem AP zu verbinden versuchen.

Authentication-Request

Ein Angreifer sendet kontinuierlich Authentifizierungs-Frames zum AP. Dies überlastet die Authentifizierungs-Tabelle des APs.

Disassociation-Request

Ein Angreifer fälscht Deassoziierungs-Frames, um einen Client vom AP abzumelden. Alle betroffenen Clients versuchen sich anschließend wieder mit dem AP zu assoziieren. Bis sich die Clients wieder assoziieren, ist keine Datenübertragung möglich.

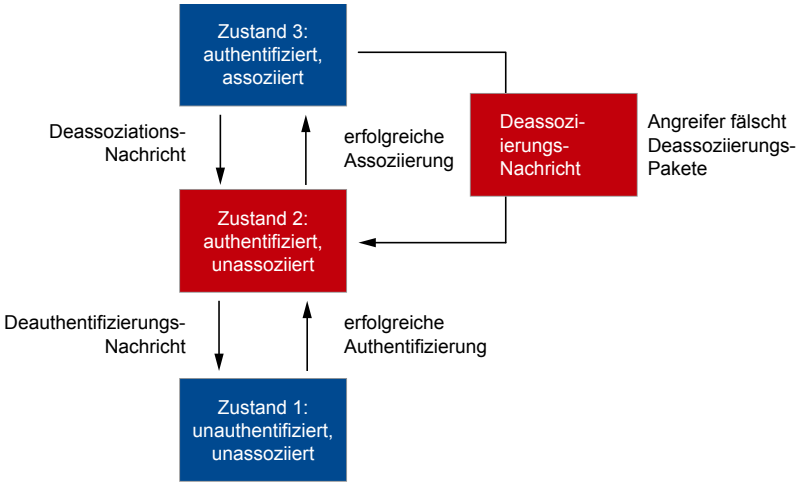


Abbildung 6: Verhalten eines Clients bei Deassoziierung

Block-Ack-DoS-Angriff

Ein Angreifer spooft die MAC-Adresse des Clients und kann folgende Angriffsvarianten durchführen:

- Der Angreifer schickt in der Setup-Phase einer Block-Ack-Session manipulierte ADDBA-Frames mit gefälschten Start-Sequenznummern an den AP. Dadurch kann der Angreifer erreichen, dass der AP legitime Frames verwirft.
- Der Angreifer verschickt manipulierte A-MPDU-Frames, die zu einer Überlastung des Re-Ordering-Buffers beim AP führen.
- Der Angreifer beendet die Block-Ack-Session mit einem gefälschten DELBA-Frame vom Client an den AP, was den Verlust gepufferter Frames beim AP zur Folge hat. Ein Angriff mit manipulierten DELBA-Frames kann außerdem den Datendurchsatz verringern, weil der Client die Block-Ack-Session erneut aufbauen muss.

Null-Data-DoS-Angriff

Wenn ein Client längere Zeit inaktiv war, kann der AP nicht entscheiden, ob der Client ausgeschaltet ist oder sich außerhalb der Funkzelle befindet. Eine Deauthentifizierung des Clients durch den AP könnte die Folge sein. Um eine ungewollte Deauthentifizierung zu verhindern, sendet der Client nach längerer

Inaktivität Null-Data-Frames an den AP, um die Session aufrechtzuerhalten. Der AP bestätigt anschließend den Erhalt des Null-Data-Frames.

Ein Angreifer kann sich das eben beschriebene Szenario folgendermaßen zunutze machen: Der Angreifer verschickt große Mengen von Null-Data-Frames an den AP. Da der AP den Erhalt jedes einzelnen Null-Data-Frames bestätigen muss, verringert sich die Bandbreite des Funkkanals derart, dass die Anfragen legitimer Clients verworfen werden.

Null-Data-PS-Angriff

Ein Client kann Null-Data-Frames nutzen, um dem AP mitzuteilen, dass er in den Ruhemodus wechselt. In diesem Fall puffert der AP die Pakete, die während des Ruhemodus des Clients für den Client eingehen und informiert den Client über das TIM-Feld im Beacon-Frame, dass der AP Pakete puffert. Der Client fordert nach Eingang des Beacon-Frames mit dem entsprechenden TIM-Bit die Pakete aus dem Puffer des APs mit einem PS-Poll-Frame an.

Ein Angreifer kann sich das eben beschriebene Szenario folgendermaßen zunutze machen: Der Angreifer spooft die MAC-Adresse des Clients und schickt dem AP die gefälschte Nachricht eines Wechsels in den Ruhemodus. Der AP puffert nun die für den Client eingehenden Pakete und löscht sie nach einem festgelegten Timeout, so lange der Client kein PS-Poll-Frame sendet. Da sich der Client in Wirklichkeit gar nicht im Ruhemodus befindet, wird er auch kein PS-Poll-Frame zur Anforderung gepufferter Pakete an den AP schicken. An den Client adressierte Pakete gehen somit verloren.

PS-Poll-Angriff

Der Angreifer spooft die MAC-Adresse des Clients im Ruhemodus und verschickt gefälschte PS-Poll-Frames an den AP, um die vom AP gepufferten Pakete anzufordern. Der Angreifer schöpft nun die vom AP verschickten Pakete ab, die für den Client bestimmt sind.

Spatial-Multiplexing-PS-Angriff

Der Einsatz mehrerer Antennen auf dem gleichen Übertragungskanal steigert den Datendurchsatz und verbessert die Funkabdeckung. Da der Einsatz mehrerer Antennen energieintensiv ist, wechselt ein Client in Zeiten geringer Datendurchsätze in den statischen Spatial-Multiplexing-Power-Save-Modus (SM-Power-Save-Modus), so dass ausschließlich eine Antenne aktiv ist. Mit SM-Power-Save-Action-Frames informiert der Client den AP über einen Wechsel in den SM-Power-Save-Modus oder über das Ende des SM-Power-Save-Modus.

Ein Angreifer kann sich das eben beschriebene Szenario folgendermaßen zunutze machen:

- Der Angreifer spooft die MAC-Adresse eines Clients mit mehreren aktiven Antennen und informiert den AP mit einem gefälschten SM-Power-Save-Action-Frame über einen Wechsel in den statischen SM-Power-Save-Modus. Der AP kommuniziert daraufhin mit dem Client ausschließlich über einen Spatial-Stream, was den Datendurchsatz erheblich verringert.
- Der Angreifer spooft die MAC-Adresse eines Clients im statischen SM-Power-Save-Modus mit ausschließlich einer aktiven Antenne und informiert den AP mit einem gefälschten SM-Power-Save-Action-Frame über die Beendigung des statischen SM-Power-Save-Modus. Der AP kommuniziert daraufhin mit dem Client über mehrere Spatial-Streams, die der Client nicht empfangen kann, da er ausschließlich eine aktive Antenne nutzt.

12.22.3 Wireless-IDS-Angreifer-Erkennung

Die Wireless-IDS-Angreifer-Erkennung bietet Ihnen die Möglichkeit, folgende Informationen über potentielle Angreifer zu erhalten:

- MAC-Adresse
- Angriffstyp
- Aktuelle Aktivität
- RSSI-Wert (empfangene Signalstärke)
- Angriffsrate
- Erkennung des Angreifers als Known Client
- DHCP-Requests des Angreifers, die in einem Ringspeicher gespeichert und via WEBconfig als .pcap-Datei an folgender Stelle heruntergeladen werden können:

  Dateimanagement > **Zertifikat oder Datei herunterladen** > **Dateityp** > **WIDS – Intruder Identification Packet Capture (*.pcap)**

Die gesammelten Informationen über den potentiellen Angreifer finden Sie im WEBconfig unter **HiLCOS-Menübaum** > **Status** > **WLAN** > **Wireless-IDS** > **Angreifer-Tabelle**.

Ausgewählte Stationen können Sie durch den Eintrag in eine White-List von der Angreifer-Erkennung ausnehmen. Dies ist beispielsweise dann sinnvoll, wenn der Administrator schon vorher weiß, dass eine vertrauenswürdige Station fälschlicherweise als Angreifer erkannt würde.

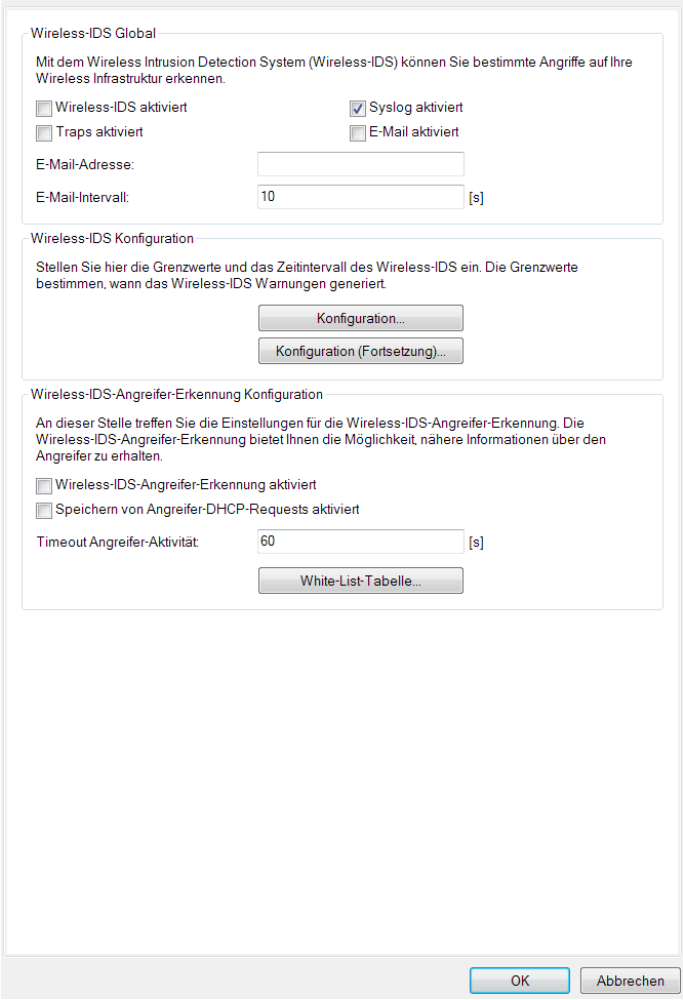
12.22.4 Tutorial: Konfiguration des Wireless-IDS

Die voreingestellten Grenzwerte sind Richtwerte, die für Ihren Anwendungsfall ungeeignet sein können. Die Grenzwerte für Ihren Anwendungsfall hängen von den Umgebungsbedingungen Ihres APs ab. Führen Sie daher zuerst eine Referenzmessung mittels eines Testlaufs des Wireless-IDS am Einsatzort Ihres WLANs durch.

Zusätzliche Referenzwerte erhalten Sie durch Mitschnitte mittels eines kostenfreien Programms wie beispielsweise Wireshark. Für das Abhören des Funkverkehrs und das Speichern sowie das Verarbeiten der daraus gewonnenen Daten benötigen Sie in vielen Ländern die Erlaubnis der Regulierungsbehörde. Das unerlaubte Mitschneiden und das unerlaubte Speichern der Daten sowie deren Weitergabe steht in vielen Ländern unter Strafe.

Um das Wireless-IDS zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht **Wireless-LAN** > **Wireless-IDS.**



2. Aktivieren Sie die Option **Wireless-IDS aktiviert**.
3. Wählen Sie die gewünschte Art der Protokollierung. Wireless-IDS protokolliert per Default im **Syslog**. Um Wireless-IDS über Traps zu protokollieren, aktivieren Sie die Option **Traps aktiviert**.
4. Um E-Mail-Benachrichtigungen zu erhalten, aktivieren Sie die Option **E-Mail aktiviert** und geben Sie die gewünschte E-Mail-Adresse ein.

Hinweis: Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

5. Setzen Sie die Grenzwerte für die Frames und die Intervalle entsprechend Ihrer Referenzmessung.
6. Um Informationen über den Angreifer zu erhalten, aktivieren Sie die Option **Wireless-IDS-Angreifer-Erkennung aktiviert**.
7. Um Informationen über die Angreifer-DHCP-Requests zu erhalten, aktivieren Sie die Option **Speichern von Angreifer-DHCP-Requests aktiviert**.
8. Setzen Sie den **Timeout Angreifer-Aktivität**.
9. Um bestimmte Stationen von der Angreifer-Erkennung auszunehmen, fügen Sie diese Stationen der **White-List-Tabelle** hinzu.
10. Klicken Sie die Schaltfläche **OK**.

Sie haben das Wireless-IDS aktiviert und konfiguriert.

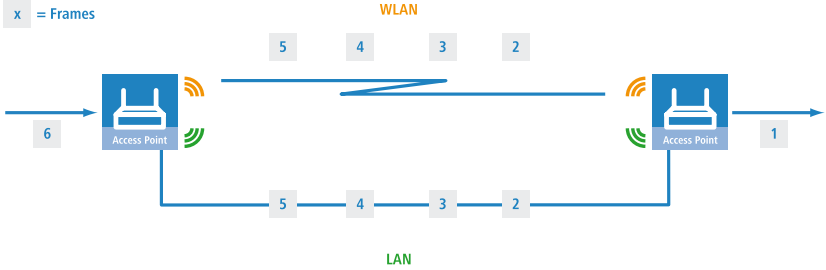
12.23 Redundante Verbindungen mittels PRP

Anwendungen, die empfindlich auf Kommunikationsausfälle reagieren, benötigen eine möglichst unterbrechungsfreie Kommunikation. Zu solchen Anwendungen zählen zum Beispiel die Automation, der Transport und mobile Anwendungen.

Mit HiLCOS haben Sie die Möglichkeit, in Ihrem WLAN redundante Funkstrecken mit dem Parallel Redundancy Protocols (PRP) herzustellen. Diese redundanten Funkstrecken bieten Ihnen eine hohe Ausfallsicherheit.

Die hohe Ausfallsicherheit erreicht PRP, indem PRP ein Zwillingspaket (verdoppeltes Paket) durch 2 unabhängige WLANs sendet. Solange 1 WLAN aktiv ist, transportiert PRP Datenpakete.

Sie haben die Möglichkeit, die gesamte Kommunikation über WLAN zu realisieren. Alternativ dazu ist auch eine Lösung möglich, in der 1 Teil der Kommunikation drahtgebunden und 1 Teil der Kommunikation drahtlos realisiert ist.



In Anwendungen mit schwierigen Rahmenbedingungen (bewegliche Teile, hohe Temperaturen) fungiert die drahtlose Strecke als umschaltfreies Backup zu einer kabelgebundenen Strecke.

12.23.1 Grundlegende Funktion

PRP-Geräte agieren als Sender und Empfänger von PRP-Paketen, wobei PRP-Geräte beide Rollen einnehmen.

Der Sender geht wie folgt vor:

1. Er dupliziert Pakete, Zwillingspakete, und sendet sie durch 2 unabhängige (W)LANs.
2. Er fügt beim Senden jedem Paket einen Redundancy Control Trailer (RCT) an.

Der RCT enthält folgende Informationen für den Empfänger:

- Er identifiziert das Paket als PRP-Paket.
- Er enthält eine Sequence-ID.
- Er weist aus, über welches (W)LAN das Paket kam.

- Er enthält die Paketgröße.

Die Sequence-ID ist eine fortlaufend hochgezählte Nummer. Die Sequence-ID sorgt mit der Quellen-MAC-Adresse dafür, dass das Paket in die Duplicate Detection eingeht. Die Duplicate Detection erkennt Duplikate und verwirft das später eingetroffene Paket.

Der Empfänger geht wie folgt vor:

- Er liest den RCT.
- Er leitet das zuerst emfpangene Zwillingspaket ohne RCT weiter.
- Über die Duplicate Detection erkennt der Empfänger später eingetroffene Zwillingspakete und verwirft diese.

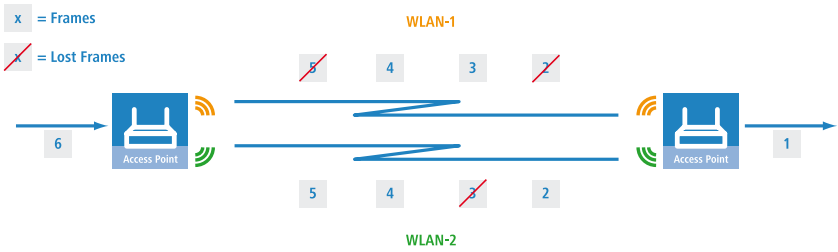
12.23.2 Vorteile von WLAN-PRP

PRP bietet Ihnen aufgrund seiner Funktionsweise bei WLAN deutliche Vorteile. In der Praxis verbesserten sich mit PRP die 3 bedeutendsten Qualitätsindikatoren eines Netzwerkes: Laufzeitschwankungen, Latenz und Paketverluste.

Mit PRP leiten Empfänger stets das zuerst eingetroffene Paket weiter und verwerfen das später eingetroffene. Da die Geräte stets das zuerst eingetroffene Paket weiterleiten, verringert sich die Latenz. In der Praxis waren deutliche Verbesserungen sowohl bei der durchschnittlichen als auch maximalen Laufzeitschwankung zu beobachten.

WLAN ist wie Ethernet als geteiltes Medium ausgelegt. In einer einzelnen WLAN-Verbindung halten die Geräte Pakete zurück, wenn das Medium belegt ist. Da die Geräte mit PRP Daten über 2 unabhängige WLANs transportieren, stehen wegen der Frequenzteilung praktisch 2 Medien zur Verfügung.

Mit PRP senden die Geräte jedes Paket doppelt, deswegen ist PRP teilweise in der Lage unsystematische Paketverluste auszugleichen. Solange der Empfänger eines der Pakete empfängt, ist die Kommunikation erfolgreich. Eine Neuübertragung eines einzelnen, verlorenen Paketes entfällt unter Umständen, was sich ebenfalls positiv auf Laufzeitschwankungen auswirkt.



12.23.3 PRP-Implementation in Dual-Radio Geräten der LANCOM IAP- und OAP-Serie

Die Dual-Radio Geräte der LANCOM IAP- und OAP-Serie (z. B. IAP-322, OAP-822 etc.) bieten Ihnen die Möglichkeit zum Aufbau eines PRP-Netzwerkes. Der AP übernimmt alle Funktionen, die für den Aufbau eines PRP-Netzwerkes notwendig sind.

Die Geräte bieten Ihnen folgende Möglichkeiten:

1. PRP-Netzwerke über beliebige Schnittstellen realisierbar; drahtlos oder drahtgebunden oder gemischt
2. pro Gerät sind bis zu 2 PRP-Netzwerke realisierbar
3. zusätzlich zu einem PRP-Netzwerk an einen AP weitere Clients anschließen
4. Dual Roaming aktivieren, sodass mit PRP die 2 WLAN-Module zeitverzögert roamen
5. umfassende Diagnosemöglichkeiten

12.23.4 PRP ausschließlich über WLAN realisieren

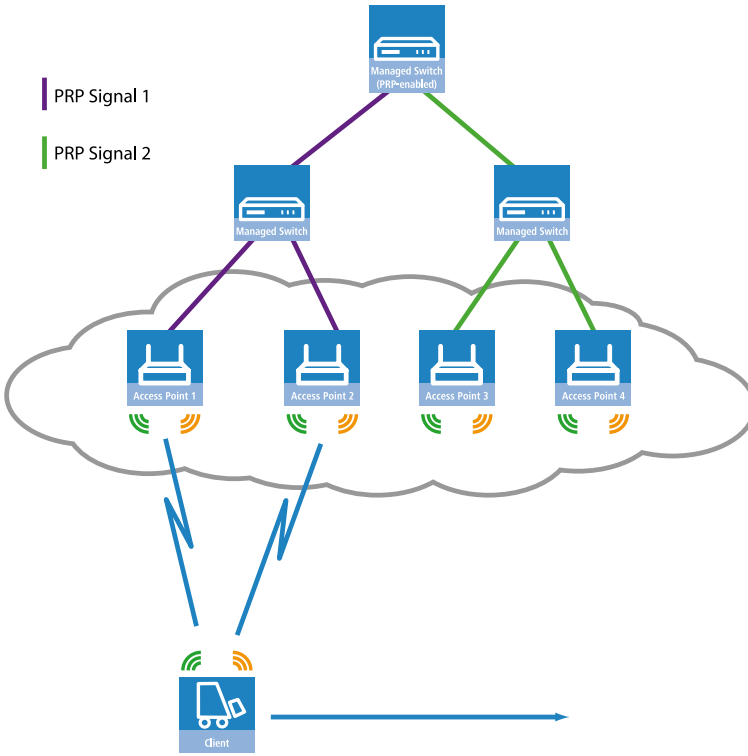
Sie haben die Möglichkeit, mit den Geräten ein PRP-Netzwerk komplett über WLAN aufzubauen. Dies eignet sich vor allem dann, wenn die Kosten einer Verkabelung hoch sind. Eine WLAN-Lösung eignet sich auch dann, wenn die Anwendungsart oder Umgebungsbedingungen dies erfordern.

12.23.5 Dual Roaming

Verfügt ein Gerät über 1 WLAN-Modul, unterbricht der Datenverkehr in einem Handover-Szenario.

Verfügt ein Gerät über 2 WLAN-Module lassen sich mit PRP Unterbrechungen verringern, wenn der Anwender in LANconfig verbietet, dass beide WLAN-Module gleichzeitig roamen. Dieser Modus heißt Dual Roaming.

Eine praktische Anwendung ist ein Client, der sich an Access Points vorbeibewegt. Durch den spezifischen Aufbau des Netzwerkes ist im Regelfall 1 WLAN-Modul verbunden und empfängt PRP-Pakete, während das andere WLAN-Modul sich in den nächsten AP einwählen kann.



Ein konkretes Anwendungsbeispiel ist die Materialwirtschaft, dort insbesondere das Überwachen von Warenbewegungen in Echtzeit.

Ein weiteres Anwendungsbeispiel ist der Bahnverkehr. Ein AP in einem Zug verbindet sich während der Fahrt mit den APs an der Strecke.

Zusätzlich können Sie im LANconfig die Block-Zeit bestimmen. Die Block-Zeit legt die Mindestsperrzeit fest, die zwischen den Roaming-Vorgängen unterschiedlicher WLAN-Module des gleichen Gerätes vergeht.

12.23.6 Unterstützung von Diagnosemöglichkeiten

Empfänger von PRP-Paketen verwerfen im Normalbetrieb Duplikate und entfernen den RCT von Paketen, die sie an ihren gebündelten Ausgangsport weiterleiten.

Um das Netzwerk auf korrekte Funktion zu untersuchen, stellt Ihnen HiLCOS folgende Optionen zur Verfügung, die Sie bei der Netzwerkdiagnose unterstützen:

1. Weiterleiten von Paket-Duplikaten ohne RCT
2. Weiterleiten von Einzelpaketen mit RCT
3. Weiterleiten von Paket-Duplikaten mit RCT

Zusätzlich verfügt HiLCOS über folgende Trace-Optionen:

1. trace # PRP-DATA
2. trace # PRP-NODES

PRP-DATA enthält Informationen zu gesendeten und empfangenen Paketen. Enthaltene Informationen: Name der Schnittstellen-Gruppe, die das Paket transportiert; Transportrichtung des Paketes (RX|TX); Trailer-Sequenznummer; MAC-Adresse des Partner-Gerätes; Schnittstelle innerhalb der PRP-Gruppe (A|B), die das Paket transportiert; Behandlung des Paketes (accept|discard)

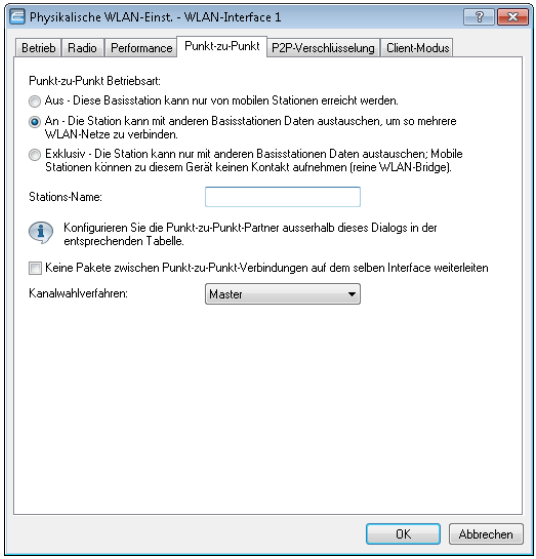
PRP-NODES enthält die folgenden Informationen: Neue Adresse in der (Proxy-)Node-Tabelle, Adresse aus der (Proxy-)Node-Tabelle entfernt, Node-Typ einer Adresse hat sich geändert.

12.23.7 Tutorial: Einrichtung einer PRP-Verbindung über ein Point-to-Point-Netz (P2P)

Hinweis: Die folgenden Schritte sind für beide P2P-Partner konform durchzuführen.

Um eine P2P-Verbindung zwischen zwei PRP-fähigen APs einzurichten, gehen Sie wie folgt vor:

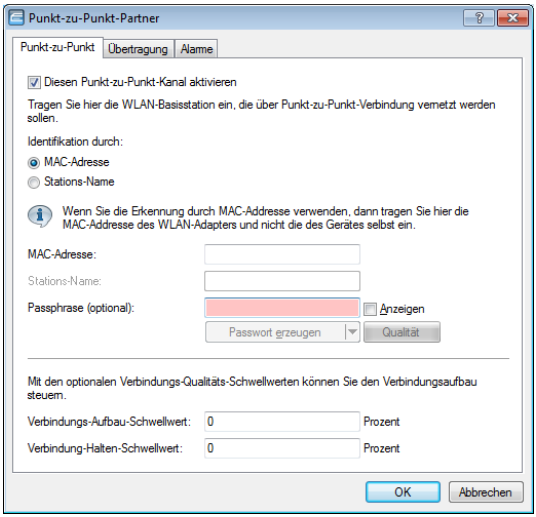
1. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** in der Ansicht **Betrieb** beide physikalischen WLAN-Schnittstellen (WLAN-Interface 1, WLAN-Interface 2) und in der Ansicht **Punkt-zu-Punkt** die **Punkt-zu-Punkt Betriebsart**.



2. Vergeben Sie für die physikalischen WLAN-Schnittstellen jeweils im Feld **Stations-Name** einen im WLAN eindeutigen Namen. Falls der P2P-Partner die betreffende Schnittstelle über die MAC-Adresse identifizieren kann oder soll, lassen Sie dieses Feld leer.

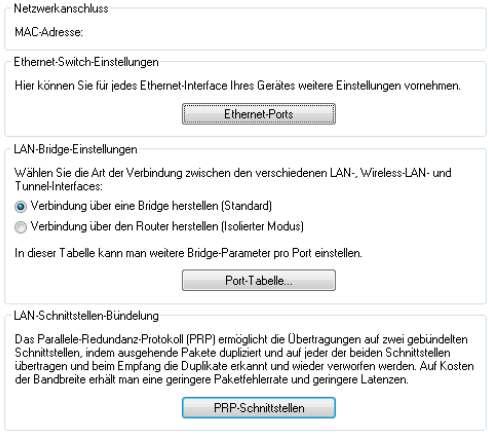
   Wichtig: Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

3. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Punkt-zu-Punkt-Partner** die Punkt-zu-Punkt-Kanäle "P2P-1-1" und "P2P-2-1" und bestimmen Sie die Schnittstellen-Kennungen der jeweiligen Punkt-zu-Punkt-Partner (**MAC-Adresse** oder **Stations-Name**).

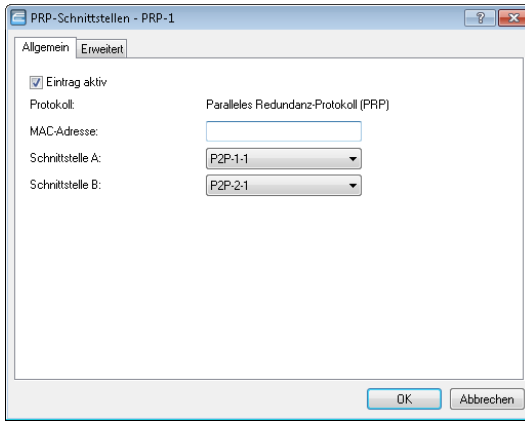


Geben Sie entweder die MAC-Adresse oder den Stations-Namen der entsprechenden WLAN-Schnittstelle des P2P-Partners an. Den Stations-Namen haben Sie im vorherigen Schritt vergeben.

4. Öffnen Sie die PRP-Konfiguration unter **Schnittstellen** > **LAN** mit einem Klick auf **PRP-Schnittstellen**.



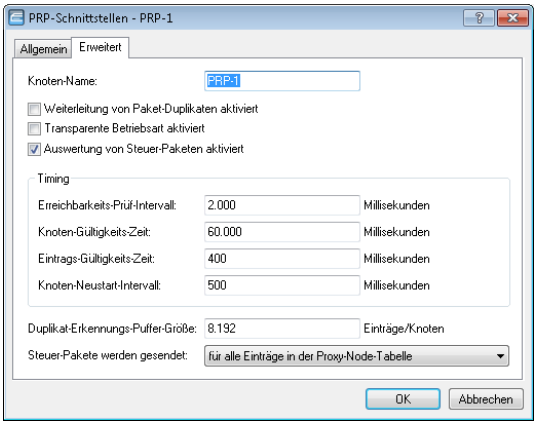
5. Aktivieren Sie die PRP-Schnittstellen und bestimmen Sie, welche Schnittstellen der AP zur Bündelung verwendet.



Wählen Sie hier die zuvor aktivierten Punkt-zu-Punkt-Schnittstellen "P2P-1-1" und "P2P-2-1" aus.

Wichtig: Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

6. Die Standard-Konfiguration der erweiterten Einstellungen übernehmen Sie mit einem Klick auf **OK**.



Die Einrichtung einer PRP-Verbindung über ein Point-to-Point-Netz ist damit abgeschlossen.

12.23.8 Tutorial: Roaming mit einem Dual-Radio-Client und PRP

Ein gängiger Weg, die Ausfallsicherheit einer WLAN-Infrastruktur zu erhöhen, ist der Betrieb der dazugehörigen APs in unterschiedlichen Frequenzbänden. Hierzu strahlen die physikalischen WLAN-Schnittstellen der APs z. B. eine SSID-1 im 2,4-Ghz-Band und eine SSID-2 im 5-GHz-Band aus. Wechselt ein PRP-fähiger Dual-Radio-Client von der Funkzelle einer physikalischen WLAN-Schnittstelle in eine benachbarte-Funkzelle der gleichen Infrastruktur, ermöglicht PRP einen verlustfreien Zellenübergang.

Dazu koppelt der Dual-Radio-Client über PRP anfangs z. B. seine physikalische WLAN-Schnittstelle WLAN-1 mit SSID-1 und WLAN-2 mit SSID-2. Verschlechtert sich der Empfang von SSID-1 und ist eine andere Funkzelle mit besserem Empfang in Reichweite, führt der Dual-Radio-Client einen Zellenwechsel durch. Beim Zellenübergang sendet der Dual-Radio-Client über WLAN-2 die Daten noch an SSID-2, während WLAN-1 bereits dieselben Daten an SSID-1 der besseren Funkzelle überträgt. Ein PRP-fähiger Switch filtert die doppelten PRP-Datenpakete heraus, bevor er die Daten ins LAN weiterleitet.

Hinweis: Die APs der WLAN-Infrastruktur müssen in einem solchen Szenario nicht für den PRP-Betrieb konfiguriert sein.

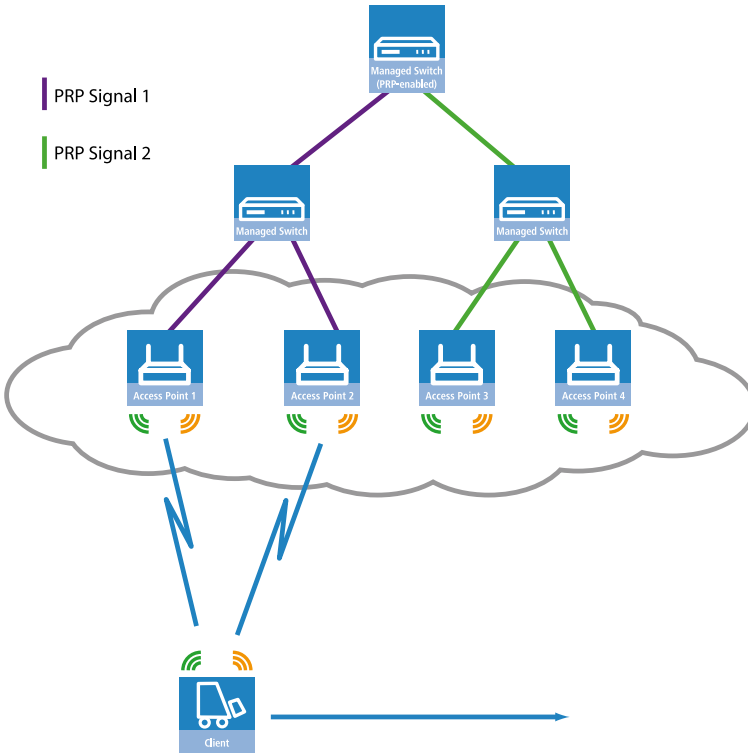
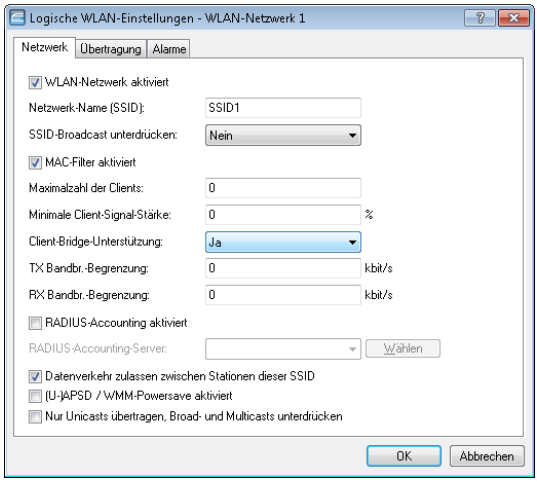


Abbildung 7: Roaming eines Dual-Radio-Clients in einer PRP-gestützten WLAN-Infrastruktur

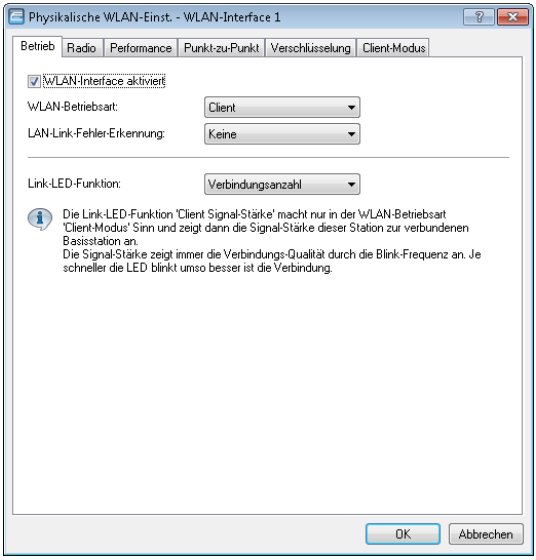
Damit der Empfänger Duplikate der Datenpakete erkennt, müssen die APs der WLAN-Infrastruktur im Client-Bridge-Modus arbeiten. Die MAC-Adresse des Dual-Radio-Clients sorgt zusammen mit dem RCT dafür, dass der Empfänger die doppelten Datenpakete erkennt. Ohne den Client-Bridge-Support würden die APs der WLAN-Infrastruktur die MAC-Adresse des Dual-Radio-Clients durch die eigene MAC-Adresse ersetzen und damit eine Erkennung der Duplikate verhindern.

Die Client-Bridge-Unterstützung lässt sich im LANconfig unter **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** in der Ansicht **Netzwerk** aktivieren.



Die PRP-Konfiguration des Dual-Radio-Clients erfolgt in den folgenden Schritten:

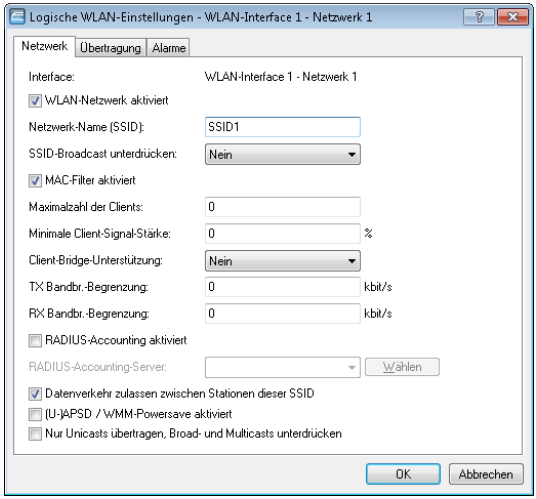
1. Aktivieren Sie unter **Wireless-LAN** > **Allgemein** > **Physikalische WLAN-Einst.** in der Ansicht **Betrieb** beide physikalische WLAN-Schnittstellen (WLAN-Interface 1, WLAN-Interface 2) und wechseln Sie die **WLAN-Betriebsart** jeweils zu **Client**.



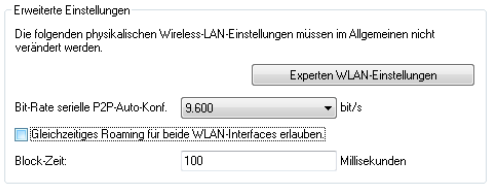
Legen Sie die restlichen WLAN-Parameter unter **Radio**, **Performance**, **Verschlüsselung** und **Client-Modus** entsprechend den Vorgaben der WLAN-Funkzellen fest.

Wichtig: Damit PRP reibungslos funktioniert, müssen beide PRP-Instanzen auf getrennten physikalischen Schnittstellen aktiv sein. Sofern Sie PRP auf zwei logischen Schnittstellen einer einzelnen physikalischen Schnittstelle einsetzen (z. B. "P2P-1-1" und "P2P-1-2"), überträgt das Gerät die Daten sequenziell. Dies führt neben dem Verlust der Redundanz z. B. auch zu Verzögerungen bei der Datenübertragung und einer Reduzierung der Bandbreite.

2. Zum Eintragen der SSID wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein**, klicken **Logische WLAN-Einstellungen** und wählen jeweils das Netz 1 der entsprechenden WLAN-Schnittstelle aus.
3. Tragen Sie im Feld **Netz-Name (SSID)** die Bezeichnung des WLANs ein, an das Sie die WLAN-Schnittstelle koppeln wollen.



4. Deaktivieren Sie unter **Wireless-LAN** > **Allgemein** im Abschnitt **Erweiterte Einstellungen** die Option **Gleichzeitiges Roaming für beide WLAN-Interfaces erlauben**.



Mit der Deaktivierung des gleichzeitigen Roamings verhindern Sie, dass beide physikalischen WLAN-Schnittstellen gleichzeitig Roaming bzw. Background-Scans durchführen und dadurch ggf. zusammen die Verbindung zu ihren Funkzellen verlieren.

So konfiguriert, kann sich der Dual-Radio-Client z. B. entlang einer Strecke von APs vorbeibewegen und zwischen den einzelnen APs roamen (siehe *Abbildung 7: Roaming eines Dual-Radio-Clients in einer PRP-gestützten WLAN-Infrastruktur* auf Seite 1243).

12.23.9 Queue-Bearbeitung für Wireless-PRP

Eine zu große Datenmenge an einer Wireless-Verbindung vermindert die Leistungsfähigkeit von Wireless-PRP. Ein beispielhaftes Szenario verdeutlicht dies:

- Die WLAN-Schnittstelle braucht länger, um den Kanal zu erreichen.
- An dieser WLAN-Schnittstelle erhöht sich die Zahl der PRP-Pakete in der Warteschleife.
- Als Ergebnis kann die PRP-Paketverzögerung größer sein als die PRP-EntryForgetTime.
- Somit entfällt die Duplicate-Detection-Funktion.
- Dies verhindert die Erkennung und Löschung redundanter PRP-Pakete.
- In der Folge wächst der Datenstrom unnötig an.

Mit dem Controlled-Delay-Algorithmus bietet Hirschmann die Möglichkeit, das oben beschriebene Szenario zu vermeiden. Der Controlled-Delay-Algorithmus hilft mit einer einer optimierten Queue-Bearbeitung, die Verzögerung des Datenstroms gering zu halten.

12.23.10 Wireless-PRP Micro-reordering Buffer

Der Wireless-PRP Micro-reordering Buffer hilft, das Vertauschen von Paketen im Datenstrom beim Einsatz von PRP über WLAN-Strecken zu vermeiden. Kommen Pakete im resultierenden Datenstrom in der falschen Reihenfolge an, ist die Ursache das gleichzeitige Auftreten der folgenden Fälle: Auf einer WLAN-Strecke treten Verzögerungen auf, während auf der anderen WLAN-Strecke Pakete verloren gehen.

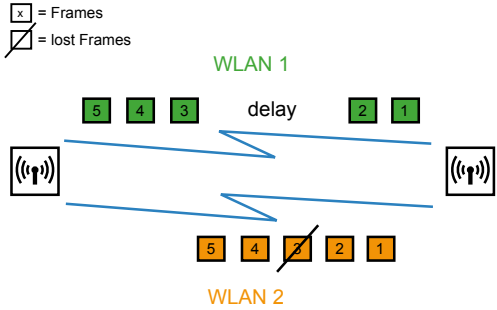
Folgende Faktoren können zu Verzögerungen auf einer WLAN-Strecke führen:

- Unterschiedliche Datenrate und damit Latenz der Übertragung eines Pakets auf einer WLAN-Strecke
- Verzögerungen aufgrund von Paket-Aggregation
- Verzögerungen beim Paketversand

Eine Ursache für den Verlust von Paketen können Interferenzen sein.

Das folgende Beispiel zeigt schematisch, wie die Pakete des resultierenden Datenstroms in eine falsche Reihenfolge geraten:

- WLAN-Strecke 1 sendet die Pakete 3–5 verzögert und WLAN-Strecke 2 verliert das Paket 3:



- Die Pakete des resultierenden Datenstroms kommen in der falschen Reihenfolge an:

Der PRP Micro-reordering Buffer bietet die Möglichkeit, die Pakete trotz des oben beschriebenen Szenarios in die richtige Reihenfolge zu bringen. Der PRP Micro-reordering Buffer arbeitet zunächst wie folgt:

- Er überwacht den Paketzähler, um fehlende Pakete zu ermitteln.
- Er puffert sämtliche Pakete, so bald ein Paket eintrifft, bei dem ein Vorgängerpaket oder mehrere Vorgängerpakete fehlen.

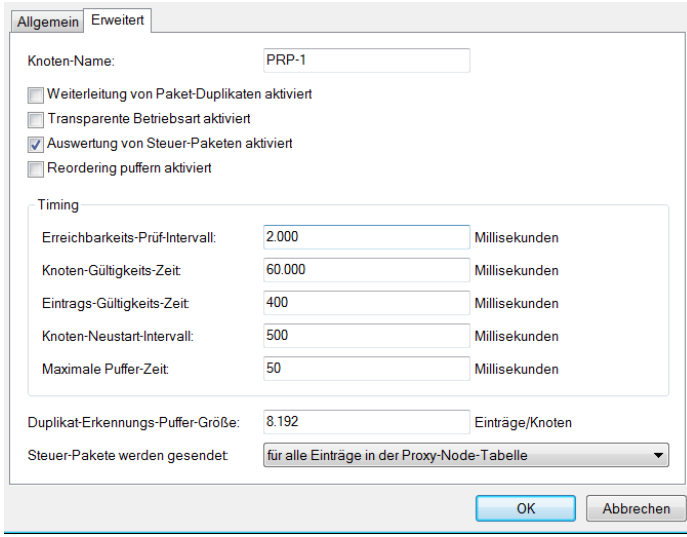
Das weitere Vorgehen des Micro-reordering Buffers hängt davon ab, ob das fehlende Paket rechtzeitig eintrifft:

- Trifft das fehlende Paket innerhalb der festgelegten Pufferzeit ein, bringt der Wireless-PRP Micro-reordering Buffer die Pakete in die richtige Reihenfolge. Anschließend entfernt er die Pakete aus dem Puffer und leitet sie weiter.
- Ist die festgelegte Pufferzeit überschritten, bevor das fehlende Paket eintrifft, bringt der Wireless-PRP Micro-reordering Buffer die vorhandenen Pakete in die richtige Reihenfolge. Anschließend entfernt er die Pakete aus dem Puffer und leitet sie ohne das fehlende Paket weiter.
- Ist die Pufferkapazität überschritten, bevor das fehlende Paket eintrifft, bringt derWireless-PRP Micro-reordering Buffer die vorhandenen Pakete in die richtige Reihenfolge. Anschließend entfernt er die Pakete aus dem Puffer und leitet sie ohne das fehlende Paket weiter.

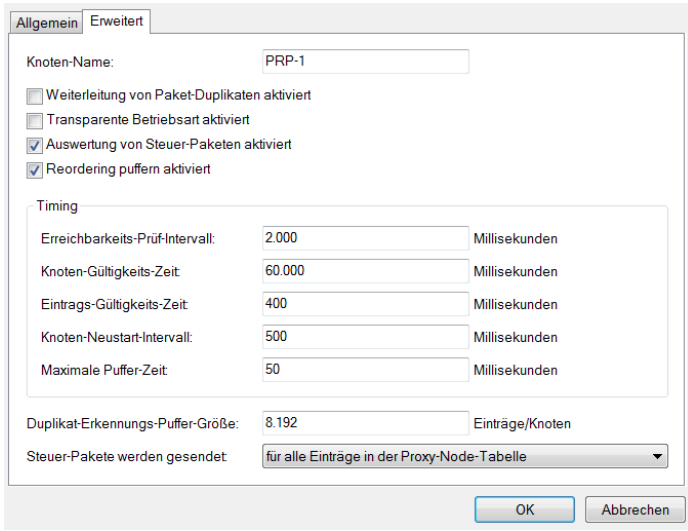
12.23.11 Tutorial: PRP Micro-reordering Buffer

Sie verfügen über einen OpenBAT mit aktivierten PRP-Schnittstellen PRP-1.

1. Wechseln Sie in die Ansicht **Schnittstellen** > **LAN** > **PRP-Schnittstellen** > **PRP-1** > **Erweitert**



2. Aktivieren Sie die Option **Reordering puffern aktiviert**.
3. Legen Sie die gewünschte **Maximale Puffer-Zeit** fest.



4. Klicken Sie **OK**.

Sie haben den PRP Micro-reordering Buffer aktiviert und die maximale Pufferzeit festgelegt.

12.24 C2C-Coupling

Die kabellose C2C-Coupling-Funktion bietet Ihnen die Möglichkeit, dass sich APs über Punkt-zu-Punkt-Verbindungen verbinden, ohne dass die MAC-Adresse oder der AP-Name zur Identifikation des Partner-APs vorkonfiguriert ist. Ein Verbindungsaufbau kommt zwischen den P2P-Partnern mit der geringsten Distanz zustande. Die kabellose Identifikation des P2P-Partners in Zugwaggons hat gegenüber einer Verkabelungslösung folgende Vorteile:

- Das serielle Überbrückungskabel, das bislang zum Aufbau der P2P-Verbindung zwischen den beiden Geräten in den Zugwaggons nötig war, entfällt.
- Wegfall der Probleme, die beispielsweise durch gestohlene Überbrückungskabel entstehen.

Beim C2C-Coupling wird der P2P-Partner nicht anhand der MAC-Adresse ermittelt, sondern anhand eines C2C-Identifiers. Die C2C-Coupling-Funktion bietet 2 Betriebsarten an:

- Automatisch: Die APs starten die Suche nach P2P-Partnern automatisch. P2P-Partner mit demselbem C2C-Identifier bauen automatisch eine P2P-Verbindung auf. Haben mehrere Partner denselben C2C-Identifier, wird die Verbindung zu dem Partner mit der geringsten Distanz aufgebaut.
- Manuell: Die APs starten und beenden die Suche nach P2P-Partnern über das CLI oder das serielle C2C-Interface-Protokoll. Die entsprechenden Kommandos gehen von jeweils einem Steuergerät aus, das den APs auch die C2C-Identifier zuweist.

Hinweis:

Verschlüsseln Sie die P2P-Verbindung entsprechend Ihrer Anforderungen. Die Einstellungen zur Verschlüsselung einer P2P-Verbindung finden Sie im Abschnitt *Konfiguration der Punkt-zu-Punkt-Verbindungen* auf Seite 1172.

12.24.1 Programmierung des C2C-Interface-Protokolls

Die APs müssen in der Lage sein, die seriellen Pakete zur Kontrolle der C2C-Coupling-Funktion zu dekodieren. Der Outband-Port der APs kann dabei

weiterhin als Konfigurations-Schnittstelle genutzt werden. Die Erkennung des Steuergerätes (Master) geschieht folgendermaßen:

1. Setzen Sie den seriellen Port auf die festgelegte Bitrate und schalten Sie das Handshaking aus.
2. Verschicken Sie ca. 0,5 Sek. lang STX-Zeichen mit einer Bitrate von mindestens 10 Zeichen pro Sekunde.
3. Wurden nach den 0,5 Sek. mindestens 3 STX-Zeichen empfangen, ist davon auszugehen, dass das Steuergerät bereit ist, über das C2C-Interface-Protokoll zu kommunizieren.
4. Nun erfolgt eine exklusive Registrierung der Outband-Ports der APs, und das C2C-Interface-Protokoll startet.

Die Kommunikations-Pakete sind von folgenden ASCII-Kontrollzeichen umschlossen: STX (start of text) und ETX (end of text). Daten außerhalb dieses Rahmens verwirft der AP. Die Datensatz-Felder sind durch Doppelpunkte voneinander getrennt. Der Empfänger prüft Forward-Pakete und Backward-Pakete und verwirft sie im Falle von Code-Verletzungen.

Forward-Paket

Ein Forward-Paket ist folgendermaßen aufgebaut:

```
<STX>:<WLANn>:<CMD>:<LENGTH>:<DATA>:<CRC><ETX>
```

WLANn	Festlegung des WLAN-Identifiers mit n = 1, 2, 3,...
CMD	1 Datenbyte "XXXX XXXX" enthält die relevanten Kommandos
LENGTH	1 Datenbyte "XXXX XXXX" enthält die Länge des Datenfeldes
DATA	255 Oktette oder weniger enthalten Daten gemäß der Kommandos
CRC	CRC-32-Prüfung der Felder CMD, LENGTH und DATA (beginnend mit dem ersten Zeichen nach STX bis zum letzten Zeichen des Wertes) als Dezimalzahl ausgedrückt

Backward-Paket

Ein Backward-Paket wird erst nach dem Empfang eines Kommandos gesendet und ist folgendermaßen aufgebaut:

```
<STX><DATA>:<CRC><ETX>
```

DATA 1 Datenbyte "XXXX XXXX" enthält abhängig vom Kommando (= Antwort) entweder eine "Yes", "No" oder 8-Bit Information:

- "Yes": 1111 1111
- "No": Der AP soll nicht reagieren
- 8-Bit-Information: XXXX XXXX

CRC CRC-32-Prüfung der Felder CMD, LENGTH und DATA (beginnend mit dem ersten Zeichen nach STX bis zum letzten Zeichen des Wertes) als Dezimalzahl ausgedrückt

Definition der Steuerkommandos

Kommando 0: 0x00 "OFF"

Stoppt die C2C-Coupling-Funktion auf dem ausgewählten WLAN und löscht den gespeicherten C2C-Identifier.

Beispiel:

```
<STX>:<WLAN1>:<0x00>:<0x00>:CRC><ETX>
```

Kommando 1: 0x01 "START"

Startet die C2C-Coupling-Funktion auf dem ausgewählten WLAN und erzeugt den C2C-Identifier. Das "START"-Kommando wird gesendet, wenn sich die Zusammenstellung des Zuges ändert bzw. nach dem "OFF"-Kommando.

Beispiel:

```
<STX>:<WLAN1>:<0x01>:<0x07>:<UId2015>:<CRC><ETX>
```

Kommando 2: 0x02 "SCHEDOFF"

Die C2C-Coupling-Funktion wird nach dem festgelegten Timeout "C2C_OFF_TIMEOUT" (max. 600 Sekunden) ausgeschaltet. Während des Timeouts zeigt Bit 5 des Statusregisters "OFFTIMERRUN" an. Wenn die C2C-Coupling-Funktion bereits ausgeschaltet ist, findet keine Veränderung statt.

Beispiel:

```
<STX>:<WLAN1>:<0x02>:<0x03>:<600>:<CRC><ETX>
```

Kommandos 3-15

Reserviert für künftige Anwendungen. Auf diese Kommandos reagiert der AP nicht.

Definition der Abfragekommandos

Kommando 16: 0x10 "STATUS"

Die Antworten im "STATUS INFORMATION"-Byte sind wie folgt definiert:

- Bit 0 "1" = ACTIVE (Die C2C-Coupling-Engine läuft.)
- Bit 1 "1" = DISCOVERY (Die C2C-Coupling-Engine befindet sich im Suchmodus.)
- Bit 3 "1" = CONNECTED (Der P2P-Link des APs ist aktiviert.)
- Bit 4 "1" = CONNLOST (Die Verbindung zum P2P-Partner ist beendet.)
- Bit 5 "1" = OFFTIMERRUN – (Der Timeout-Vorgang läuft.)

Der AP aktualisiert die "STATUS INFORMATION" gemäß der aktuellen Gegebenheiten regelmäßig.

Beispiel:

```
<STX>:<WLAN1>:<0x10>:<0x00>:<CRC><ETX>
```

Kommandos im Überblick

Kommando-Nummer	*Kommando-Code*	*Kommando-Name*
0	0x00	OFF
1	0x01	START
2	0x02	SCHEDOFF

Kommando-Nummer	*Kommando-Code*	*Kommando-Name*
3-15	-	RESERVED
16	0x10	STATUS

12.24.2 Fehlerbehebung

Dieses Kapitel unterstützt Sie dabei, mögliche Ursachen für etwaige Fehler beim C2C-Coupling zu erkennen und korrigierende Maßnahmen zu ergreifen.

Fehlerbehebung Betriebsart "Automatisch"

Fehler	*Mögliche Ursache*	*Fehlerbehebung*
C2C-Coupling kommt nicht zustande	Schlechte WLAN-Verbindung während des Kopplungsvorgangs	**1.** Sind die Antennen aufeinander ausgerichtet? **2.** Besteht zwischen den Antennen eine direkte Sichtbeziehung?
	Verbindung zum anderen AP kommt nicht zustande	**1.** Überprüfen Sie die Qualität der WLAN-Verbindung: Sind die Antennen aufeinander ausgerichtet? Besteht zwischen den Antennen eine direkte Sichtbeziehung? **2.** Ist die Konfiguration des P2P-Links korrekt? **3.** Ist der Verbindungs-Aufbau-Schwellwert zu hoch gesetzt?
	AP ohne Stromversorgung	Überprüfen Sie die Stromversorgung der APs.
C2C-Coupling startet immer wieder von neuem	Verbindungs-Qualitäts-Schwellwerte ungeeignet	Überprüfen Sie die Einstellungen des Verbindungs-Aufbau-Schwellwerts und des Verbindungs-Halten-Schwellwerts.
C2C-Coupling mit neuem Waggon nicht möglich	Abriss der Verbindung nicht erkannt	Setzen Sie einen geeigneten Verbindungs-Halten-Schwellwert. Die Verbindung wird ausschließlich dann als abgerissen erkannt, wenn das Signal-Rausch-Verhältnis für den aktuellen P2P-Partner geringer als

Fehler	*Mögliche Ursache*	*Fehlerbehebung*
		der festgelegte Verbindungs-Halten-Schwellwert ist.
Datenverbindung zum falschen Waggon	C2C-Coupling mit dem falschen Waggon	Setzen Sie einen geeigneten Verbindungs-Aufbau-Schwellwert, um Kopplungsversuche mit zu weit entfernten Waggons zu vehindern.
Verbindung zum anderen AP kommt nicht zustande	P2P-Link falsch konfiguriert	Überprüfen Sie die Konfiguration des P2P-Links.
	Verbindungs-Aufbau-Schwellwert zu hoch gesetzt	Setzen Sie einen geeigneten Verbindungs-Aufbau-Schwellwert.
	Schlechte WLAN-Verbindung	**1.** Sind die Antennen aufeinander ausgerichtet? **2.** Besteht zwischen den Antennen eine direkte Sichtbeziehung?

Fehlerbehebung Betriebsart "Manuell"

Fehler	*Mögliche Ursache*	*Fehlerbehebung*
C2C-Coupling kommt nicht zustande	Steuergerät defekt	Überprüfen Sie die Funktionsfähigkeit des Steuergerätes.
	Serielle Verbindung defekt	Überprüfen Sie Kabel und Stecker der seriellen Verbindung.
	Keine Verbindung des APs zum Steuergerät während des Kopplungsvorgangs	Überprüfen Sie die serielle Verbindung zwischen Steuergerät und AP: **1.** Parameter der seriellen Verbindung OK? **2.** Probeverbindung mittels STATUS-Kommando erfolgreich?
	Empfang falscher Kommandos während des Kopplungsvorgangs	**1.** Überprüfen Sie Kabel und Stecker der seriellen Verbindung. **2.** Überprüfen Sie, ob das Steuergerät vor dem Kopplungsvorgang die Kommandos entsprechend der Spezifikation sendet.

Fehler	*Mögliche Ursache*	*Fehlerbehebung*
	Kopplungsvorgang startet bei einem der APs zu spät	Überprüfen Sie, ob die Steuergeräte den Kopplungs-Trigger synchron senden.
	Schlechte WLAN-Verbindung während des Kopplungsvorgangs	**1.** Sind die Antennen aufeinander ausgerichtet? **2.** Besteht zwischen den Antennen eine direkte Sichtbeziehung?
	Verbindung zum anderen AP kommt nicht zustande	**1.** Überprüfen Sie die Qualität der WLAN-Verbindung: Sind die Antennen aufeinander ausgerichtet? Besteht zwischen den Antennen eine direkte Sichtbeziehung? **2.** Ist die Konfiguration des P2P-Links korrekt? **3.** Ist der Verbindungs-Aufbau-Schwellwert zu hoch gesetzt?
	AP ohne Stromversorgung	Überprüfen Sie die Stromversorgung der APs.
C2C-Coupling vorübergehend außer Betrieb	Empfang falscher Kommandos nach erfolgtem Kopplungsvorgang	Überprüfen Sie, ob das Steuergerät nach dem Kopplungsvorgang die Kommandos entsprechend der Spezifikation sendet.
	Abriss der Verbindung nicht erkannt	Setzen Sie einen geeigneten Verbindungs-Halten-Schwellwert. Die Verbindung wird ausschließlich dann als abgerissen erkannt, wenn das Signal-Rausch-Verhältnis für den aktuellen P2P-Partner geringer als der festgelegte Verbindungs-Halten-Schwellwert ist.
C2C-Coupling bricht ab	AP ohne Stromversorgung	Überprüfen Sie die Stromversorgung der APs.
Verbindung zum anderen AP kommt nicht zustande	P2P-Link falsch konfiguriert	Überprüfen Sie die Konfiguration des P2P-Links.
	Verbindungs-Aufbau-Schwellwert zu hoch gesetzt	Setzen Sie einen geeigneten Verbindungs-Aufbau-Schwellwert.

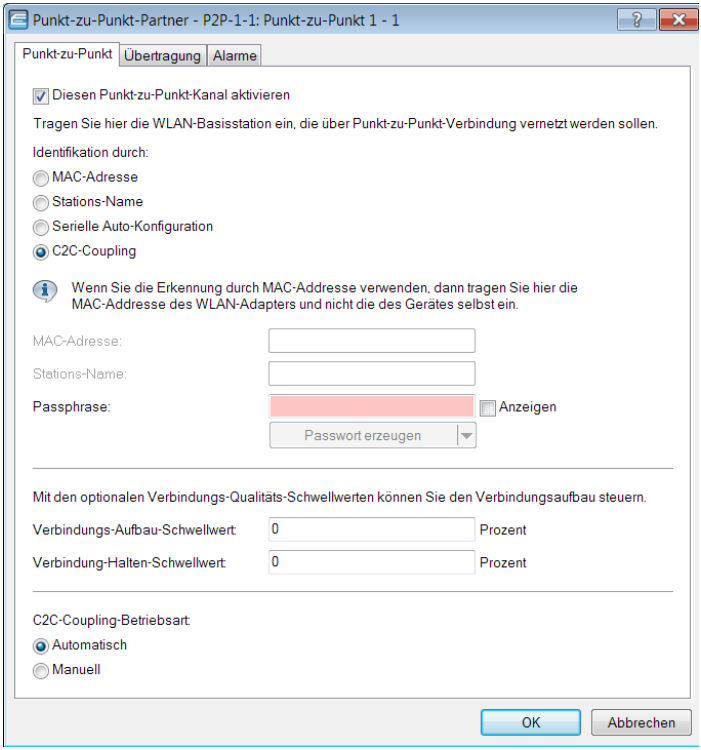
Fehler	*Mögliche Ursache*	*Fehlerbehebung*
	Schlechte WLAN-Verbindung	**1.** Sind die Antennen aufeinander ausgerichtet? **2.** Besteht zwischen den Antennen eine direkte Sichtbeziehung?

12.24.3 Tutorial: Konfiguration der C2C-Coupling-Funktion

Um die C2C-Coupling-Funktion zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein** > **Punkt-zu-Punkt-Partner**.
2. Wählen Sie einen Punkt-zu-Punkt-Partner aus, beispielsweise P2P-1-1.

   Hinweis: Die C2C-Coupling-Funktion unterstützt die folgenden P2P-Verbindungen: P2P-1-1 und P2P-2-1.



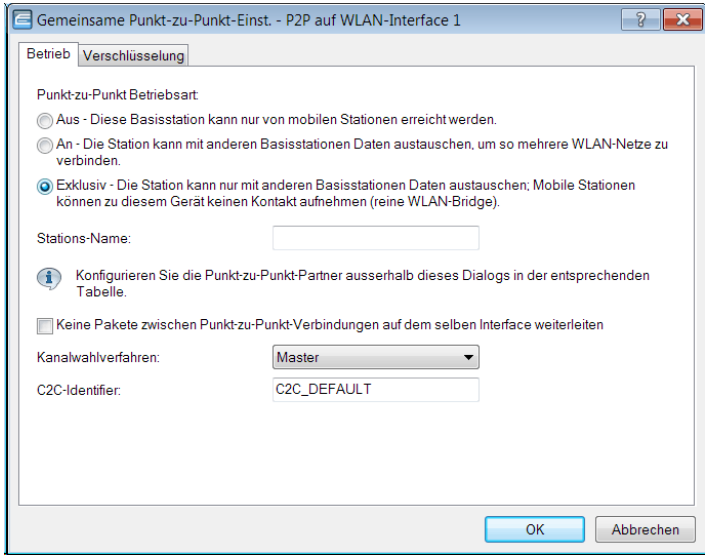
3. Aktivieren Sie auf der Registerkarte **Punkt-zu-Punkt** die Option **Diesen Punkt-zu-Punkt-Kanal aktivieren**.
4. Wählen Sie die Identifikation des P2P-Partners durch **C2C-Coupling**.
5. Geben Sie die **Passphrase** ein.
6. Wählen Sie für das C2C-Coupling die gewünschte Betriebsart **Automatisch** oder **Manuell**.
7. Setzen Sie die optionalen Verbindungs-Qualitäts-Schwellwerte.

   - **Verbindungs-Aufbau-Schwellwert**: Dieser Schwellwert gibt die Signalstärke in Prozent an, die ein P2P-Partner mindestens aufweisen muss, damit ein AP einen Versuch zum Einbuchen bei diesem P2P-Partner startet.
   - **Verbindungs-Halten-Schwellwert**: Dieser Schwellwert gibt die Signalstärke in Prozent an, die der aktuelle P2P-Partner mindestens

aufweisen muss, damit die Verbindung nicht als abgerissen betrachtet wird.

Hinweis: Der Verbindungs-Aufbau-Schwellwert bietet Ihnen die Möglichkeit, die Distanz, innerhalb derer nach P2P-Partnern gesucht wird, einzuschränken. In der Voreinstellung sind die Verbindungs-Qualitäts-Schwellwerte ausgeschaltet (Werte auf 0 % voreingestellt). Ermitteln Sie die Werte in Abhängigkeit Ihres konkreten Anwendungsfalles.

8. Klicken Sie die Schaltfläche **OK**.
9. Wechseln Sie in die Ansicht **Wireless-LAN** > **Allgemein** > **Gemeinsame Punkt-zu-Punkt-Einstellungen**.
10. Wählen Sie eine gemeinsame Punkt-zu-Punkt-Einstellung aus, beispielsweise "P2P auf WLAN-Interface 1".



11. Wählen Sie auf der Registerkarte **Betrieb** die Punkt-zu-Punkt-Betriebsart **Exklusiv**.
12. Wählen Sie unter **Kanalwahlverfahren** die Einstellung **Master**.
13. Geben Sie im Feld **C2C-Identifier** den gewünschten Namen für den C2C-Identifier ein. Der C2C-Identifier dient beim C2C-Coupling dazu, die P2P-

Partner eindeutig zu identifizieren. Die Default-Einstellung ist "C2C_DEFAULT".

14. Klicken Sie die Schaltfläche **OK**.
15. Aktivieren Sie auf der Registerkarte **Verschlüsselung** die Option **Verschlüsselung aktivieren**.
16. Klicken Sie die Schaltfläche **OK**.

Sie haben die C2C-Coupling-Funktion aktiviert und konfiguriert.

12.25 WLAN-Link-Status-Log

Das WLAN-Link-Status-Log bietet Ihnen die Möglichkeit, Informationen zur Qualität von WLAN-Links aufzuzeichnen und zu überwachen. Überwacht werden P2P-Links und AP-Client-Links. Die Überwachung startet mit der Aktivierung des WLAN-Links. Die Speicherung der Informationen zur Qualität der WLAN-Links im WLAN-Link-Status-Log erfolgt in bestimmten Zeitintervallen, die der Benutzer festlegt. Die Überwachung deaktivierter WLAN-Links endet nach einem durch den Benutzer festgelegten Zeitintervall, wobei die bestehenden Einträge erhalten bleiben. Die Informationen des WLAN-Link-Status-Logs sind verfügbar über eine Log-Tabelle des Gerätes, über ein USB-Speichermedium, über Syslog-Einträge oder über SNMP-Traps.

Im laufenden Betrieb können Sie via WEBconfig unter **HiLCOS-Menübaum** > **Status** > **WLAN** > **WLAN-Link-Status-Log** Informationen zur Qualität von WLAN-Links in den folgenden Tabellen einsehen:

- **Audit**

  Diese Tabelle enthält aktuelle Informationen zur Qualität von WLAN-Links und wird ständig aktualisiert.

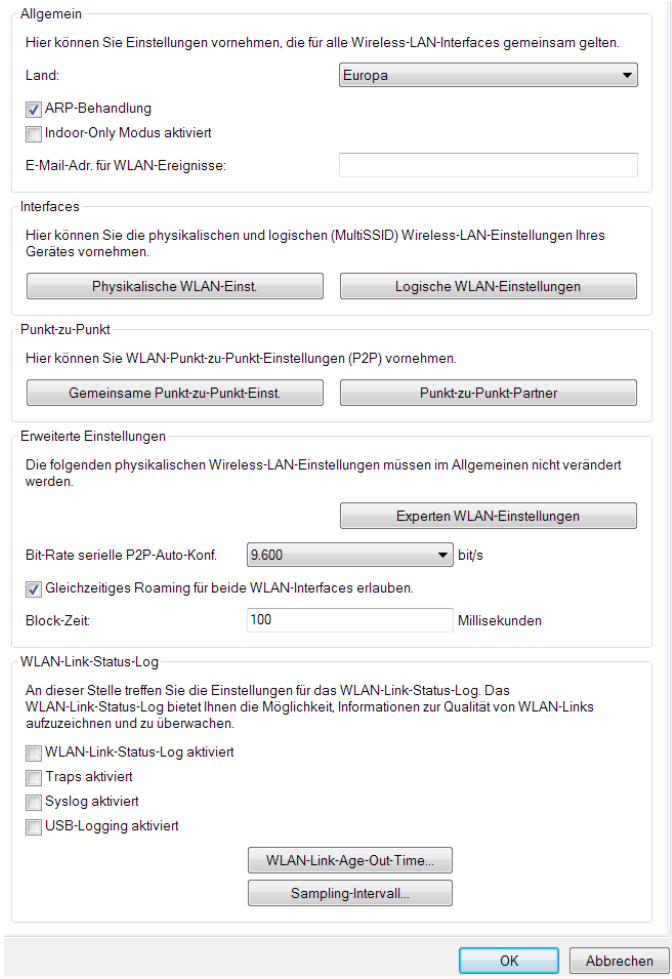
- **Log-Table**

  Diese Tabelle enthält die gespeicherten Informationen zur Qualität von WLAN-Links entsprechend des gewählten Zeitintervalls.

12.25.1 Tutorial: Konfiguration des WLAN-Link-Status-Logs

Um das WLAN-Link-Status-Log zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein**.



2. Aktivieren Sie im Abschnitt **WLAN-Link-Status-Log** die Option **WLAN-Link-Status-Log aktiviert**.

3. Wählen Sie die gewünschte Benachrichtigungsform (Mehrfachauswahl möglich) und aktivieren Sie dementsprechend die Option **Traps aktiviert**, **Syslog aktiviert** oder **USB-Logging aktiviert**.

   Hinweis: Weitere Informationen zur Konfiguration von Syslog finden Sie im Abschnitt *Konfiguration von SYSLOG über LANconfig* auf Seite 416.

   Hinweis: Die durch die Option **Traps aktiviert** generierten Traps und alle anderen im Gerät generierten Traps werden an alle manuell konfigurierten Trap-Empfänger gesendet.

4. Setzen Sie im Dialog **Sampling-Intervall** das gewünschte Zeitintervall für die Speicherung der Informationen zur Qualität der WLAN-Links.
5. Setzen Sie im Dialog **WLAN-Link-Age-Out-Time** das gewünschte Zeitintervall, nachdem die Überwachung eines inaktiven WLAN-Links enden soll.
6. Klicken Sie **OK**.

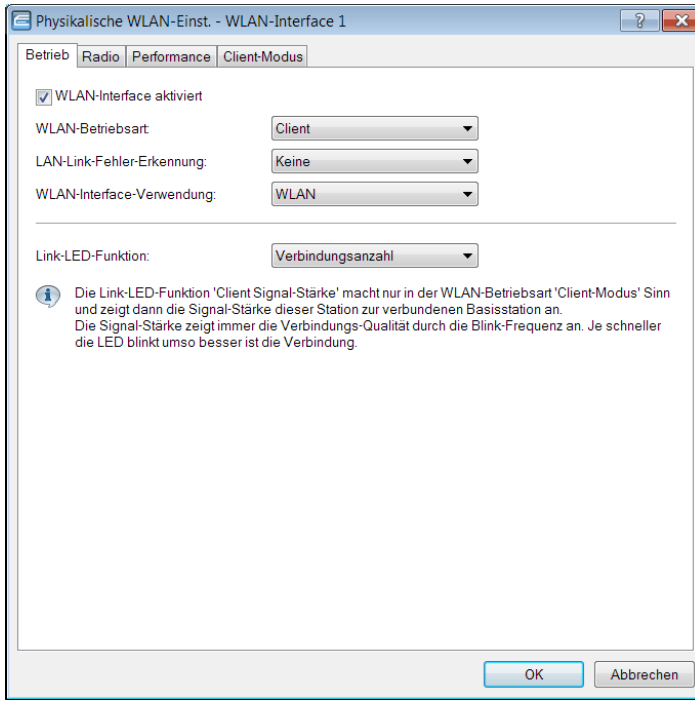
Sie haben das WLAN-Link-Status-Log aktiviert und konfiguriert.

12.26 Tutorial: N:N-Mapping über die WLAN-Schnittstelle

Detaillierte Informationen zu Anwendungsfällen und zur Konfiguration des N:N-Mapping finden Sie im Abschnitt *N:N-Mapping* auf Seite 530.

Um die Funktion "N:N-Mapping" über das WLAN-Interface des Gerätes zu aktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht **Wireless-LAN** > **Allgemein** > **Interfaces** > **Physikalische WLAN-Einstellungen**.
2. Wählen Sie ein WLAN-Interface aus, beispielsweise WLAN-Interface 1.



3. Aktivieren Sie auf der Registerkarte **Betrieb** die Option **WLAN-Interface aktiviert**.
4. Wählen Sie unter **WLAN-Betriebsart** die Option **Client**.
5. Wählen Sie unter **WLAN-Interface-Verwendung** die Option **DSL**.
6. Klicken Sie die Schaltfläche **OK**.

Sie haben die Funktion "N:N-Mapping" aktiviert.

13 WLAN-Management

13.1 Ausgangslage

Der weit verbreitete Einsatz von Wireless Access Points (APs) und Wireless Routern hat zu einem deutlich komfortableren und flexibleren Zugang zu Netzwerken in Firmen, Universitäten und anderen Organisationen geführt.

Bei allen Vorzügen der WLAN-Strukturen bleiben einige offene Aspekte:

- Alle APs benötigen eine Konfiguration und ein entsprechendes Monitoring zur Erkennung von unerwünschten WLAN-Clients etc. Die Administration der APs erfordert gerade bei größeren WLAN-Strukturen mit entsprechenden Sicherheitsmechanismen eine hohe Qualifikation und Erfahrung der Verantwortlichen und bindet erhebliche Ressourcen in den IT-Abteilungen.
- Die manuelle Anpassung der Konfigurationen in den APs bei Änderungen in der WLAN-Struktur zieht sich ggf. über einen längeren Zeitraum hinweg, sodass es zur gleichen Zeit unterschiedliche Konfigurationen im WLAN gibt.
- Durch die gemeinsame Nutzung des geteilten Übertragungsmediums (Luft) ist eine effektive Koordination der APs notwendig, um Frequenzüberlagerungen zu vermeiden und die Netzwerkperformance zu optimieren.
- APs an öffentlich zugänglichen Orten stellen ein potenzielles Sicherheitsrisiko dar, weil mit den Geräten auch die darin gespeicherten, sicherheitsrelevanten Daten wie Kennwörter etc. gestohlen werden können. Außerdem können ggf. unbemerkt fremde APs mit dem LAN verbunden werden und so die geltenden Sicherheitsrichtlinien umgehen.

13.2 Technische Konzepte

Mit einem zentralen WLAN-Management lassen sich diese Probleme lösen. Die Konfiguration der APs wird dabei nicht mehr in den Geräten selbst vorgenommen, sondern in einer zentralen Instanz, dem WLAN-Controller (WLC).

Der WLC authentifiziert die APs und überträgt den zugelassenen Geräten eine passende Konfiguration. Dadurch kann die Konfiguration des WLANs komfortabel von einer zentralen Stelle übernommen werden und die Konfigurationsänderungen wirken sich zeitgleich auf alle APs aus. Da die vom WLC zugewiesene Konfiguration in den APs optional **nicht** im Flash, sondern im RAM abgelegt wird, können in besonders sicherheitskritischen Netzen bei einem Diebstahl der Geräte auch keine sicherheitsrelevanten Daten in unbefugte Hände geraten. Nur im "autarken Weiterbetrieb" wird die Konfiguration für eine definierte Zeit optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist).

13.2.1 Der CAPWAP-Standard

Mit dem CAPWAP-Protokoll (Control And Provisioning of Wireless Access Points) stellt die IETF (Internet Engineering Task Force) einen Standard für das zentrale Management großer WLAN-Strukturen vor.

CAPWAP verwendet zwei Kanäle für die Datenübertragung:

- Kontrollkanal, verschlüsselt mit Datagram Transport Layer Security (DTLS). Über diesen Kanal werden die Verwaltungsinformationen zwischen dem WLC und dem AP ausgetauscht.

  Hinweis: DTLS ist ein auf TLS basierendes Verschlüsselungsprotokoll, welches im Gegensatz zu TLS auch über verbindungslose, ungesicherte Transportprotokolle wie UDP übertragen werden kann. DTLS verbindet so die Vorteile der hohen Sicherheit von TLS mit der schnellen Übertragung über UDP. DTLS eignet sich damit – anders als TLS – auch für die Übertragung von VoIP-Paketen, da hier nach einem Paketverlust die folgenden Pakete wieder authentifiziert werden können.

- Datenkanal, optional ebenfalls verschlüsselt mit DTLS. Über diesen Kanal werden die Nutzdaten aus dem WLAN vom AP über den WLC ins LAN übertragen – gekapselt in das CAPWAP-Protokoll.

13.2.2 Die Smart-Controller-Technologie

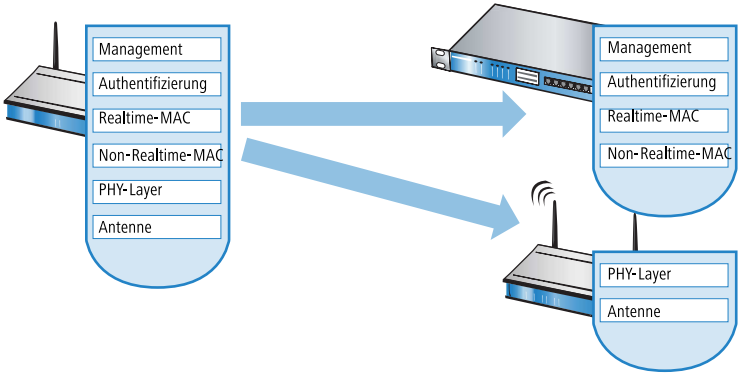
In einer dezentralen WLAN-Struktur mit autonomen APs (Stand-Alone-Betrieb als so genannte "Rich Access Points") sind alle Funktionen für die Datenübertragung auf dem PHY-Layer, die Kontroll-Funktionen auf dem MAC-Layer

sowie die Management-Funktionen in den APs enthalten. Mit dem zentralen WLAN-Management werden diese Aufgaben auf zwei verschiedene Geräte aufgeteilt:

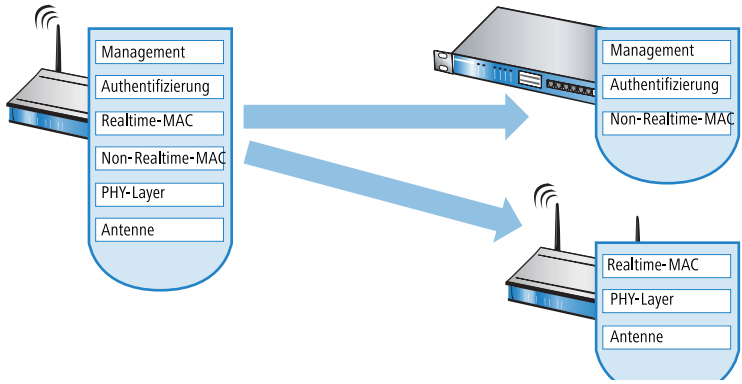
- Der zentrale WLC übernimmt die Verwaltungsaufgaben.
- Die verteilten APs übernehmen die Datenübertragung auf dem PHY-Layer und die MAC-Funktionen.
- Als dritte Komponenten kommt ggf. ein RADIUS- oder EAP-Server zur Authentifizierung der WLAN-Clients hinzu (was in autonomen WLANs aber auch der Fall sein kann).

CAPWAP beschreibt drei unterschiedliche Szenarien für die Verlagerung von WLAN-Funktionen in den zentralen WLC.

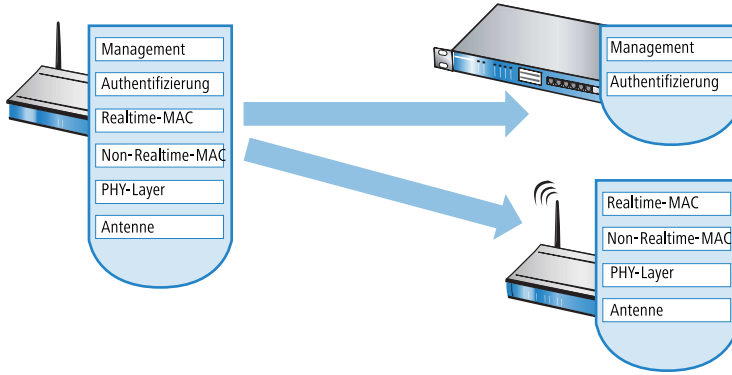
- Remote-MAC: Hier werden alle WLAN-Funktionen vom AP an den WLC übertragen. Die APs dienen hier nur als "verlängerte Antennen" ohne eigene Intelligenz.



- Split-MAC: Bei dieser Variante wird nur ein Teil der WLAN-Funktionen an den WLC übertragen. Üblicherweise werden die zeitkritischen Anwendungen (Realtime-Applikationen) weiterhin auf dem AP abgearbeitet, die nicht zeitkritischen Anwendungen (Non-Realtime-Applikationen) werden über den zentralen WLC abgewickelt.



- Local-MAC: Die dritte Möglichkeit sieht eine vollständige Verwaltung und Überwachung des WLAN-Datenverkehrs direkt in den APs vor. Zwischen dem AP und dem WLC werden lediglich Nachrichten zur Sicherung einer einheitlichen Konfiguration der APs und zum Management des Netzwerks ausgetauscht.



Die Smart-Controller-Technologie von Hirschmann setzt das Local-MAC-Verfahren ein. Durch die Reduzierung der zentralisierten Aufgaben bieten die WLAN-Strukturen eine optimale Skalierbarkeit. Gleichzeitig wird der WLC in einer solchen Struktur nicht zum zentralen Flaschenhals, der große Teile des gesamten Datenverkehrs verarbeiten muss. In Remote-MAC- und Split-MAC-Architekturen müssen immer **alle** Nutzdaten zentral über den WLC laufen. In Local-MAC-Architekturen können die Daten jedoch alternativ auch direkt von den APs in das LAN ausgekoppelt werden, sodass eine hochperformante Datenübertragung ermöglicht wird. WLCs mit Smart-Controller-Technologie

eignen sich daher auch für WLANs nach dem Standard IEEE 802.11n mit deutlich höheren Bandbreiten als in den bisher bekannten WLANs. Bei der Auskopplung in das LAN können die Daten auch direkt in spezielle VLANs geleitet werden, die Einrichtung von geschlossenen Netzwerken z. B. für Gast-Zugänge sind so leicht möglich.

Layer-3-Tunneling und Layer-3-Roaming

WLCs mit HiLCOS unterstützen ebenfalls die Übertragung der Nutzdaten durch einen CAPWAP-Tunnel. Auf diese Weise können z. B. ausgewählte Applikationen wie VoIP über den zentralen WLC geleitet werden. Beim Wechsel der WLAN-Clients in eine andere Funkzelle bleibt so die zugrundeliegende IP-Verbindung ohne Unterbrechung, da sie fortlaufend vom zentralen WLC verwaltet wird (Layer-3-Roaming).

Die zentrale Verwaltung der Datenströme kann in Umgebungen mit zahlreichen VLANs auch die Konfiguration der VLANs auf den Switch-Ports überflüssig machen, da alle CAPWAP-Tunnel zentral auf dem WLC verwaltet werden.

13.2.3 Kommunikation zwischen Access Point und WLAN-Controller

Die Kommunikation zwischen einem AP und dem WLC wird immer vom AP aus eingeleitet. Die Geräte suchen in folgenden Fällen nach einem WLC, der ihnen eine Konfiguration zuweisen kann:

- Bei Hirschmann APs sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die APs nach einem zentralen WLC, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLC gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.
- Während der AP nach einem WLC sucht, sind dessen WLAN-Module ausgeschaltet.

Der AP sendet zu Beginn der Kommunikation eine "Discovery Request Message", um die verfügbaren WLCs zu ermitteln. Dieser Request wird grundsätzlich als Broadcast versendet. Da in manchen Strukturen ein potenzieller WLC aber nicht über Broadcast zu erreichen ist, können auch spezielle Adressen von weiteren WLCs in die Konfiguration der APs eingetragen werden.

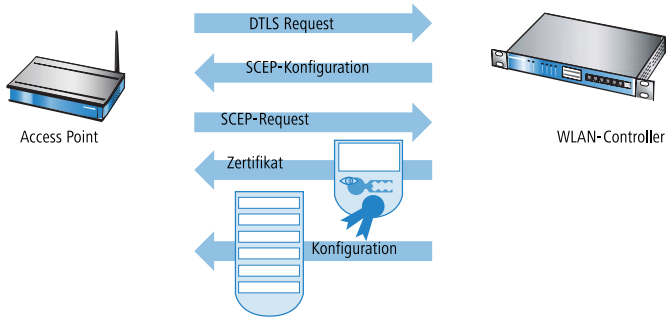
Hinweis: Außerdem können auch DNS-Namen von WLCs aufgelöst werden. Alle APs mit HiLCOS 7.22 oder höher haben den Standardnamen 'WLC-Address' bereits konfiguriert, sodass ein DNS-Server diesen Namen zu einem WLC auflösen kann. Gleiches gilt auch für die über DHCP gelernten DHCP-Suffixe. Somit können auch WLCs erreicht werden, die nicht im gleichen Netz stehen, ohne die APs konfigurieren zu müssen.

Aus den verfügbaren WLCs wählt der AP den besten aus und fragt bei diesem nach dem Aufbau der DTLS-Verbindung an. Der "beste" WLC ist für den AP derjenige mit der geringsten Auslastung, also dem kleinsten Verhältnis von gemanagten APs zu den maximal möglichen APs. Bei zwei oder mehreren gleich "guten" WLCs wählt der AP den im Netzwerk nächsten, also den mit der geringsten Antwortzeit.

Der WLC ermittelt daraufhin mit einer internen Zufallszahl einen eindeutigen und sicheren Sitzungsschlüssel, mit dem er die Verbindung zum AP schützt. Die CA im WLC stellt dem AP ein Zertifikat mittels SCEP aus. Das Zertifikat ist mit einem Kennwort für einmalige Verwendung als "Challenge" gesichert, der AP kann sich mit diesem Zertifikat gegenüber dem WLC für die Abholung des Zertifikats authentifizieren.

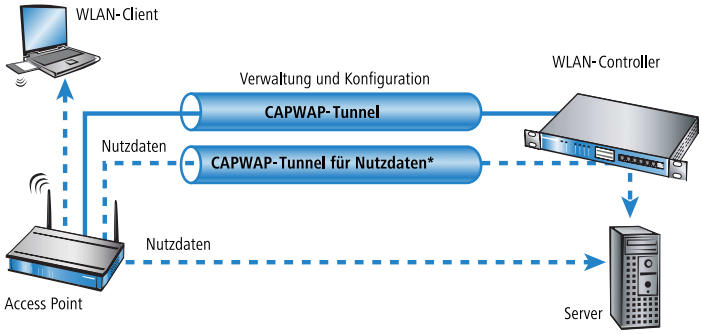
Über die gesicherte DTLS-Verbindung wird dem AP die Konfiguration für den integrierten SCEP-Client mitgeteilt – der AP kann dann über SCEP sein Zertifikat bei der SCEP-CA abholen. Anschließend wird die dem AP zugewiesene Konfiguration übertragen.

Hinweis: SCEP steht für Simple Certificate Encryption Protocol, CA für Certification Authority.



Sowohl Authentifizierung als auch Konfiguration können entweder automatisch vorgenommen werden oder nur bei passendem Eintrag der MAC-Adresse des AP in der AP-Tabelle des WLC. Sofern bei dem AP die WLAN-Module bei Beginn der DTLS-Kommunikation ausgeschaltet waren, werden diese nach erfolgreicher Übertragung von Zertifikat und Konfiguration eingeschaltet (sofern sie nicht in der Konfiguration explizit ausgeschaltet sind).

In der Folgezeit werden über den CAPWAP-Tunnel die Verwaltungs- und Konfigurationsdaten übertragen. Die Nutzdaten vom WLAN-Client werden im AP direkt in das LAN ausgekoppelt und z. B. an den Server übertragen.



13.2.4 Zero-Touch-Management

Mit der Möglichkeit, einem anfragenden AP ein Zertifikat und eine Konfiguration automatisch zuzuweisen, realisieren WLCs ein echtes "Zero-Touch-Management". Neue APs brauchen nur noch mit dem LAN verbunden werden; weitere Konfigurationsschritte sind erforderlich. Diese Reduzierung auf die reine Installation der Geräte entlastet die IT-Abteilungen gerade bei verteilten Strukturen, da in den entfernten Standorten kein spezielles IT- oder WLAN-Know-How zur Inbetriebnahme erforderlich ist.

13.2.5 Split-Management

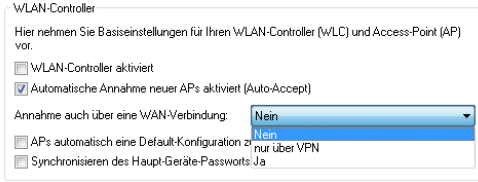
APs sind fähig, ihren WLC auch in entfernten Netzen zu suchen – eine einfache IP-Verbindung z. B. über eine VPN-Strecke reicht aus. Da die WLCs ausschließlich den WLAN-Teil der Konfiguration im AP beeinflussen, lassen sich alle anderen Funktionen separat verwalten. Durch diese Aufteilung der Konfigurationsaufgaben eignen sich WLCs ideal für den Aufbau einer firmen-

weiten WLAN-Infrastruktur in der Zentrale inklusive aller angeschlossenen Niederlassungen und Home-Offices.

13.2.6 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN

Der WLC oder behandelt CAPWAP-Anfragen aus dem LAN und dem WAN identisch. Bei von WAN-Gegenstellen stammenden Anfragen übernimmt er die APs in seine AP-Verwaltung und übergibt ggf. eine Default-Konfiguration. Entsprechend konfiguriert wird der CAPWAP-Dienst auf WAN-Gegenstellen nicht mehr angeboten, so dass keine Annahme von APs und Konfigurationsvergabe auf WAN-Gegenstellen mehr stattfindet.

Die Konfiguration erfolgt unter **WLAN-Controller** > **Allgemein** im Bereich **WLAN-Controller**. Ist die automatische Annahme neuer APs aktiviert, können Sie unter **Annahme auch über eine WAN-Verbindung** wählen, ob der CAPWAP-Dienst auch auf WAN-Gegenstellen angeboten wird.



Nein

Das Gerät nimmt keine neuen APs über die WAN-Verbindung an.

Nur über VPN

Das Gerät nimmt nur neue APs an, wenn die WAN-Verbindung über VPN erfolgt.

Ja

Das Gerät nimmt alle neuen APs über die WAN-Verbindung an.

13.3 Grundkonfiguration der WLAN Controller Funktion

Für den Start benötigt ein WLC zur weitestgehend automatisierten Konfiguration der APs die beiden folgenden Informationen:

- Eine aktuelle Zeitinformation (Datum und Uhrzeit), damit die Gültigkeit der benötigten Zertifikate sichergestellt werden kann.
- Ein WLAN-Profil, welches der WLC den APs zuweisen kann.

Weiterführende, optionale Konfigurationsbeispiele schließen das Einrichten von redundanten WLCs, das manuelle Trennen und Verbinden von APs sowie das Durchführen eines Backups der notwendigen Zertifikate ein.

Hinweis: Standardmäßig wartet der WLC auf Port 1027 (konfigurierbar) auf Verbindungen. Die Verteilung der Zertifikate erfolgt über SCEP, welches Port 80 (HTTP) nutzt.

13.3.1 Zeitinformation für den WLAN Controller einstellen

Die Verwaltung von APs in einer WLAN-Infrastruktur basiert auf der automatischen Verteilung von Zertifikaten über Simple Certificate Enrollment Protocol (SCEP).

Der WLC kann die Gültigkeit dieser zeitlich beschränkten Zertifikate nur dann prüfen, wenn er über eine aktuelle Zeitinformation verfügt. Solange der WLC nicht über eine aktuelle Zeitinformation verfügt, leuchtet die WLAN-LED dauerhaft rot, das Gerät ist nicht betriebsbereit.

Um dem Gerät eine Zeit zuzuweisen, klicken Sie in LANconfig mit der rechten Maustaste auf den Eintrag für den WLC und wählen im Kontext-Menü den Eintrag **Datum/Zeit setzen**. Alternativ klicken Sie in WEBconfig im Bereich **Extras** den Link **Datum und Uhrzeit einstellen**.

Hinweis:

Die WLCs können die aktuelle Zeit alternativ auch automatisch über das Network Time Protocol (NTP) von einem Zeit-Server beziehen. Informationen

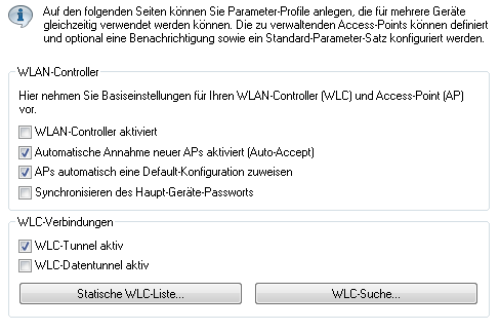
über NTP und die entsprechende Konfiguration finden Sie im HiLCOS-Referenzhandbuch.

Sobald der WLC über eine gültige Zeitinformation verfügt, beginnt die Erstellung der Zertifikate (Root- und Geräte-Zertifikat). Wenn die Zertifikate erfolgreich erzeugt wurden, meldet der WLC Betriebsbereitschaft, die WLAN-LED blinkt dann rot.

Hinweis: Nach Herstellung der Betriebsbereitschaft sollten Sie eine Sicherung der Zertifikate anlegen (*Sicherung der Zertifikate*)

13.3.2 Beispiel einer Default-Konfiguration

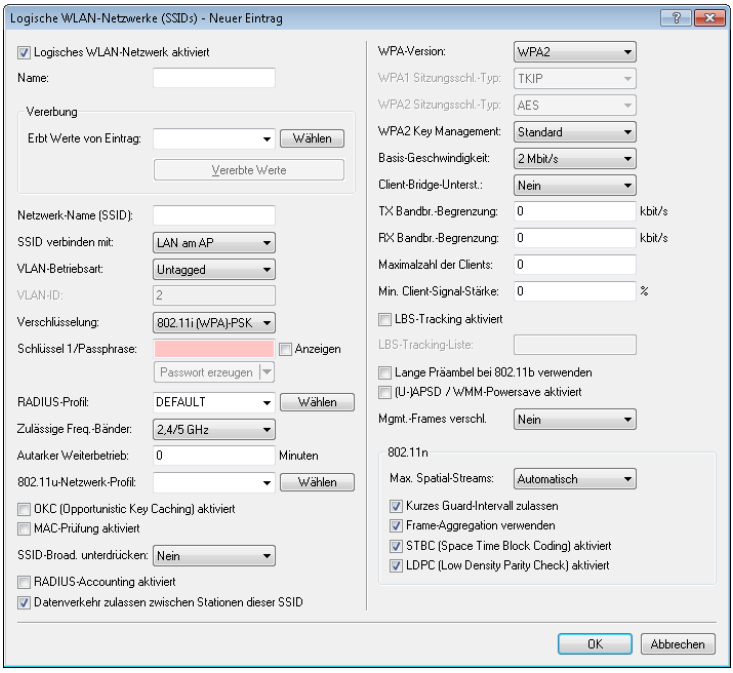
1. Öffnen Sie die Konfiguration des WLCs durch einen Doppelklick auf den entsprechenden Eintrag in LANconfig.
2. Aktivieren Sie unter **WLAN Controller** > **Allgemein** die Optionen für die automatische Annahme neuer APs sowie die Zuweisung einer Default-Konfiguration.



- **Automatische Annahme neuer APs aktiviert (Auto-Accept)**: Ermöglicht dem WLC, allen neuen APs ohne gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss entweder für den AP eine Konfiguration in der AP-Tabelle eingetragen sein oder die Automatische Zuweisung der Default-Konfiguration ist aktiviert.
- **APs automatisch eine Default-Konfiguration zuweisen** : Ermöglicht dem WLC, allen neuen APs eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde.

Durch die Kombination dieser beiden Optionen kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen, z. B. temporär während der Rollout-Phase einer WLAN-Installation.

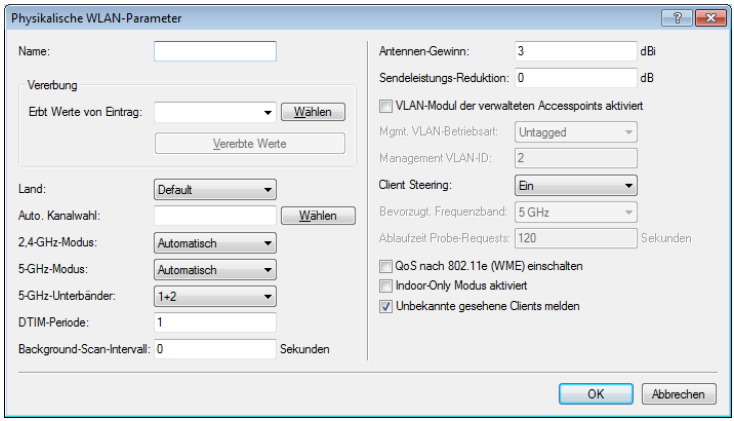
3. Wechseln Sie in der Ansicht **Profile** in die logischen WLAN-Netzwerke. Erstellen Sie einen neuen Eintrag mit folgenden Werten:



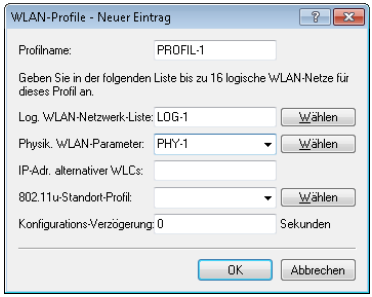
- **Netzwerkname**: Geben Sie dem WLAN einen Namen. Dieser Name wird nur für die Verwaltung im WLC verwendet.
- **SSID**: Mit dieser SSID verbinden sich die WLAN-Clients.
- **Verschlüsselung**: Wählen Sie die Verschlüsselung passend zu den Möglichkeiten der verwendeten WLAN-Clients und geben Sie ggf. einen Schlüssel bzw. eine Passphrase ein.
- Deaktivieren Sie die MAC-Prüfung. Hinweise zur Nutzung der MAC-Filterlisten in gemanagten WLAN-Strukturen finden Sie unter *Prüfung der WLAN-Clients über RADIUS (MAC-Filter)*.

4. Erstellen Sie auch bei den physikalischen WLAN-Parametern einen neuen Eintrag. Für die Default-Konfiguration reicht hier in vielen Fällen nur die Angabe eines Namens. Die restlichen Einstellungen können bei Bedarf angepasst werden.

   Hinweis: In normalen AP-Anwendungen sollten Sie nur die 5-GHz-Unterbänder 1 und 2 verwenden. Das Unterband 3 steht nur für besondere Anwendungen zur Verfügung (z. B. BFWA – Broadband Fixed Wireless Access).



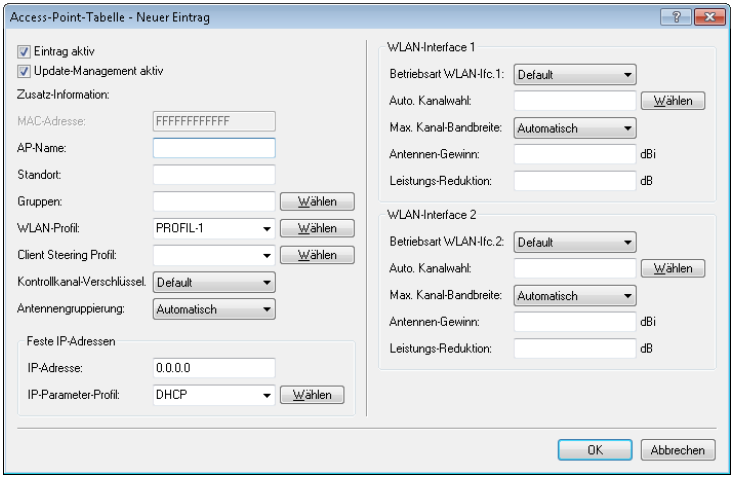
5. Erstellen Sie ein neues WLAN-Profil, geben Sie ihm einen eindeutigen Namen und weisen Sie ihm das eben erstellte logische WLAN-Netzwerk sowie die physikalischen WLAN-Parameter zu.



6. Wechseln Sie auf in Ansicht **AP-Konfiguration**, öffnen Sie die **Access-Point-Tabelle** und erstellen Sie einen neuen Eintrag mit einem Klick auf

die Schaltfläche **Default**. Weisen Sie dabei dem Eintrag das eben erstellte WLAN-Profil zu, **AP-Name** und **Standort** sollten frei bleiben.

Hinweis: Die **MAC-Adresse** wird für die Default-Konfiguration auf 'ffffffffffff' gesetzt und ist nicht editierbar. Damit gilt dieser Eintrag als Standard für alle APs, die nicht mit ihrer MAC-Adresse explizit in dieser Tabelle eingetragen sind.

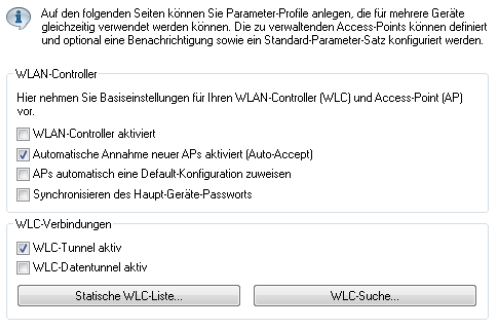


13.3.3 Zuweisung der Default-Konfiguration zu den neuen Access Points

Mit diesen Einstellungen haben Sie alle erforderlichen Werte definiert, damit der WLC den APs die erforderlichen WLAN-Parameter zuweisen kann. Mit dieser Konfigurations-Zuweisung ändern die APs in der Verwaltung des WLCs ihren Status von "Neuer Access Point" auf "Erwarteter Access Point", die im Display des Gerätes unter **Exp. APs** aufgeführt werden. Sobald allen neuen APs die Default-Konfiguration zugewiesen wurde, erlischt die New-APs-LED.

Hinweis: Nach der ersten Startphase kann die Option **Automatische Zuweisung der Default-Konfiguration** wieder deaktiviert werden, damit keine weiteren APs automatisch in das Netzwerk aufgenommen werden. Die **Automatische Annahme neuer APs** kann aktiviert bleiben, damit der WLC

den erwarteten APs – die in der AP-Tabelle eingetragen sind – z. B. nach einem Reset automatisch wieder ein gültiges Zertifikat zuweisen kann.

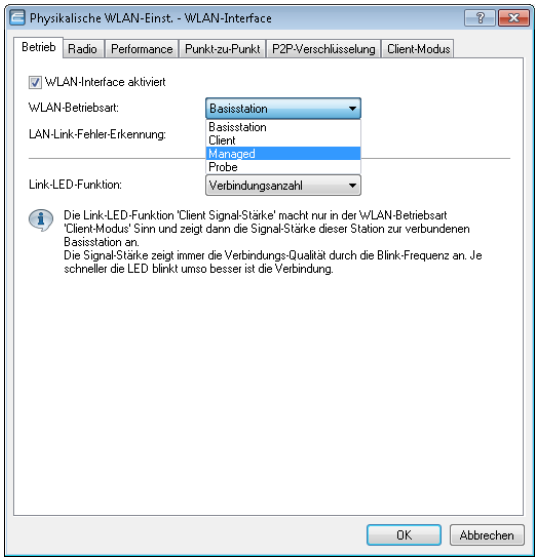


13.3.4 Konfiguration der Access Points

- Bei APs sind im Auslieferungszustand die WLAN-Module auf die Betriebsart 'Managed' eingestellt. In diesem Modus suchen die APs nach einem zentralen WLC, der ihnen eine Konfiguration zuweisen kann, und bleiben so lange im "Such-Modus", bis sie einen passenden WLC gefunden haben oder die Betriebsart für die WLAN-Module manuell geändert wird.

Hinweis: Die Betriebsart kann für jedes WLAN-Modul separat eingestellt werden. Bei Modellen mit zwei WLAN-Modulen kann so ein Modul mit einer lokalen Konfiguration arbeiten, das zweite kann zentral über den WLC verwaltet werden.

Für einzelne Geräte finden Sie die Betriebsart der WLAN-Module in LANconfig über **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einstellungen** > **Betrieb**:



Wenn Sie die Betriebsart für mehrere Geräte gleichzeitig umstellen möchten, können Sie auf die Geräte ein einfaches Script anwenden mit folgenden Zeilen:

```
# Script
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

13.4 Konfiguration

Die meisten Parameter zur Konfiguration der WLAN Controller entsprechen denen der Access Points. In diesem Abschnitt werden daher nicht alle WLAN-Parameter explizit beschrieben sondern nur die für den Betrieb der WLAN-Controller erforderlichen Aspekte.

13.4.1 Allgemeine Einstellungen

In diesem Bereich nehmen Sie die Basiseinstellungen für Ihren WLC vor.

- Automatische Annahme neuer APs (Auto-Accept)

  Ermöglicht dem WLC, allen neuen APs eine Konfiguration zuzuweisen, auch wenn diese nicht über ein gültiges Zertifikat verfügen.

  Ermöglicht dem WLC, allen neuen APs **ohne** gültiges Zertifikat ein solches Zertifikat zuzuweisen. Dazu muss eine der beiden Bedingungen erfüllt sein:

  - Für den AP ist unter seiner MAC-Adresse eine Konfiguration in der AP-Tabelle eingetragen.
  - Die Option 'Automatische Zuweisung der Default-Konfiguration' ist aktiviert.

- Automatische Zuweisung der Default-Konfiguration

  Ermöglicht dem WLC, allen neuen APs (also **ohne** gültiges Zertifikat) eine Default-Konfiguration zuzuweisen, auch wenn für diese keine explizite Konfiguration hinterlegt wurde. Im Zusammenspiel mit dem Auto-Accept kann der WLC alle im LAN gefundenen APs im Managed-Modus automatisch in die von ihm verwaltete WLAN-Struktur aufnehmen (bis zur maximalen Anzahl der auf einem WLC verwalteten APs). Per Default aufgenommene APs werden auch in die MAC-Liste aufgenommen.

  Hinweis: Mit dieser Option können möglicherweise auch unbeabsichtigte APs in die WLAN-Struktur aufgenommen werden. Daher sollte diese Option nur während der Startphase bei der Einrichtung einer zentral verwalteten WLAN-Struktur aktiviert werden

Mit der Kombination der Einstellungen für Auto-Accept und Default-Konfiguration können Sie verschiedene Situationen für die Einrichtung und den Betrieb der APs abdecken:

Auto-Accept	*Default-Konfiguration*	*Geeignet für*
Ein	Ein	Rollout-Phase: Verwenden Sie diese Kombination nur dann, wenn **keine APs unkontrolliert** mit dem LAN verbunden werden können und so unbeabsichtigt in die WLAN-Struktur aufgenommen werden.

Auto-Accept	*Default-Konfiguration*	*Geeignet für*
Ein	Aus	Kontrollierte Rollout-Phase: Verwenden Sie diese Kombination, wenn Sie alle erlaubten APs mit ihrer MAC-Adresse in die AP-Tabelle eingetragen haben und diese automatisch in die WLAN-Struktur aufgenommen werden sollen.
Aus	Aus	Normalbetrieb: Es werden keine neuen APs ohne Zustimmung der Administratoren in die WLAN-Struktur aufgenommen.

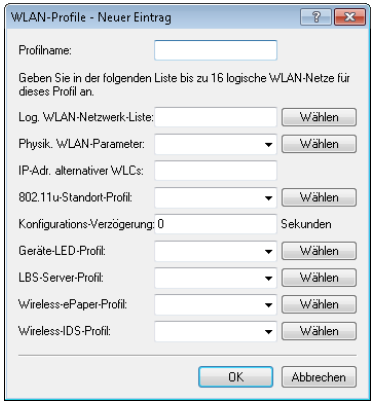
13.4.2 Profile

Im Bereich der Profile definieren Sie die logischen WLAN-Netzwerke, die physikalischen WLAN-Parameter sowie die WLAN-Profile, die eine Kombination aus den beiden vorgenannten Elementen darstellen.

WLAN-Profile

In den WLAN-Profilen werden die Einstellungen zusammengefasst, die den APs zugewiesen werden. Die Zuordnung der WLAN-Profile zu den APs erfolgt in der AP-Tabelle.

Für jedes WLAN-Profil können Sie unter **WLAN-Controller** > **Profile** > **WLAN-Profile** die folgenden Parameter definieren:



Profil-Name

Name des Profils, unter dem die Einstellungen gespeichert werden.

Log. WLAN-Netzwerk-Liste

Liste der logischen WLAN-Netzwerke, die über dieses Profil zugewiesen werden.

Hinweis: Die APs nutzen aus dieser Liste nur die ersten 816 Einträge, die mit der eigenen Hardware kompatibel sind. Somit können in einem Profil z. B. jeweils 816 WLAN-Netzwerke für reinen 2,4 GHz-Betrieb und 816 für reinen 5 GHz-Betrieb definiert werden. Für jeden AP – sowohl Modelle mit 2,4 GHz- als auch die mit 5 GHz-Unterstützung – stehen damit die maximal möglichen 816 logischen WLAN-Netzwerke zur Verfügung.

Physik. WLAN-Parameter

Ein Satz von physikalischen Parametern, mit denen die WLAN-Module der APs arbeiten sollen.

IP-Adr. alternativer WLCs

Liste der WLCs, bei denen der AP eine Verbindung versuchen soll. Der AP leitet die Suche nach einem WLC über einen Broadcast ein. Wenn nicht alle WLCs über einen solchen Broadcast erreicht werden können (WLC steht z. B. in einem anderen Netz), dann ist die Angabe von alternativen WLCs sinnvoll.

802.11u-Standort-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

Konfigurations-Verzögerung

Geben Sie hier die Verzögerung an, nach der ein vom WLAN-Controller gemanagter AP die übertragene Konfiguration übernimmt.

Dies ist insbesondere in AutoWDS-Szenarien sinnvoll, in denen mehrere gemanagte APs über Punkt-zu-Punkt-Strecken hintereinander verbunden sind. Durch eine vorzeitige Konfigurations-Änderung auf einem AP, welcher die Verbindung zu einem entfernteren AP herstellt, könnte sonst die Verbindung zu dem entfernteren AP abgeschnitten werden.

Eine grobe Regel für die Berechnung der Verzögerung ist (unabhängig von der Topologie): Eine Sekunde pro gemanagtem AP, also z. B. 200 Sekunden bei 200 APs.

Hinweis: Die Verzögerung gilt nicht für übertragene Skripte.

Geräte-LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Geräte-LED-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile**.

LBS-Allgemein-Profil

Wählen Sie hier aus der Liste der allgemeinen LBS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die allgemeinen LBS-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Erweiterte Profile** mit der Schaltfläche **LBS - Allgemein**.

Wireless-ePaper-Profil

Wählen Sie hier aus der Liste der Wireless-ePaper-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-ePaper-Profile verwalten Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** mit der Schaltfläche **Wireless-ePaper-Profile**.

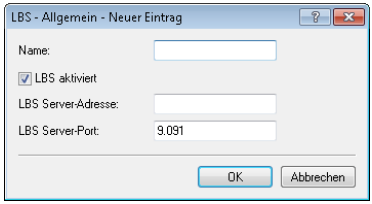
Wireless-IDS-Profil

Wählen Sie hier aus der Liste der Wireless-IDS-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Wireless-IDS-Profile verwalten Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** mit der Schaltfläche **Wireless-IDS-Profile**.

Allgemeines LBS-Profil und Gerätestandort-Profil

Um die Einstellungen von Location Based Services-Servern (LBS-Servern) und AP-Standorten komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **Profile** mit der Schaltfläche **Erweiterte Profile** das entsprechende Profil für den LBS-Server.

Mit der Schaltfläche **LBS - Server** erstellen Sie ein allgemeines LBS-Server-Profil.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

LBS aktiviert

Aktivieren oder deaktivieren Sie LBS.

LBS Server-Adresse

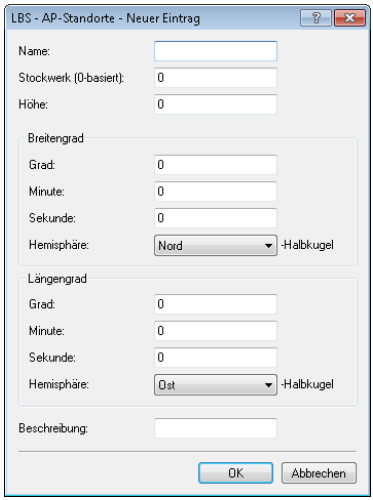
Geben Sie hier die Adresse des LBS-Servers ein.

LBS Server-Port

Geben Sie hier den Port des LBS-Servers ein (Default: 9091).

Sie erstellen das entsprechende Profil für Standorte der LBS APs über **WLAN Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen**.

Mit der Schaltfläche **LBS-AP-Standorte** erstellen Sie ein Standort-Profil der LBS-APs.



Name

Vergeben Sie einen aussagekräftigen Namen für das Profil.

Stockwerk (0-basiert)

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

Höhe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Grad (Breitengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Breitengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Breitengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Breitengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Breite (Latitude) sind folgende Werte möglich:

- Nord: nördliche Breite
- Süd: südliche Breite

Grad (Längengrad)

Dieses Feld gibt den Winkel in Grad des geographischen Koordinatensystems an.

Minute (Längengrad)

Dieses Feld gibt die Minute des geographischen Koordinatensystems an.

Sekunde (Längengrad)

Dieses Feld gibt die Sekunde des geographischen Koordinatensystems an.

Hemisphäre (Längengrad)

Dieses Feld gibt die Orientierung des geographischen Koordinatensystems an. Für die geographische Länge (Longitude) sind folgende Werte möglich:

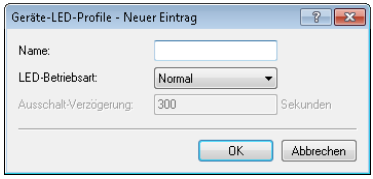
- Ost: östliche Länge
- West: westliche Länge

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

Geräte-LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile** entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.



Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

LED-Betriebsart

Die folgenden Optionen stehen zur Auswahl:

- **Normal**: Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.
- **Verzögert aus**: Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustartes auf kritische Fehler hinweisen.
- **Alle aus**: Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

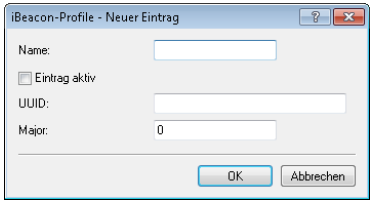
Ausschalt-Verzögerung

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

ESL- und iBeacon-Profile

Um die Einstellungen von Wireless-ePaper-Informationen und iBeacon-Informationen der einzelnen APs komfortabel über einen WLC zu verwalten, erstellen Sie über **WLAN-Controller** > **AP-Konfiguration** mit der Schaltfläche **Erweiterte Einstellungen** die entsprechenden Profile für Wireless-ePapaper und iBeacon.

Mit der Schaltfläche **iBeacon-Profile** erstellen Sie iBeacon-Profile für die Zuweisungsgruppen und die AP-Tabelle, die festlegen, welche iBeacon-Informationen die einzelnen APs ausstrahlen.



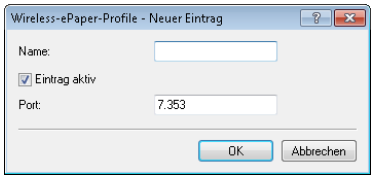
Name
Name des Profils

Eintrag aktiv
Aktiviert oder deaktiviert dieses Profil.

UUID
Eindeutige Kennzeichnung des Senders

Major
Gibt den Major-Wert des iBeacons an.

Mit der Schaltfläche **Wireless-ePaper-Profile** erstellen Sie Wireless-ePaper-Profile für die WLAN-Profile-Tabelle, die festlegen, welche Wireless-ePaper-Informationen die einzelnen APs ausstrahlen.



Name
Name des Profils

Eintrag aktiv
Aktiviert oder deaktiviert dieses Profil.

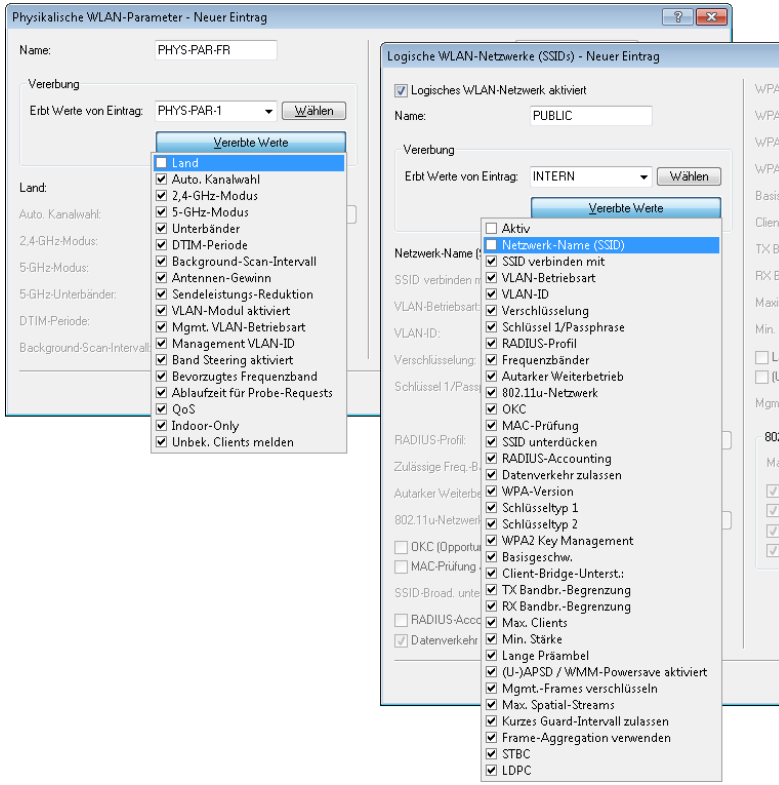
Port
Gibt den Port an.

Vererbung von Parametern

Mit einem WLC können sehr viele unterschiedliche APs an verschiedenen Standorten verwaltet werden. Nicht alle Einstellungen in einem WLAN-Profil eignen sich dabei für jeden der verwalteten APs gleichermaßen. Unterschiede gibt es z. B. in den Ländereinstellungen oder bei den Geräteeigenschaften.

Damit auch in komplexen Anwendungen die WLAN-Parameter nicht in mehreren Profilen redundant je nach Land oder Gerätetyp gepflegt werden müssen, können die logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter ausgewählte Eigenschaften von anderen Einträgen "erben".

1. Erstellen Sie dazu zunächst die grundlegenden Einstellungen, die für die meisten verwalteten APs gültig sind.
2. Erzeugen Sie danach Einträge für die spezifischeren Werte, z. B. physikalische Einstellungen für ein bestimmtes Land oder ein logisches WLAN-Netzwerk für den öffentlichen Zugang von mobilen Clients.



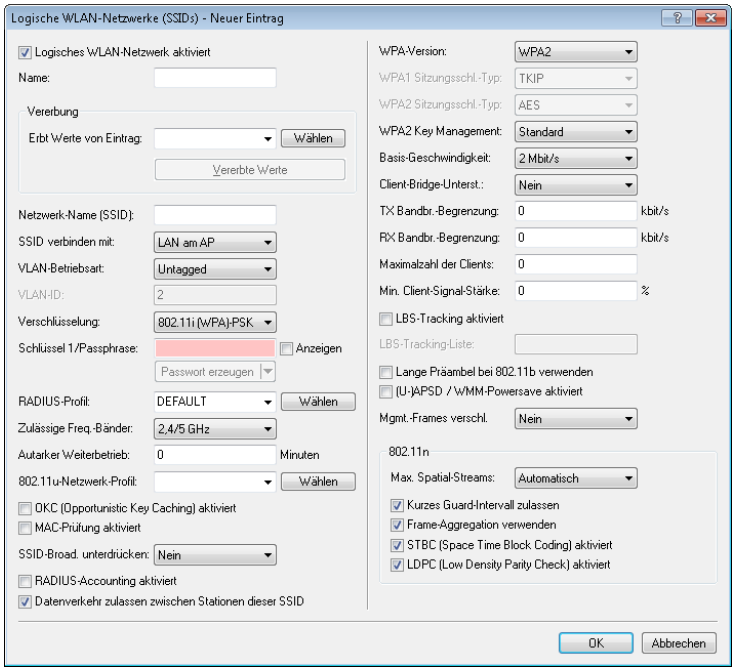
3. Wählen Sie aus, von welchem Eintrag Werte geerbt werden sollen und markieren Sie die vererbten Werte. Die so übernommenen Parameter werden im Konfigurationsdialog grau dargestellt und können nicht verändert werden.
4. Die so zusammengestellten WLAN-Einstellungen werden dann je nach Verwendung zu separaten Profilen zusammengefasst, die wiederum gezielt den jeweiligen Access Points zugewiesen werden.

Hinweis: Bei der Vererbung sind grundsätzlich Ketten über mehrere Stufen (Kaskadierung) möglich. So können z. B. länder- und gerätespezifische Parameter komfortabel zusammengestellt werden.

Auch Rekursionen sind möglich – Profil A erbt von Profil B, gleichzeitig erbt B aber auch von A. Die verfügbaren Parameter für die Vererbung beschränken sich dabei aber auf eine "Vererbungsrichtung" pro Parameter.

Logische WLAN-Netzwerke

Unter **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke** können Sie die Parameter für die logischen WLAN-Netzwerke einstellen, die der WLC den APs zuweisen soll. Für jedes logische WLAN-Netzwerk können Sie die folgenden Parameter definieren:



Logisches WLAN-Netzwerk aktiviert

Aktivieren Sie das logische WLAN-Netzwerk, indem Sie diese Option anklicken.

Name

Geben Sie hier einen Namen an, der das logische WLAN-Netzwerk eindeutig kennzeichnet.

Vererbung

Möchten Sie Einträge erzeugen, die sich nur in wenigen Werten von vorhandenen Einträgen unterscheiden, können Sie einen "Eltern"-Eintrag sowie die zu übernehmenden Einträge hier gezielt auswählen.

Hinweis: Auch ein "Eltern"-Eintrag kann selber geerbte Einträge enthalten. Achten Sie darauf, dass die Konstruktionen für geerbte Einträge nicht zu komplex und damit schwer nachvollziehbar und konfigurierbar sind.

Netzwerk-Name (SSID)

Geben Sie hier die SSID des WLAN-Netzwerkes an. Alle Stationen, die zu diesem WLAN-Netz gehören, müssen dieselbe SSID verwenden.

SSID verbinden mit

Wählen Sie hier aus, mit welcher logischen Schnittstelle des APs die SSID verknüpft sein soll bzw. wohin der AP Datenpakete dieser SSID leiten soll.

- "LAN": Der AP lädt die Datenpakete standardmäßig lokal ins LAN weiter (LAN-1). Dazu muss er entsprechend konfiguriert sein.
- "WLC-Tunnel-x": Die SSID ist mit einem WLC-Bridge-Layer-3-Tunnel verbunden. Bitte beachten Sie, dass maximal 7 WLC-Bridge-Layer-3-Tunnel unterstützt werden. Der AP liefert alle Datenpakete in diesen Tunnel und damit zum WLC. Dieser Tunnel muss auf dem WLC konfiguriert sein.

Hinweis: Beachten Sie, dass Sie bei Weiterleitung aller Datenpakete zum WLC zwar zentrale Routen und Filter definieren können, dieses jedoch eine hohe Last auf dem WLC erzeugt. Dafür müssen dort entsprechend hohe Bandbreiten zur Verfügung stehen, um den gesamten Datenverkehr dieser und ggf. weiterer über WLC-Tunnel mit diesem WLC verbundenen SSIDs übertragen zu können.

VLAN-Betriebsart

Stellen Sie hier die VLAN-Betriebsart des APs für Pakete dieses WLAN-Netzwerkes (SSID) ein. Die Verwendung von VLAN-IDs ist abhängig davon, ob das VLAN-Modul in den physikalischen WLAN-Parametern des APs aktiviert ist. Ansonsten ignoriert der AP alle VLAN-Einstellungen in den logischen Netzwerken. Es ist möglich, das Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben:

- "Untagged": Der AP markiert Datenpakete dieser SSID nicht mit einer VLAN-ID.

  Hinweis: Es ist möglich ein WLAN-Netzwerk trotz aktiviertem VLAN auch ungetagged zu betreiben. Intern ist dafür die VLAN-ID "1" reserviert.

- "Tagged": Der AP markiert die Datenpakete mit der nachfolgend bestimmten VLAN-ID.

VLAN-ID

VLAN-ID für dieses logische WLAN-Netzwerk.

Hinweis: Bitte beachten Sie, dass für die Nutzung der VLAN-IDs in einem logischen WLAN-Netzwerk die Einstellung einer Management-VLAN-ID erforderlich ist (siehe Physikalische WLAN Parameter)!

Verschlüsselung

Bestimmen Sie hier das Verschlüsselungsverfahren bzw. bei WEP die Schlüssellänge für die Verschlüsselung von Datenpaketen in diesem WLAN.

Schlüssel 1/Passphrase

Sie können die Schlüssel oder Passphrasen als ASCII-Zeichenkette eingeben. Bei WEP ist alternativ die Eingabe einer Hexadezimalzahl durch ein vorangestelltes "0x" möglich. Folgende Zeichenkettenlängen ergeben sich für die verwendeten Formate:

- WPA-PSK: 8 bis 63 ASCII-Zeichen
- WEP128 (104 Bit): 13 ASCII- oder 26 Hexadezimal-Zeichen

- WEP64 (40 Bit): 5 ASCII- oder 10 Hexadezimal-Zeichen

RADIUS-Profil

Geben Sie an, welches RADIUS-Profil der AP für dieses Netzwerk erhalten soll, damit dieser bei Bedarf eine direkte Verbindung zum RADIUS-Server aufbauen kann. Lassen Sie dieses Feld leer, wenn der WLC RADIUS-Anfragen abwickeln soll.

Hinweis: Die RADIUS-Profile müssen Sie in der entsprechenden Tabelle konfigurieren.

Zulässige Freq.-Bänder

Bestimmen Sie das Frequenzband, das die Netzwerkteilnehmer zur Übertragung von Daten im WLAN verwenden sollen. Sie können sowohl das 2,4 GHz-Band, das 5 GHz-Band als auch beide Bänder auswählen.

Autarker Weiterbetrieb

Zeit in Minuten, für die der AP im Managed-Modus mit seiner aktuellen Konfiguration weiterarbeitet.

Der WLC weist dem AP die Konfiguration zu, der sie optional im Flash gespeichert (in einem Bereich, der nicht mit LANconfig oder anderen Tools auszulesen ist). Falls die Verbindung zum WLC abbricht, arbeitet der AP für die hier eingestellte Zeit mit seiner Konfiguration aus dem Flash weiter. Auch nach einem eigenen Stromausfall kann der AP mit der Konfiguration aus dem Flash weiterarbeiten.

Wenn die eingestellte Zeit abgelaufen ist, bevor die Verbindung zum WLC wiederhergestellt ist, löscht der AP die Konfiguration im Flash – der AP stellt seinen Betrieb ein. Sobald der WLC wieder erreichbar ist, überträgt der WLC die Konfiguration erneut zum AP.

Diese Maßnahme stellt einen wirksamen Schutz gegen Diebstahl dar, da der AP die sicherheitsrelevanten Parameter der Konfiguration nach Ablauf der eingestellten Zeit automatisch löscht.

Hinweis: Stellt der AP im Backup-Fall eine Verbindung zu einem sekundären WLC her, so unterbricht der AP den Count-Down für den autarken Weiterbetrieb. Der AP bleibt also mit seinen WLAN-Netzwerken

auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLC hat.

Hinweis: Bitte beachten Sie, dass der AP die Konfigurationsdaten im Flash erst nach Ablauf der eingestellten Zeit für den autarken Weiterbetrieb löscht, nicht jedoch durch die Trennung vom Stromnetz!

802.11u-Netzwerk-Profil

Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus.

OKC aktiviert

Mit dieser Option aktivieren Sie das opportunistische Schlüssel-Caching (Opportunistic Key Caching). Das OKC ermöglicht es WLAN-Clients, schnell und komfortabel in WLAN-Umgebungen mit WPA2-Enterprise-Verschlüsselung zwischen WLAN-Zellen zu wechseln (Roaming).

MAC-Prüfung aktiviert

In der MAC-Filterliste (**Wireless-LAN** > **Stationen** > **Stationen**) sind die MAC-Adressen der Clients hinterlegt, die sich bei einem AP einbuchen dürfen. Mit dem Schalter **MAC-Filter aktiviert** können Sie die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausschalten.

SSID-Broad. unterdrücken

Sie können Ihr Funk-LAN entweder in einem öffentlichen oder in einem privaten Modus betreiben. Ein Funk-LAN im öffentlichen Modus kann von Mobilstationen in der Umgebung ohne weiteres kontaktiert werden. Durch Aktivieren der Closed-Network-Funktion versetzen Sie Ihr Funk-LAN in einen privaten Modus. In dieser Betriebsart sind Mobilstationen ohne Kenntnis des Netzwerknamens (SSID) von der Teilnahme am Funk-LAN ausgeschlossen.

Schalten Sie den "Closed-Network-Modus" ein, wenn Sie verhindern möchten, dass sich WLAN-Clients mit der SSID "Any" oder einer leeren SSID in Ihrem Funknetzwerk anmelden.

Die Option **SSID-Broadcast unterdrücken** ermöglicht folgende Einstellungen:

- **Nein**: Der AP veröffentlicht die SSID der Funkzelle. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP mit der SSID der Funkzelle (öffentliches WLAN).
- **Ja**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer SSID, antwortet der AP ebenfalls mit einer leeren SSID.
- **Verschärft**: Der AP veröffentlicht die SSID der Funkzelle nicht. Sendet ein Client einen Probe Request mit leerer oder falscher SSID, antwortet der AP überhaupt nicht.

Hinweis: Das einfache Unterdrücken der SSID bietet keinen ausreichenden Zugriffsschutz, da der AP diese bei der Anmeldung berechtigter WLAN-Clients im Klartext überträgt und sie somit für alle im WLAN-Netz befindlichen WLAN-Clients kurzfristig sichtbar ist.

RADIUS-Accounting aktiviert

Aktivieren Sie diese Option, wenn Sie das RADIUS-Accounting in diesem logischen WLAN-Netzwerkm aktivieren wollen.

Datenverkehr zulassen zwischen Stationen dieser SSID

Aktivieren Sie diese Option, wenn alle Stationen, die an dieser SSID angemeldet sind, untereinander kommunizieren dürfen.

WPA-Version

Wählen Sie hier die WPA-Version aus, die der AP den WLAN-Clients zur Verschlüsselung anbieten soll.

- WPA1: Nur WPA1
- WPA2: Nur WPA2
- WPA1/2: Sowohl WPA1 als auch WPA2 in einer SSID (Funkzelle)

WPA1 Sitzungsschl.-Typ

Wenn Sie als Verschlüsselungsmethode "802.11i (WPA)-PSK" nutzen, können Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA1 auswählen:

- AES: Der AP verwendet das AES-Verfahren.
- TKIP: Der AP verwendet das TKIP-Verfahren.

- AES/TKIP: Der AP verwendet das AES-Verfahren. Falls die Client-Hardware das AES-Verfahren nicht unterstützt, wechselt der AP zum TKIP-Verfahren.

WPA2 Sitzungsschl.-Typ

Wählen Sie hier das Verfahren zur Generierung des Sitzungs- bzw. Gruppenschlüssels für WPA2 aus.

Basis-Geschwindigkeit

Die eingestellte Basis-Geschwindigkeit sollte es auch unter ungünstigen Bedingungen erlauben, die langsamsten Clients im WLAN zu erreichen. Stellen Sie hier nur dann eine höhere Geschwindigkeit ein, wenn alle Clients in diesem logischen WLAN auch "schneller" zu erreichen sind. Bei automatischer Festlegung der Übertragungsrate sammelt der AP die Informationen über die Übertragungsraten der einzelnen WLAN-Clients. Die Rate teilen die Clients dem AP automatisch bei jeder Unicast-Kommunikation mit. Aus der Liste der angemeldeten Clients wählt der AP nun ständig die jeweils niedrigste Übertragungsrate aus und überträgt damit die Multicast- und Broadcast-Sendungen.

Client-Bridge-Unterst.

Aktivieren Sie diese Option für einen AP, wenn Sie im WLAN-Client-Modus für eine Client-Station die Client-Bridge-Unterstützung aktiviert haben.

Hinweis: Der Client-Bridge-Modus ist ausschließlich zwischen zwei Hirschmann-Geräten verwendbar.

TX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Senderichtung für die betreffende SSID. Der Wert `0` deaktiviert die Begrenzung.

RX Bandbr.-Begrenzung

Über diese Einstellung definieren Sie die zur Verfügung stehende Gesamtbandbreite in Empfangsrichtung für die betreffende SSID. Der Wert `0` deaktiviert die Begrenzung.

Maximalzahl der Clients

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem AP einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, lehnt der AP ab.

Min. Client-Signal-Stärke

Mit diesem Eintrag bestimmen Sie den Schwellwert in Prozent für die minimale Signalstärke für Clients beim Einbuchen. Unterschreitet ein Client diesen Wert, sendet der AP keine Probe-Responses mehr an diesen Client und verwirft die entsprechenden Anfragen.

Ein Client mit schlechter Signalstärke findet den AP somit nicht und kann sich nicht darauf einbuchen. Das sorgt beim Client für eine optimierte Liste an verfügbaren APs, da keine APs aufgeführt werden, mit denen der Client an der aktuellen Position nur eine schwache Verbindung aufbauen könnte.

LBS-Tracking aktiviert

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Hinweis: Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public Spot-Modul bestimmen Sie, ob der LBS-Server die am Public Spot angemeldeten Benutzer tracken darf.

LBS-Tracking-Liste

Mit diesem Eintrag legen Sie den Listennamen für das LBS-Tracking fest. Bei einem erfolgreichen Einbuchen eines Clients in diese SSID überträgt der AP den angegebenen Listennamen, die MAC-Adresse des Clients und die eigene MAC-Adresse an den LBS-Server.

Lange Präambel bei 802.11b verwenden

Normalerweise handeln die Clients im 802.11b-Modus die Länge der zu verwendenden Präambel mit dem AP selbst aus. Stellen Sie hier die "lange Präambel" nur dann fest ein, wenn die Clients diese feste Einstellung verlangen.

(U-)APSD / WMM-Powersave aktiviert

Aktivieren Sie diese Option, um Stationen die Unterstützung für den Stromsparmechanismus (U-)APSD ([Unscheduled] Automatic Power Save Delivery) zu signalisieren.

(U-)APSD ist im Standard 802.11e verankert und hilft VoWLAN-Geräten dabei, ihre Akkulaufzeit zu erhöhen. Die betreffenden Geräte schalten dafür nach der Anmeldung an einem (U-)APSD-fähigen AP in den Energiesparmodus um. Erhält der AP nun Datenpakete für das betreffende Gerät, speichert es die Daten kurz zwischen und wartet, bis das VoWLAN-Gerät wieder verfügbar ist. Erst dann leitet er die Daten weiter. (U-)APSD erhöht demnach die Latenzzeit des Funkmoduls, wodurch es letztlich weniger Strom verbraucht. Die einzelnen Ruhezeiten können dabei so kurz ausfallen, dass ein VoWLAN-Gerät selbst im Gesprächszustand noch den Stromsparmechanismus benutzen kann. Die betreffenden Geräte müssen (U-)APSD allerdings ebenfalls unterstützen.

Bei WWM (Wi-Fi Multimedia) Power Save handelt es sich um einen Stromsparmechanismus der Wi-Fi Alliance, welcher auf U-APSD basiert.

Max. Spatial-Streams

Mit der Funktion des Spatial-Multiplexing kann der AP mehrere separate Datenströme über separate Antennen übertragen, um so den Datendurchsatz zu verbessern. Der Einsatz dieser Funktion ist nur dann zu empfehlen, wenn die Gegenstelle die Datenströme mit entsprechenden Antennen verarbeiten kann.

Hinweis: In der Einstellung 'Automatisch' nutzt der AP alle Spatial-Streams, die das jeweilige WLAN-Modul unterstützt.

Kurzes Guard-Intervall zulassen

Dieser Option reduziert die Sendepause zwischen zwei Signalen von 0,8 µs (Standard) auf 0,4 µs (Short Guard Interval). Dadurch steigt die effektiv für die Datenübertragung genutzte Zeit und damit der Datendurchsatz. Auf der anderen Seite ist das WLAN-System damit anfälliger für Störungen, welche durch die Interferenzen zwischen zwei aufeinanderfolgenden Signalen auftreten können.

Im Automatik-Modus wird das kurze Guard-Intervall aktiviert, sofern die jeweilige Gegenstelle diese Betriebsart unterstützt. Alternativ kann die Nutzung des kurzen Guard-Intervalls auch ausgeschaltet werden.

Frame-Aggregation verwenden

Bei der Frame-Aggregation werden mehrere Datenpakete (Frames) zu einem größeren Paket zusammengefasst und gemeinsam versendet. Dieses Verfahren reduziert den Overhead der Pakete, der Datendurchsatz steigt.

Die Frame-Aggregation eignet sich weniger gut bei schnell bewegten Empfängern oder für zeitkritische Datenübertragungen wie Voice over IP.

STBC (Space Time Block Coding) aktiviert

Aktivieren Sie hier das Space Time Block Coding.

Die Funktion 'STBC' variiert den Versand von Datenpaketen zusätzlich über die Zeit, um auch zeitliche Einflüsse auf die Daten zu minimieren. Durch den zeitlichen Versatz der Sendungen besteht für den Empfänger eine noch bessere Chance, fehlerfreie Datenpakete zu erhalten, unabhängig von der Anzahl der Antennen.

LDPC (Low Density Parity Check) aktiviert

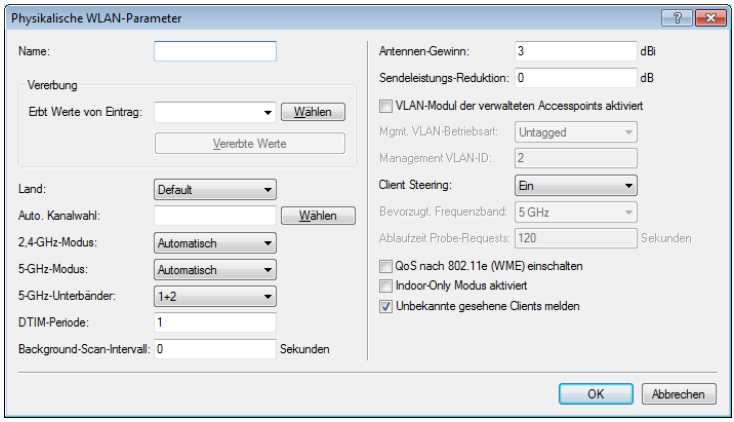
Aktivieren Sie hier den Low Density Parity Check.

Bevor der Sender die Datenpakete abschickt, erweitert er den Datenstrom abhängig von der Modulationsrate um Checksummen-Bits, um dem Empfänger damit die Korrektur von Übertragungsfehlern zu ermöglichen. Standardmäßig nutzt der Übertragungsstandard IEEE 802.11n das bereits aus den Standards 802.11a und 802.11g bekannte 'Convolution Coding' (CC) zur Fehlerkorrektur, ermöglicht jedoch auch eine Fehlerkorrektur nach der LDPC-Methode (Low Density Parity Check).

Im Unterschied zur CC-Kodierung nutzt die LDPC-Kodierung größere Datenpakete zur Checksummenberechnung und kann zusätzlich mehr Bit-Fehler erkennen. Die LDPC-Kodierung ermöglicht also bereits durch ein besseres Verhältnis von Nutz- zu Checksummen-Daten eine höhere Datenübertragungsrate.

Physikalische WLAN-Parameter

Hier werden die physikalischen WLAN-Parameter eingestellt, die den APs zugewiesen werden. Für jeden Satz von physikalischen WLAN-Parametern können Sie die folgenden Parameter definieren:



LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Radioprofile**

- **Name**

  Eindeutiger Name für diese Zusammenstellung von physikalischen WLAN-Parametern.

- **Vererbung**

  Auswahl eines schon definierten Satzes von physikalischen WLAN-Parametern, von dem die Einstellungen übernommen werden sollen.

- **Land**

  Land, in dem die APs betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wie die erlaubten Kanäle etc. festgelegt.

- **Automatische Kanalwahl**

  Standardmäßig können die APs alle Kanäle nutzen, die aufgrund der Ländereinstellung erlaubt sind. Um die Auswahl auf bestimmte Kanäle zu beschränken, können hier die gewünschten Kanäle als kommaseparierte Liste eingetragen werden. Dabei ist auch die Angabe von Bereichen (z. B. '1,6,11') möglich.

- **Management VLAN-ID**

Die VLAN-ID, die für das Management-Netz der APs verwendet wird.

Hinweis: Die Management-VLAN-ID **muss** auf einen Wert ungleich null eingestellt werden, um VLANs auf den WLAN-Netzwerken nutzen zu können. Das gilt auch dann, wenn das Management-Netz selbst nicht mit VLAN-IDs getaggt werden soll (Mgmt-VLAN-ID = 1).

Hinweis: Die VLAN-Aktivierung gilt jeweils nur für logischen WLAN-Netzwerke, die mit diesen physikalischen WLAN-Parametern verbunden sind.

- **Band Steering aktiviert**

  Dieser Eintrag bestimmt, ob der AP das Band-Steering aktivieren soll. In diesem Fall kann ein Dual-Port-Access-Point einen WLAN-Client auf ein bevorzugtes Frequenzband umleiten.

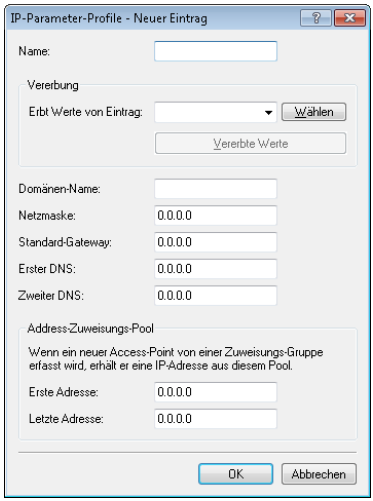
Hinweis: Alle weiteren physikalischen WLAN-Parameter entsprechen denen der üblichen Konfiguration für APs.

Hinweis: Für denn erfolgreichen Profilbezug ist es erforderlich, dass der HTTP-Zugriff auf den WLC aus dem lokalen Netz erlaubt ist.

13.4.3 Access Point Konfiguration

IP-Parameter-Profile

In dieser Tabelle definieren Sie bestimmte Netzprofile, welche sich einem AP zuweisen lassen, den der WLC nicht automatisch via DHCP konfigurieren soll. Auf diese Weise legen Sie gezielt fest, welche IP-Parameter ein AP nutzt.



Name

Name des IP-Parameter-Profils.

Vererbung

Auswahl eines schon definierten IP-Parameter-Profils, von dem die Einstellungen übernommen werden sollen (siehe *Vererbung von Parametern* auf Seite 1288).

Domänen-Name

Name der Domäne (DNS-Suffix), die dieses Profil nutzen soll.

Netzmaske

Netzmaske des Profils.

Standard-Gateway

Standard-Gateway, welches das Profil verwendet.

Erster DNS

Der DNS (Domain Name System), den das Profil verwenden soll.

Zweiter DNS

Zweiter, alternativer DNS, sollte der erste nicht erreichbar sein.

Erste Adresse

Anfang des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann

und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

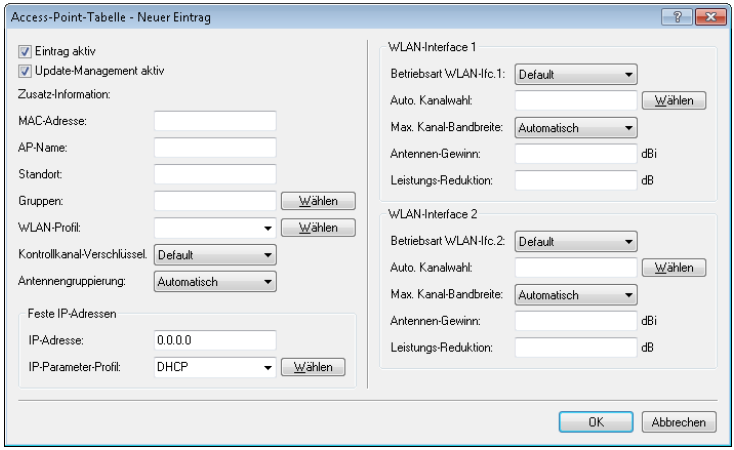
Letzte Adresse

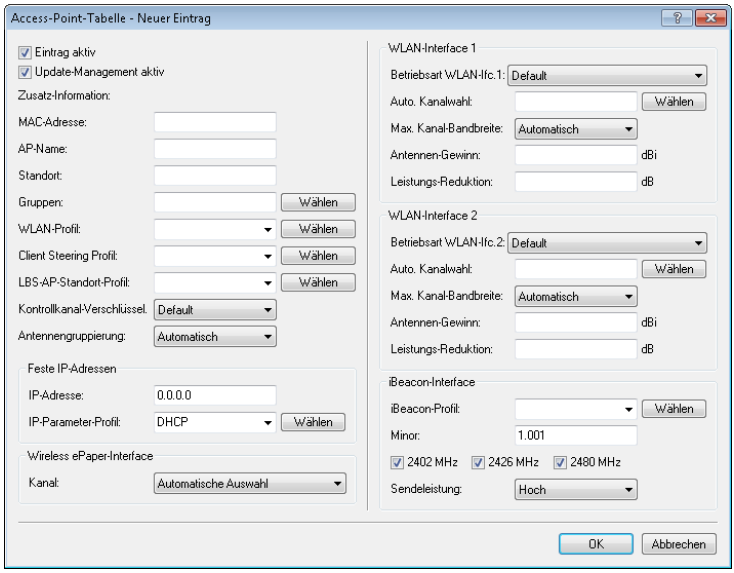
Ende des IPv4-Adressbereichs, aus dem ein neuer AP eine IP-Adresse erhält, wenn der WLC den AP einer Zuweisungs-Gruppe zuordnen kann und Sie für den betreffenden AP in der AP-Tabelle keine konkrete IP-Adresse definiert haben.

Weitere Informationen zu den Zuweisungs-Gruppen finden Sie im Abschnitt *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 1326.

Liste der Access Points

Die AP-Tabelle ist ein zentraler Aspekt der Konfiguration für WLCs. Hier ordnet der WLC den APs über WLAN-Profile (also Kombinationen aus logischen und physikalischen WLAN-Parametern) ihre MAC-Adresse zu. Außerdem hat die reine Existenz eines Eintrages in der AP-Tabelle für einen bestimmten AP Auswirkungen auf die Möglichkeit, eine Verbindung zu einem WLC aufbauen zu können. Für jeden AP können Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** die folgenden Parameter definieren:





Eintrag aktiv

Aktiviert bzw. deaktiviert diesen Eintrag.

Update-Management aktiv

Wenn Sie für diesen AP das Update-Management aktivieren, können er neue Firmware- oder Script-Versionen automatisch laden. Nehmen Sie alle weiteren Einstellungen unter AP-Update vor (*Zentrales Firmware- und Skript-Management*).

MAC-Adresse

MAC-Adresse des APs.

AP-Name

Name des APs im Managed-Modus.

Standort

Standort des APs im Managed-Modus.

Gruppen

Ordnet den AP einer oder mehrerer Gruppen zu

WLAN-Profil

WLAN-Profil aus der Liste der definierten Profile.

Client Steering Profil

Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.

LBS-AP-Standort-Profil

LBS-Standort-Profil aus der Liste der definierten Profile.

Kontrollkanal-Verschlüsselung

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung tauschen AP und WLC die Kontrolldaten im Klartext aus. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

Antennengruppierung

Um den Gewinn durch Spatial-Multiplexing zu optimieren, kann die Antennengruppierung konfiguriert werden.

IP-Adresse

Spezifizieren Sie hier eine feste IP-Adresse des APs.

IP-Parameter-Profil

Geben Sie hier den Profilnamen an, über den der WLC die IP-Einstellungen für den AP referenzieren muss. Wenn Sie den Standardwert DHCP beibehalten, ignoriert der WLC die Angabe der festen IP-Adresse, so dass der AP seine IP-Adresse über DHCP beziehen muss.

Kanal (Wireless ePaper-Interface)

Bestimmen Sie hier, wie die Kanalwahl der Wireless ePaper-Schnittstelle erfolgen soll.

Betriebsart WLAN-Ifc. 1

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 1. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der AP das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 2,4GHz-Band bevorzugt, sofern dieses verfügbar ist.

Betriebsart WLAN-Ifc. 2

Über diese Einstellung konfigurieren Sie das Frequenzband, in dem der AP die 2. physikalische WLAN-Schnittstelle betreibt. In der Einstellung **Default** wählt der AP das Frequenzband für die physikalische WLAN-Schnittstelle selbstständig aus. Dabei behandelt der AP das 5GHz-Band bevorzugt, sofern dieses verfügbar ist.

Hinweis: Sofern ein verwalteter AP lediglich über eine physikalische WLAN-Schnittstelle verfügt, ignoriert der AP die Einstellungen für die 2. physikalische WLAN-Schnittstelle.

Auto. Kanalwahl

Die Kanalauswahl erfolgt vom AP grundsätzlich automatisch für das Frequenzband des eingestellten Landes, wenn hier kein Eintrag erfolgt.

Tragen Sie hier die Kanäle ein, auf die sich die automatische Auswahl für das erste WLAN-Modul beschränken soll. Geben Sie hier nur einen Kanal an, so verwendet der AP nur diesen und es findet keine automatische Auswahl statt. Achten Sie deshalb darauf, dass die angegebenen Kanäle wirklich im Frequenzband des eingestellten Landes zur Verfügung stehen. Für das jeweilige Frequenzband ungültige Kanäle ignoriert der AP.

Max. Kanal-Bandbreite

Geben Sie an, wie und in welchem Umfang der AP die Kanal-Bandbreite für die physikalische(n) WLAN-Schnittstelle(n) festlegt. Folgende Werte sind möglich:

- **Automatisch**: Der AP ermittelt automatisch die maximale Kanal-Bandbreite (Default).
- **20MHz**: Der AP benutzt auf 20MHz gebündelte Kanäle.
- **40MHz**: Der AP benutzt auf 40MHz gebündelte Kanäle.
- **80MHz**: Der AP benutzt auf 80MHz gebündelte Kanäle.

Standardmäßig bestimmt die physikalische WLAN-Schnittstelle den Frequenzbereich, in dem die zu übertragenen Daten auf die Trägersignale aufmoduliert werden, automatisch. 802.11a/b/g nutzen 48 Trägersignale in einem 20 MHz-Kanal. Durch die Nutzung des doppelten Frequenzbereiches von 40 MHz können 96 Trägersignale eingesetzt werden, was zu einer Verdoppelung des Datendurchsatzes führt.

802.11n kann in einem 20 MHz-Kanal 52, in einem 40 MHz-Kanal sogar 108 Trägersignale zur Modulation nutzen. Für 802.11n bedeutet die Nutzung der 40 MHz-Option also einen Performance-Gewinn auf mehr als das Doppelte.

Antennen-Gewinn

Mit diesem Eintrag können Sie den Antennen-Verstärkungsfaktor (Gewinn in dBi) abzüglich der Dämpfungen für Kabel und ggf. Blitzschutz angeben. Hieraus errechnet der AP die im jeweiligen Land und für das jeweilige Frequenzband maximal zulässige Sendeleistung.

Wenn Sie das Feld leer lassen, verwendet der AP die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

Sie können die Sendeleistung auf minimal 0,5dBm im 2,4GHz-Band bzw. 6,5dBm im 5GHz-Band reduzieren. Das begrenzt den maximal einzutragenden Wert im 2,4GHz-Band auf 17,5dBi, im 5GHz-Band auf 11,5dBi.

Wichtig: Achten Sie darauf, dass Ihr Antennen-, Kabel- und Blitzschutz-Aufbau unter diesen Bedingungen den Regulierungsanforderungen des Landes entspricht, in dem Sie das System einsetzen.

Die Empfindlichkeit des Empfängers bleibt hiervon unbeeinflusst.

Tipp: Die aktuelle Sendeleistung können Sie mit Hilfe von WEBconfig bzw. Telnet unter **Status** > **WLAN-Statistik** > **WLAN-Parameter** > **Sendeleistung** oder per LANmonitor unter **System-Informationen** > **WLAN-Karte** > **Sendeleistung** einsehen.

Leistungs-Reduktion

Wenn Sie eine Antenne mit einem hohen Verstärkungsfaktor verwenden, können Sie mit diesem Eintrag die Sendeleistung des APs auf die in verwendeten Land und die im jeweiligen Frequenzband zulässige Sendeleistung herunterdämpfen.

Wenn Sie das Feld leer lassen, verwendet der AP die Default-Einstellung der Konfigurationsgruppe im verwendeten WLAN-Profil.

Es gelten dieselben Werte und Einschränkungen wie im Feld **Antennen-Gewinn**.

iBeacon-Profil (iBeacon-Interface)

Wählen Sie ein iBeacon-Profil aus der Liste der angelegten Profile aus.

Hinweis: iBeacon-Profile erstellen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Erweiterte Einstellungen** > **iBeacon-Profile**.

Minor

Legen Sie eine Minor-ID für das iBeacon-Modul fest.

2402 MHz, 2426 MHz, 2480 MHz

Definieren Sie hier, welche Sendekanäle das iBeacon-Modul verwenden soll.

Sendeleistung

Geben Sie an, Mit welcher Leistung das iBeacon-Modul senden soll. Folgende Werte sind möglich:

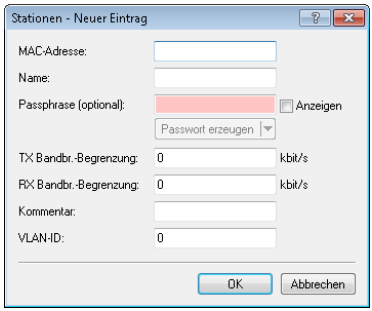
- **Hoch**: Das Modul sendet mit maximaler Leistung (Default).
- **Mittel**: Das Modul sendet mit durchschnittlicher Leistung.
- **Gering**: Das Modul sendet mit minimaler Leistung.

Stationen

Mit Hilfe der Stationstabelle legen Sie fest, welche WLAN-Clients sich in den WLAN-Netzwerken der APs anmelden können, die durch den WLC zentral verwaltet werden. Außerdem können Sie den einzelnen WLAN-Clients auf diesem Wege sehr komfortabel eine individuelle Passphrase zur Authentifizierung und eine VLAN-ID zuweisen.

Zur Nutzung der Stationstabelle unter **WLAN Controller** > **Stationen** > **Stationen** muss grundsätzlich der RADIUS-Server im WLC aktiviert sein. Alternativ kann auch eine Weiterleitung zu einem anderen RADIUS-Server konfiguriert werden. Weitere Information zu RADIUS finden Sie unter *RADIUS*.

Für jedes logische WLAN-Netzwerk, in dem die WLAN-Clients über RADIUS geprüft werden sollen, muss die MAC-Prüfung aktiviert werden.



MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressenbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Hinweis: Die Verwendung von Wildcards ist möglich.

SSID

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Hinweis: Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** (beim WLC in der Definition der logischen WLAN-Netzwerke (SSIDs)) für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrases verwendet.

TX Bandbreitenbegrenzung

Sende-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

RX Bandbreitenbegrenzung

Empfangs-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Hinweis: Die RX-Bandbreiten-Begrenzung ist nur aktiv für WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

VLAN-ID

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden. Bei der VLAN-ID '0' wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von Einträgen darauf zu achten, dass sich die Filterregeln nicht

widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

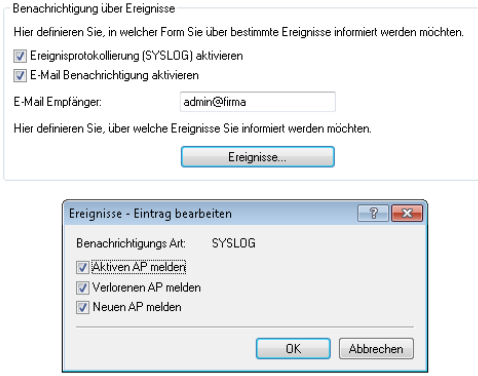
Wichtig: Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

Optionen für den WLAN-Controller

Im Bereich der **Optionen** werden die Benachrichtigungen bei Ereignissen im WLC eingestellt sowie einige Defaultwerte definiert.

Benachrichtigungen über Ereignisse

Die Benachrichtigungen können über SYSLOG oder E-Mail erfolgen. Dazu können Sie die folgenden Parameter definieren:



LANconfig: **WLAN-Controller** > **Optionen**

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** > **Benachrichtigung**

- **SYSLOG**

  Aktiviert die Benachrichtigung über SYSLOG.

  – Mögliche Werte: Ein/Aus.

- **E-Mail**

  Aktiviert die Benachrichtigung über E-Mail.

  – Mögliche Werte: Ein/Aus.

- **Ereignisse**

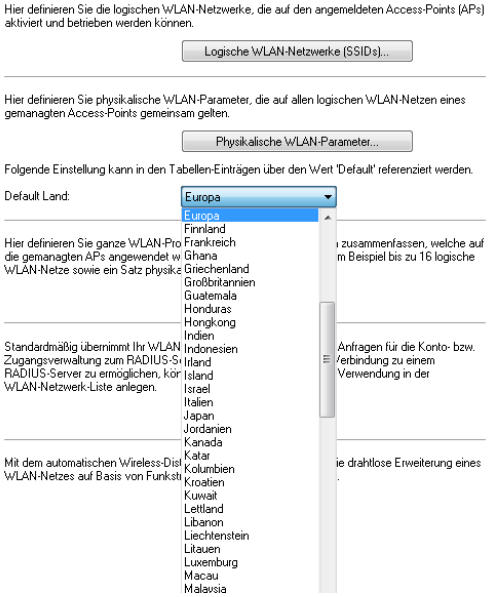
  Wählt die Ereignisse, die über die eine Benachrichtigung erfolgen soll.

  – Mögliche Werte:

  - Aktiven AP melden
  - Verlorenen AP melden
  - Neuen AP melden

Default-Parameter

Für einige Parameter können zentral Default-Werte definiert werden, die an anderen Stellen der Konfiguration als 'Default' referenziert werden können.



LANconfig: **WLAN-Controller** > **Profile** > **Default Land**

Webconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN Management** > **AP-Konfiguration** > **Laendereinstellung**

▶ **Default Land**

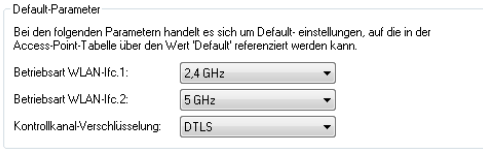
Land, in dem die Access Points betrieben werden sollen. Aufgrund dieser Information werden landesspezifische Einstellungen wir die erlaubten Kanäle etc. festgelegt.

– Mögliche Werte:

• Auswahl aus den verfügbaren Ländern

– Default:

• Europa



LANconfig: **WLAN-Controller** > **AP-Konfig** >

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration**

▶ **WLAN-Interface 1**

Frequenzband für das erste WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

▶ **WLAN-Interface 2**

Frequenzband für das zweite WLAN-Modul. Mit diesem Parameter kann das WLAN-Modul auch deaktiviert werden.

▶ **Verschlüsselung**

Verschlüsselung für die Kommunikation über den Kontrollkanal. Ohne Verschlüsselung werden die Kontrolldaten im Klartext ausgetauscht. Eine Authentifizierung mittels Zertifikat findet in beiden Fällen statt.

WLAN Layer-3 Tunneling

Einleitung

Der CAPWAP-Standard für das zentrale WLAN-Management bietet zwei verschiedene Übertragungskanäle an:

- Der obligatorische Kontrollkanal überträgt Verwaltungsdaten zwischen dem verwalteten AP und dem WLC.
- Der optionale Datenkanal überträgt die Nutzdaten aus den jeweiligen WLAN-Netzwerken (SSID) zwischen dem verwalteten AP und dem WLC.

Die optionale Nutzung des Datenkanals zwischen dem verwalteten AP und dem WLC entscheidet über den Weg der Nutzdaten:

- Wenn Sie den Datenkanal deaktivieren, leitet der AP die Nutzdaten direkt in das LAN weiter. In diesem Fall steuern Sie die Zuordnung von WLAN-Clients zu bestimmten LAN-Segmenten z. B. über die Zuweisung von VLAN-IDs. Der Vorteil dieser Anwendung liegt vor allem in der geringen Belastung des WLCs und des gesamten Netzwerks, weil der AP ausschließlich die Verwaltungsdaten über den CAPWAP-Tunnel überträgt, während er die Nutzdaten auf dem kürzesten Weg überträgt.
- Wenn Sie den Datenkanal aktivieren, leitet der AP auch die Nutzdaten an den zentralen WLC weiter. Dieser Ansatz hat folgende Vorteile:
  - Die APs können Netzwerke anbieten, die nur auf dem WLC verfügbar sind, z. B. einen zentralen Internetzugang für einen Public Spot.
  - Die von den APs angebotenen WLANs (SSIDs) sind auch ohne die Nutzung von VLAN voneinander separiert verfügbar. Der Verzicht auf VLAN reduziert den Aufwand für die Konfiguration der anderen Netzwerkkomponenten wie Switches etc.
  - Die an den APs in verschiedenen IP-Netzwerken angemeldeten WLAN-Clients können ohne Unterbrechung der IP-Verbindung zu einem anderen AP roamen, weil die Verbindung fortlaufen vom zentralen WLC verwaltet wird und nicht vom AP (Layer-3-Roaming).

Mit der Nutzung des Datenkanals entstehen auf der Basis der vorhandenen, physikalischen Netzwerkstruktur zusätzliche logische Netzwerke, die so genannten Overlay-Netzwerke.

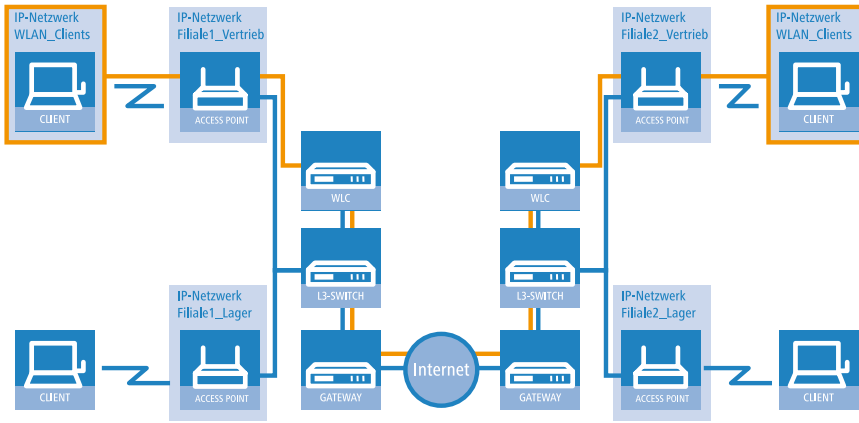


Abbildung 8: Overlay-Netzwerk über mehrere IP-Netzwerke hinweg

Über den Datenkanal können Sie so sogar über mehrere WLCs hinweg logische Overlay-Netzwerke aufspannen.

Mehrere WLCs innerhalb einer Broadcast-Domäne können das gleiche Overlay-Netzwerk unterstützen. Deaktivieren Sie den WLC-Datenkanal zwischen diesen WLCs (WEBconfig: LCOS-Menübaum > Setup > WLAN-Management > WLC-Cluster > WLC-Daten-Tunnel-aktiviert). Der mehrfache Empfang der Broadcast-Nachrichten führt ansonsten zu Schleifen. Da Router die Broadcast-Nachrichten verwerfen, haben Sie für WLC in getrennten Netzen die Möglichkeit, den CAPWAP-Datenkanal zu aktivieren.

Die APs nutzen virtuelle WLC-Schnittstellen (WLC-Tunnel), um die Datenkanäle der jeweiligen SSIDs zwischen dem AP und dem WLC zu verwalten. Jeder WLC bietet je nach Modell 16 bis 32 WLC-Tunnel an, die Sie bei der Konfiguration der logischen WLANs nutzen können.

Hinweis: Die Geräte bieten die virtuellen WLC-Schnittstellen in allen Dialogen zur Auswahl von logischen Schnittstellen an (LAN oder WLAN), z. B. in den Port-Tabellen der LAN- und VLAN-Einstellungen oder bei der Definition von IP-Netzwerken.

Tutorials

In den folgenden Abschnitten finden Sie konkrete Szenarien mit Schritt-für-Schritt Anleitungen für eine Reihe von Standard-Szenarien beim Einsatz von WLCs.

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Hinweis: Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

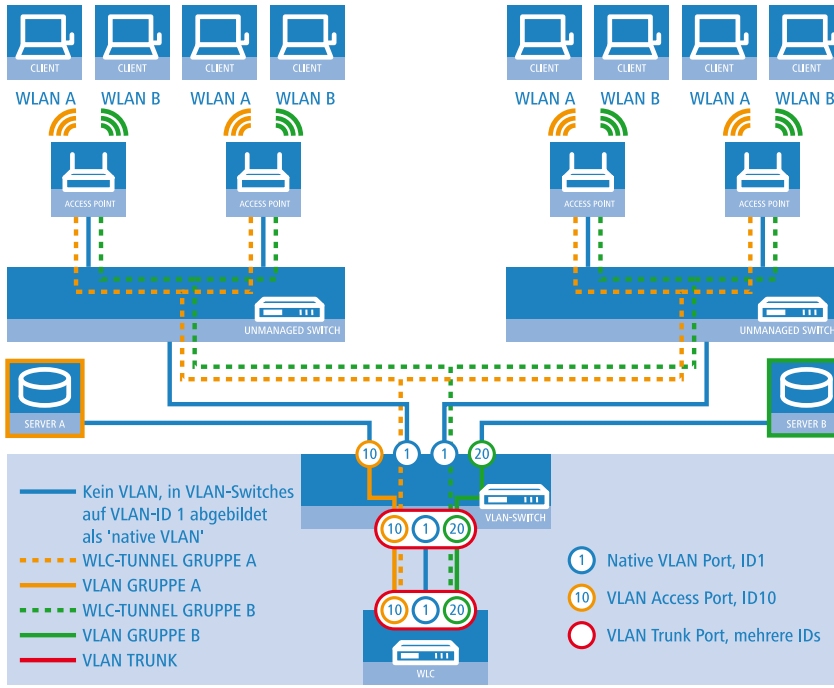


Abbildung 9: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

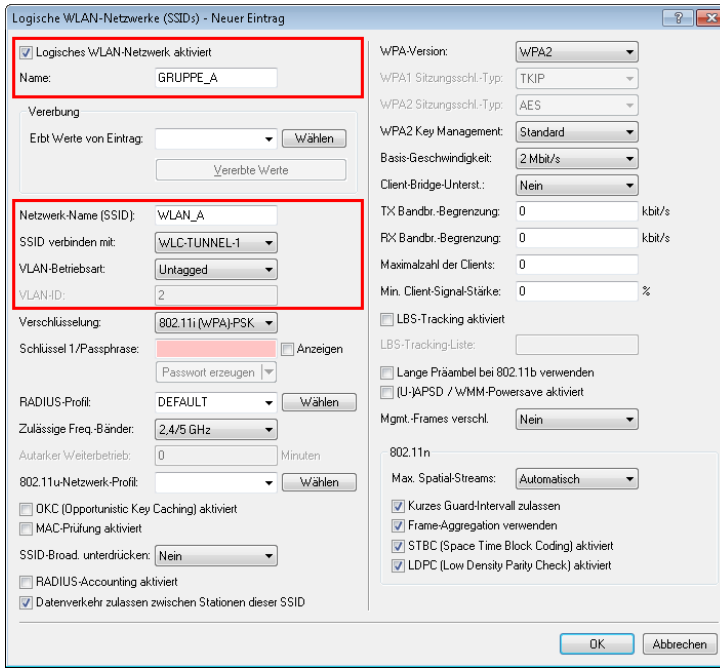
- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

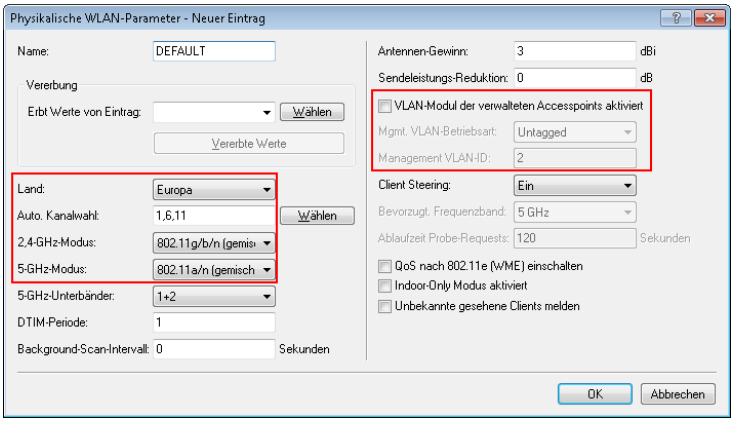
Hinweis: Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

Konfiguration der WLAN-Einstellungen

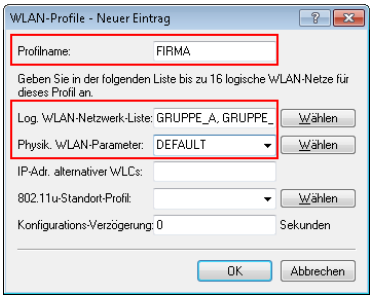
1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



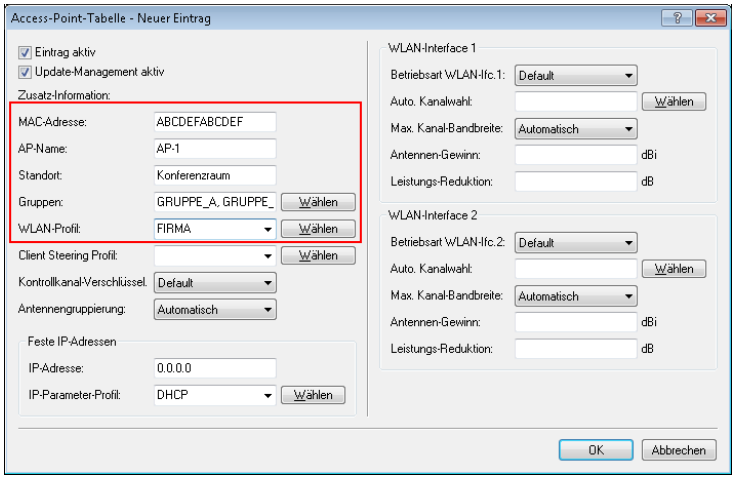
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

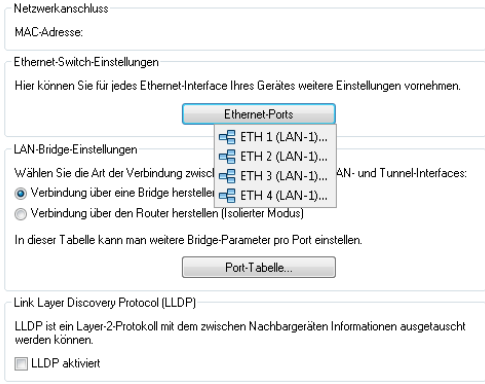


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.

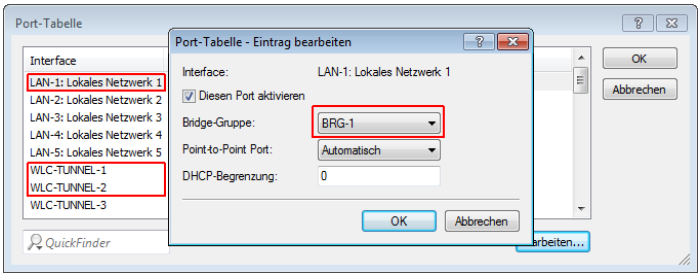


Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.

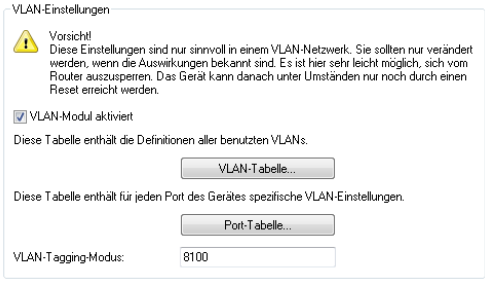


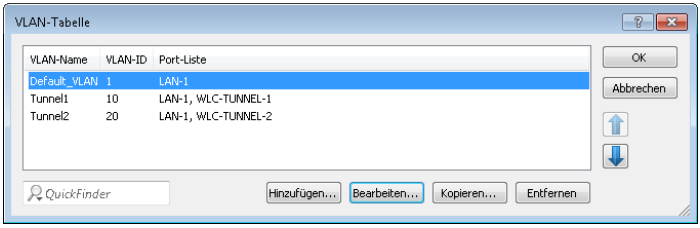
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



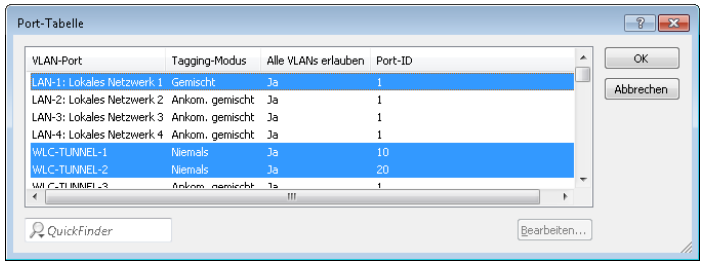
Hinweis: Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN**das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

Wichtig: Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

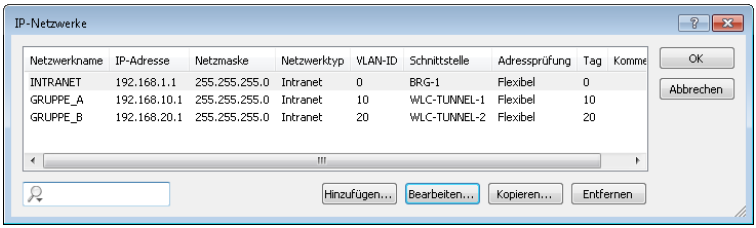
Hinweis:

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

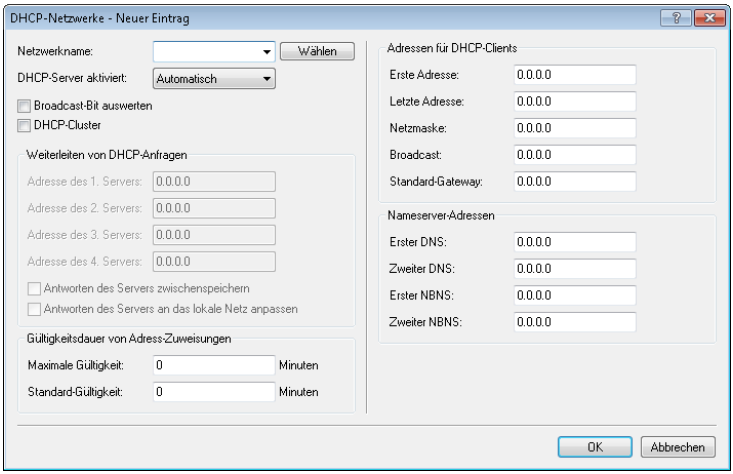
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

Wichtig: Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



"Layer-3-Roaming"

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht das Roaming auch über die Grenzen von Broadcast-Domänen hinweg. In diesem Anwendungsbeispiel verhindert ein Layer-3-Switch zwischen den Etagen die Weiterleitung der Broadcasts und trennt so die Broadcast-Domänen.

In diesem Beispiel haben zwei Benutzergruppen A und B jeweils Zugang zu einem eigenen WLAN (SSID). Die APs in mehreren Etagen des Gebäudes bieten die beiden SSIDs 'GRUPPE_A' und 'GRUPPE_B' an.

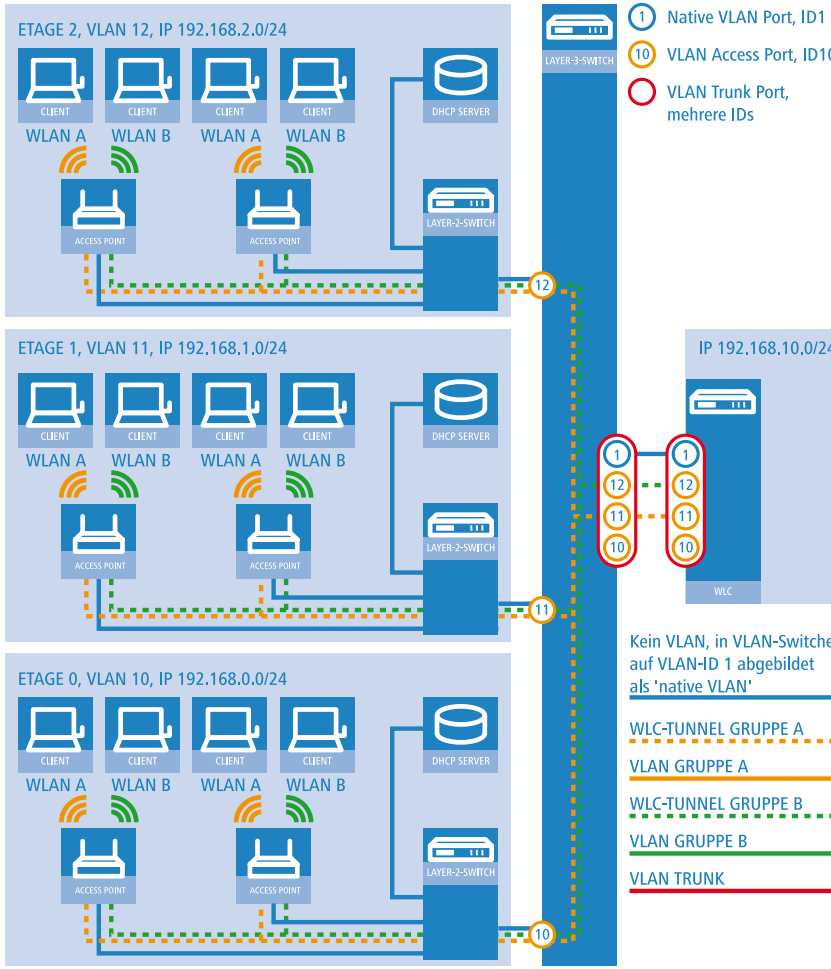


Abbildung 10: Anwendungsbeispiel Layer-3-Roaming

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

- Das Netz besteht aus 3 Segmenten in separaten Etagen eines Gebäudes.
- Ein zentraler Layer-3-Switch verbindet die Segmente und teilt das Netzwerk in 3 Broadcast-Domänen auf.
- Jedes Segment nutzt einen eigenen IP-Adressbereich und ein eigenes VLAN.

- In jedem Segment arbeitet ein lokaler DHCP-Server, der den APs die folgenden Informationen übermittelt:
  - IP-Adresse des Gateways
  - IP-Adresse des DNS-Servers
  - Domänen-Suffix

  Hinweis: Die Bereitstellung dieser Informationen ermöglicht es den APs, Kontakt mit dem WLC in einer anderen Broadcast-Domäne aufzunehmen.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll beim Wechsel der Etage nahtlos Zugang zu "seinem" WLAN behalten – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet. Da die Segmente in diesem Beispiel unterschiedliche IP-Adresskreise nutzen, gelingt das nur durch die Verwaltung der APs auf Layer 3 direkt über den zentralen WLC über die Grenzen der VLANs hinweg.

Hinweis: Die Konfiguration entspricht dem Beispiel *"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN* auf Seite 1316.

13.4.4 IP-abhängige Autokonfiguration und Tagging von APs

Sämtliche APs, die Sie einem gemanagten Netz hinzufügen, verwalten Sie im einfachsten Falle in einer flachen Hierarchie. In größeren Installationen mit Hunderten von APs über mehrere Standorte hinweg wird diese Form der Organisation jedoch schnell unübersichtlich und erzeugt einen hohen Administrationsaufwand. Über die Einrichtung von **Zuweisungs-Gruppen** haben Sie daher die Möglichkeit, das Management verteilter APs zu vereinfachen. Hierbei lassen Sie neue APs in Abhängigkeit von der erhaltenen IP-Adresse automatisch vom WLC konfigurieren. Dadurch entfällt die manuelle Zuweisung eines IP-Parameter-Profils, eines WLAN-Profils und eines Client Steering-Profils durch einen Administrator.

Die Anwendung einer Zuweisungs-Gruppe bei Anmeldung eines neuen APs an einem zentralen WLC läuft nach folgendem Schema ab: Nachdem die

neuen APs am gewünschten Einsatzort (z. B. einem Firmen- bzw. Filialnetz) installiert sind, versuchen diese, eine Verbindung zum eingetragenen WLC aufzubauen und via CAPWAP eine Konfiguration zu beziehen. Der WLC erkennt die Verbindungsanfragen und prüft für jeden neuen AP, ob in der AP-Tabelle ein geeignetes AP-Profil (z. B. das Default-Profil) vorliegt oder/und eine geeignete Zuweisungs-Gruppe definiert ist. Liegen eine oder mehrere Konfigurationsmöglichkeiten vor, prüft der WLC diese auf folgende Zustände:

1. Für einen neuen AP existiert eine Zuweisungs-Gruppe, jedoch kein AP-Profil. In diesem Fall weist der WLC dem neuen AP die innerhalb der Zuweisungs-Gruppe definierten Profile zu.
2. Für einen neuen AP existiert sowohl eine Zuweisungs-Gruppe als auch ein AP-Profil. In diesem Fall ignoriert der WLC die Zuweisungs-Gruppe und weist dem neuen AP die innerhalb des AP-Profils definierten Profile zu.
3. Für einen neuen AP existiert ein AP-Profil, aber keine Zuweisungs-Gruppe. Das Verhalten entspricht dem von Punkt (2).

Existieren für einen neuen AP weder ein AP-Profil, noch eine Zuweisungs-Gruppe, gibt der WLC eine Warnung aus, welche den Administrator auf die Fehlkonfiguration hinweist.

Nach der erfolgreichen Gruppenzuweisung legt der WLC in der Access-Point-Tabelle automatisch ein AP-Profil für jeden neuen AP an. Im Feld **Gruppen** referenziert der WLC die Zuweisungs-Gruppen, die er beim Hinzufügen des neuen AP angewandt hat.

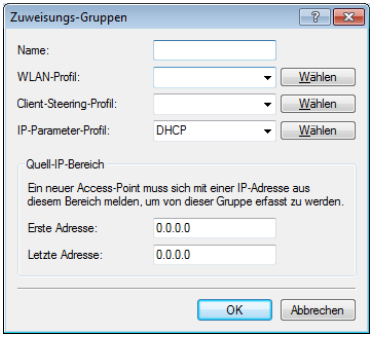
Wichtig: Ein AP darf immer nur eine Zuweisungsgruppe erhalten. Sobald sich Anwendungsbereiche von Zuweisungsgruppen überschneiden, erkennt HiLCOS derartige Konfigurationsfehler und schreibt die Meldungen in die entsprechende Status-Tabelle unter **Status** > **WLAN-Management** > **AP-Konfiguration**.

Über das Gruppen-Feld haben Sie ebenfalls die Möglichkeit, einen AP mit individuell definierbaren Tags zu versehen. Diese **Tag-Gruppen** lassen sich z. B. beim Ausführen von Aktionen auf dem WLC als Filterkriterien einsetzen, um eine Aktion auf eine Auswahl von APs zu beschränken.

Einrichten von Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration

Das nachfolgende Tutorial zeigt Ihnen, wie Sie auf einem WLC Zuweisungs-Gruppen für die IP-abhängige Autokonfiguration neuer APs einrichten.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Zuweisungs-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie als **Name** eine eindeutige Bezeichnung für die Zuweisungs-Gruppe an, z. B. `Filiale_Berlin`.
4. Wählen Sie das **WLAN-Profil** aus, welches der WLC einem neuen AP automatisch zuweist, wenn die IP-Adresse des neuen APs innerhalb des Quell-IP-Bereichs liegt.
5. Geben Sie ein **IP-Parameter-Profil** an, sofern der neue AP eine manuelle Netzkonfiguration erhalten soll. Andernfalls belassen Sie den Einzelwert **DHCP**; hierbei erhält der AP eine automatische Netzkonfiguration vom DHCP-Server. Der DHCP-Server muss dazu entsprechend konfiguriert sein.

   Sofern Sie eine manuelle Netzkonfiguration zuweisen wollen, bei der ein neuer AP eine abweichende IP-Adresse erhält, so geben Sie den entsprechenden Adressbereich im **IP-Parameter-Profil** unter **Address-Zuweisungs-Pool** an.

6. **Optional**: Geben Sie ein **Client Steering-Profil** an, um bei mehreren neuen APs die sich im Sendebereich befindlichen, künftigen WLAN-Clients auf den für sie idealen AP umzuleiten.

Wichtig: Sofern Sie Client Steering aktivieren, muss dieses innerhalb der zu managenden Infrastruktur für jeden AP aktiviert sein. Weitere Informationen dazu finden Sie im Abschnitt *Client Steering über den WLC* auf Seite 1388.

7. Geben Sie den Anfang und das Ende des **Quell-IP-Bereich**s an, für den die Zuweisungs-Gruppe gilt.
   Ein neuer AP muss sich mit einer IP-Adresse aus diesem Bereich beim WLC anmelden, um die für die Gruppe hinterlegte Konfiguration zu erhalten.
8. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

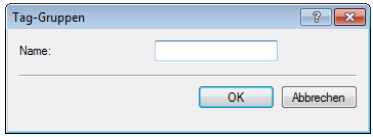
Der WLC weist fortan allen neuen APs die in den Zuweisungs-Gruppen referenzierten Profile zu. Über die HiLCOS-Konsole haben Sie dann die Möglichkeit, Informationen zur Kategorisierung abzurufen, siehe *Übersicht der capwap-Parameter im show-Befehl* auf Seite 73.

Wichtig: Achten Sie darauf, dass in der Access-Point-Tabelle kein AP-Profil (z. B. das Default-Profil) vorliegt, welches der WLC den neuen APs zuweisen könnte. Sofern ein geeignetes AP-Profil vorliegt, erhält dies gegenüber Zuweisungs-Gruppen stets die höhere Priorität.

Einrichten von Tag-Gruppen für die selektive Auswahl von APs

Das nachfolgende Tutorial zeigt Ihnen, wie Sie eine AP-Konfiguration auf einem WLC um eine Tag-Gruppe erweitern. Dazu legen Sie zunächst eine Tag-Gruppe an und weisen diese Gruppe anschließend einem WLAN-Profil zu.

1. Öffnen Sie den Konfigurationsdialog für Ihr Gerät und wählen Sie **WLAN-Controller** > **AP-Konfiguration** > **Tag-Gruppen**.
2. Klicken Sie **Hinzufügen**, um eine neue Gruppe anzulegen.



3. Geben Sie unter **Name** den zu definierenden Tag ein und speichern Sie den Eintrag mit **OK**.
4. Wechseln Sie in den Dialog **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**.
5. Wählen Sie ein bestehendes AP-Profil über **Bearbeiten** aus oder fügen Sie ggf. ein neues hinzu.
6. Wählen Sie unter **Gruppen** die zuvor anlegte(n) Tag-Gruppe(n) aus. Mehrere Tag-Gruppen trennen Sie durch eine kommaseparierte Liste.

   Hinweis: Die Taggruppen sind unabhängig von den Zuweisungs-Gruppen, deren Zuweisung im selben Eingabefeld erfolgt. Zuweisungs-Gruppen werden generell vom Gerät zugewiesen und bedürfen keiner nutzerseitigen Zuordnung. Das manuelle Zuordnen einer Zuweisungs-Gruppe hat gemäß der unter *IP-abhängige Autokonfiguration und Tagging von APs* auf Seite 1326 beschriebenen Zustandsprüfung keinen Effekt auf die AP-Konfiguration. Auswirkungen bestehen lediglich auf die Filterung im Befehl `show capwap group` an der Konsole.

   Wichtig: Das manuelle Hinzufügen von Zuweisungs-Gruppen zu Filterungszwecken ist nicht empfehlenswert. Legen Sie stattdessen separate Tag-Gruppen an.

7. Schließen Sie alle Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf Ihr Gerät.

Der WLC versieht fortan alle APs, die das bearbeitete WLAN-Profil erhalten, mit den darin referenzierten Tags.

13.5 Access Point Verwaltung

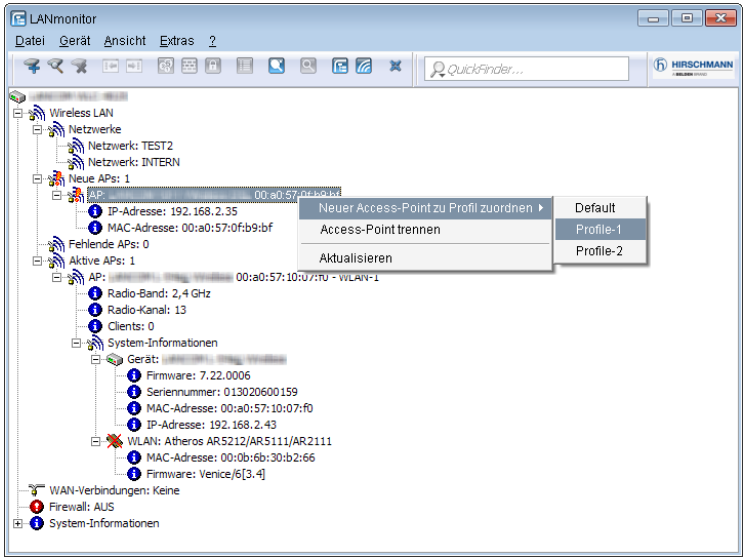
13.5.1 Neue Access Points manuell in die WLAN-Struktur aufnehmen

Wenn Sie die APs nicht automatisch in die WLAN-Struktur aufnehmen wollen, können Sie die APs auch manuell akzeptieren.

Access Points akzeptieren über den LANmonitor

Neue APs können sehr komfortabel über den LANmonitor akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem AP nach der Übertragung eines neuen Zertifikats zugewiesen wird.

Klicken Sie dazu im LANmonitor mit der rechten Maustaste auf den neuen AP, den Sie in die WLAN-Struktur aufnehmen möchten. Wählen Sie dann im Kontextmenü die Konfiguration, die Sie dem Gerät zuordnen wollen.

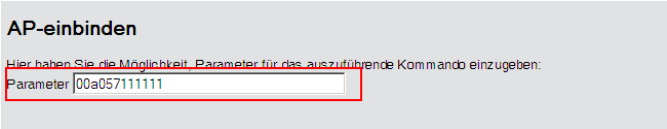


Hinweis: Mit dem Zuweisen der Konfiguration wird der AP in der AP-Tabelle des WLCs eingetragen. Es dauert jedoch einige Sekunden, bis der WLC dem AP auch ein Zertifikat zugewiesen hat und dieser ein aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene AP wird also für eine kurze Zeit als "Lost AP" im LANmonitor und soweit vorhanden durch die rote Lost-AP-LED und im Gerätedisplay angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

Access Points akzeptieren über WEBconfig mit Zuweisung eines Zertifikats

Neue APs, die kein gültiges Zertifikat haben, für die jedoch ein Eintrag in der AP-Tabelle vorliegt, können über eine Aktion in WEBconfig manuell akzeptiert werden.

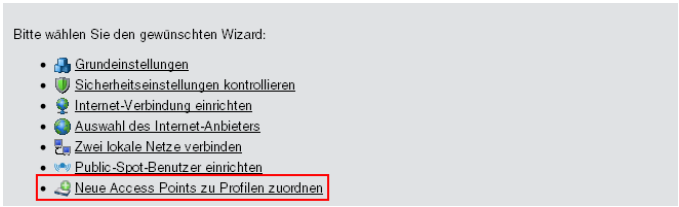
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig.
2. Wählen Sie unter **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** die Aktion **AP-einbinden**.
3. Geben Sie als Parameter für die Aktion die MAC-Adresse des APs ein, den Sie akzeptieren möchten, und bestätigen Sie mit **Ausführen**.



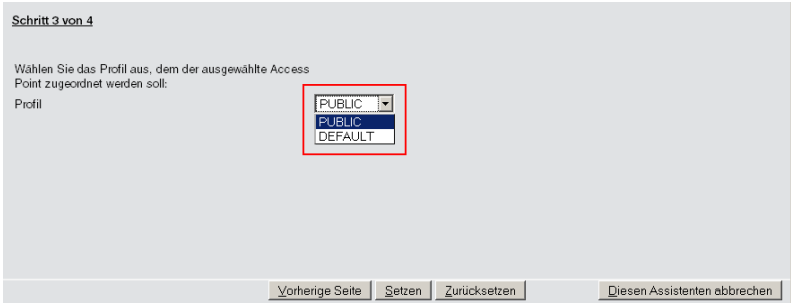
Access Points akzeptieren über WEBconfig mit Zuweisung von Zertifikat und Konfiguration

Neue APs, die kein gültiges Zertifikat haben und für die kein Eintrag in der AP-Tabelle vorliegt, können über einen Assistenten in WEBconfig manuell akzeptiert werden. Dabei wird eine Konfiguration ausgewählt, welche dem AP nach der Übertragung eines neuen Zertifikats zugewiesen wird.

1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig. Wählen Sie unter **Setup-Wizards** den Wizard **Neue Access Points zu Profilen zuordnen**.



2. Klicken Sie auf den Link, um den Assistenten zu starten. Wählen Sie den gewünschten AP anhand seiner MAC-Adresse aus und geben Sie die WLAN-Konfiguration an, die dem AP zugewiesen werden soll.



Hinweis: Mit dem Zuweisen der Konfiguration wird der AP in der AP-Tabelle des WLAN-Controllers eingetragen. Es dauert jedoch einige Sekunden, bis der WLC dem AP auch ein Zertifikat zugewiesen hat und er damit aktives Element der zentralen WLAN-Struktur wird. Der neu aufgenommene AP wird also für eine kurze Zeit als „Lost AP“ im LANmonitor und soweit vorhanden durch die rote Lost-AP-LED und im Gerätedisplay angezeigt, bis die Zertifikatszuweisung abgeschlossen ist.

Neue APs über den WEBconfig Setup-Wizard hinzufügen

Ab HiLCOS 9.00 verfügen WLCs über einen überarbeiteten Setup-Wizard **Neue Access Points zu Profilen zuordnen**, der Ihnen das Hinzufügen neuer APs über WEBconfig erleichtert. Der neue Setup-Wizard erlaubt Ihnen, mit wenigen Mausklicks

- gezielt nach einem neuen AP zu suchen;
- ein oder mehrere neue APs gleichzeitig zu akzeptieren;
- einem neuen AP ein WLAN-Profil oder eine Kanalliste zuzuweisen;
- die Konfiguration eines bereits akzeptierten AP an einen neuen AP zu vererben;
- die Konfiguration eines akzeptierten fehlenden AP mit der eines neuen AP zu wechseln. Beim Wechseln einer Konfiguration erhält der neue AP die vollständige Konfiguration des akzeptierten fehlenden AP (mit Ausnahme der MAC-Adresse). Beim Einbinden des neuen AP löscht der WLC anschließend die Konfiguration des akzeptierten fehlenden AP.

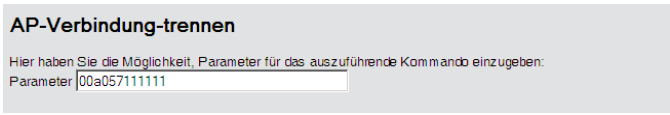
Um einen neuen AP mit den getätigten Einstellungen zu akzeptieren, klicken Sie abschließend auf **AP-einbinden**.

Hinweis: Sofern ein Sie einen AP über Zuweisungs-Gruppen konfigurieren lassen, brauchen Sie für den betreffenden AP keine Einstellungen in diesem Setup-Wizard vornehmen. Der WLC weist dem AP automatisch beim Einbinden die Einstellungen aus den entsprechenden Gruppen zu.

13.5.2 Access Points manuell aus der WLAN-Struktur entfernen

Um einen AP, der vom WLC verwaltet wird, aus der WLAN-Struktur zu entfernen, müssen Sie folgende Aktionen ausführen:

1. Stellen Sie im AP die WLAN-Betriebsart für die WLAN-Module von 'Managed' auf 'Client' oder 'Access-Point' um.
2. Löschen Sie im WLC die Konfiguration für den AP bzw. deaktivieren Sie die **Automatische Zuweisung der Default-Konfiguration** über **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-automatisch-einbinden**.
3. Trennen Sie die Verbindung zum AP unter WEBconfig im Bereich **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** mit der Aktion **AP-Verbindung-trennen** oder alternativ im LANmonitor.
4. Geben Sie als Parameter für die Aktion die MAC-Adresse des APs ein, zu dem Sie die Verbindung trennen möchten, und bestätigen Sie mit **Ausführen**.



13.5.3 Access Point deaktivieren oder dauerhaft aus der WLAN-Struktur entfernen

In manchen Fällen ist es notwendig, einen vom WLC verwalteten AP entweder vorübergehend zu deaktivieren oder dauerhaft aus der WLAN-Struktur zu entfernen.

Access Point deaktivieren

Um einen AP zu deaktivieren, setzen Sie den entsprechenden Eintrag in der AP-Tabelle auf 'inaktiv' oder löschen Sie den Eintrag aus der Tabelle. Dadurch werden die WLAN-Module im Managed-Modus ausgeschaltet, die entsprechenden SSIDs werden im AP gelöscht.

Hinweis: Die WLAN-Module und die WLAN-Netzwerke (SSIDs) werden auch dann abgeschaltet, wenn der autarke Weiterbetrieb aktiviert ist.

Ein so deaktivierter AP bleibt mit dem WLC verbunden, die Zertifikate bleiben erhalten. Der WLC kann also jederzeit durch das Aktivieren des Eintrags in der AP-Tabelle oder durch einen neuen Eintrag in der AP-Tabelle für die entsprechende MAC-Adresse den AP und seine WLAN-Module im Managed-Modus wieder einschalten.

Wird die Verbindung zu einem deaktivierten AP getrennt (unbeabsichtigt z. B. durch Störung im LAN oder gezielt durch den Administrator), dann beginnt der AP eine neue Suche nach einem passenden WLC. Der bisherige WLC kann zwar das Zertifikat auf Gültigkeit prüfen, hat aber keinen (aktiven) Eintrag in der AP-Tabelle – er wird also zum sekundären WLC für diesen AP. Findet der AP einen primären WLC, so wird er sich bei diesem anmelden.

Access Point dauerhaft aus der WLAN-Struktur entfernen

Damit ein AP auf Dauer nicht mehr Mitglied der zentral verwalteten WLAN-Struktur ist, müssen die Zertifikate im SCEP-Client gelöscht oder widerrufen werden.

- Wenn Sie Zugriff auf den AP haben, können Sie die Zertifikate am schnellsten durch einen Reset des Geräts löschen.

- Wurde das Gerät gestohlen und soll aus diesem Grund aus der WLAN-Struktur entfernt werden, so müssen die Zertifikate in der CA des WLCs widerrufen werden. Wechseln Sie dazu unter WEBconfig in den Bereich **HiLCOS-Menübaum** > **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate** in die **Zertifikatsstatus-Tabelle**. Löschen Sie dort das Zertifikat für die MAC-Adresse des APs, den Sie aus der WLAN-Struktur entfernen möchten. Die Zertifikate werden dabei nicht gelöscht, aber als abgelaufen markiert.

Hinweis: Bei einer Backup-Lösung mit redundanten WLCs müssen die Zertifikate in allen WLCs widerrufen werden!

13.6 AutoWDS – Kabellose Integration von APs über P2P-Verbindungen

In einem zentral gemanagten WLAN sind die angeschlossenen Access Points (APs) klassischerweise über das LAN mit dem WLAN-Controller (WLC) verbunden. Diese LAN-Verbindungen geben gleichzeitig die Topologie des verwalteten Netzes vor. Eine Erweiterung des Netzes um zusätzliche APs ist jedoch auf die Reichweite der kabelgebundenen Netzarchitektur beschränkt und erfordert ggf. einen Ausbau der betreffenden Infrastruktur.

Mittels **AutoWDS** haben Sie die Möglichkeit, die Erweiterung eines WLANs auf Basis von Funkstrecken (P2P) vorzunehmen und dadurch kostengünstig und schnell sehr skalierbare Netze zu errichten. "AutoWDS" steht dabei für "Automatic Wireless Distribution System". Die Funktion erlaubt Ihnen, ein FunkNetz aus mehreren APs herzustellen, welche ausschließlich drahtlos untereinander verbunden sind: die logische Verbindung allein genügt. Die möglichen Einsatzgebiete erstrecken sich z. B. auf die flächendeckende Anbindung kleiner Areale oder ganzer Gebiete an das Internet oder ein FirmenNetz, in denen eine Verbindung über LAN nicht sinnvoll oder unpraktikabel ist.

Im einfachsten Fall benötigen Sie lediglich einen WLC, der mit einem AutoWDS-fähigen AP via LAN verbunden ist. Der AP spannt das gemanagte WLAN auf und agiert gleichzeitig als "Zugangs-AP". Über den Zugangs-AP stellen hinzukommende AutoWDS-fähige APs die Verbindung zum WLC her, welcher ihnen mittels CAPWAP eine Konfiguration übermittelt. Nach Erhalt

der Konfiguration und Eingliederung in das gemanagte WLAN nutzen die einzelnen APs P2P-Strecken, um Nutzerdaten weiterzuleiten, miteinander zu kommunizieren und die Topologie aufrecht zu erhalten. Weitere hinzukommende APs sind in der Lage, die eingebundenen APs ihrerseits als Zugangs-APs zu nutzen. Auf diese Weise lassen sich mehrere APs miteinander verketten und vermaschte Netze aufbauen, die optional via RSTP redundante Verbindungen aufweisen. Aus Sicht eines hinzukommenden AP sind eingebundene APs "Master-APs". Aus Sicht des Master-AP sind hinzukommende APs "Slave-APs".

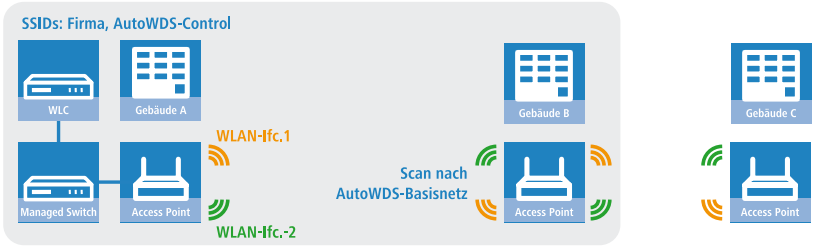


Abbildung 11: Phase 1 – Hinzukommender AP in Gebäude B sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude A

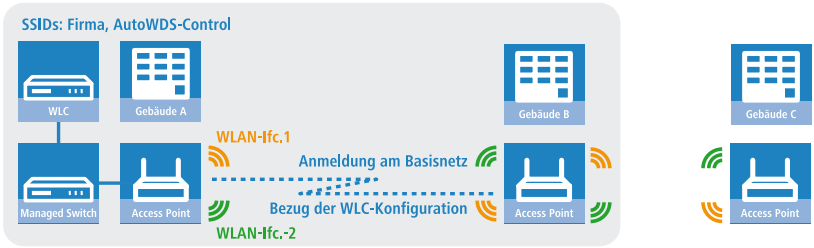


Abbildung 12: Phase 2 – Hinzukommender AP in Gebäude B findet WLC und bezieht AP-Konfiguration über CAPWAP

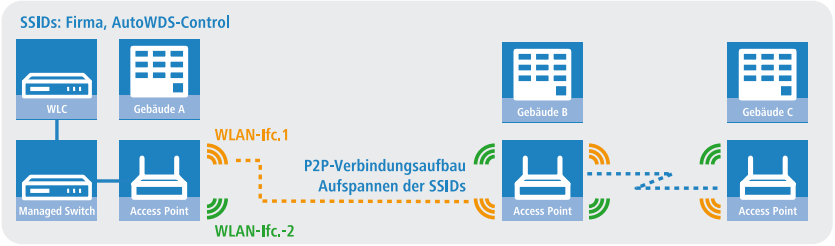


Abbildung 13: Phase 3 – Hinzukommender AP in Gebäude B integriert sich in das gemanagte WLAN. Hinzukommender AP in Gebäude C sucht nach AutoWDS-Basisnetz und findet Zugangs-AP in Gebäude B.

Genauere Informationen zum Integrationsablauf und zu den Betriebsmodi beim Topologie-Management erhalten Sie in den nachfolgenden Abschnitten zur Funktionsweise von AutoWDS.

Wichtig: AutoWDS eignet sich ausschließlich für statische Infrastrukturen, nicht für sich bewegende APs. Sollte ein AP aus der Reichweite seines P2P-Partners wandern und die Verbindung zum Netz verlieren, erfolgt eine temporäre Downtime mit anschließender *Rekonfiguration*. Das Roaming von WLAN-Clients zwischen einzelnen AutoWDS-APs hingegen unterscheidet sich nicht von dem zwischen normalen APs.

Wichtig: AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Wichtig: Das DFS-Verhalten eines AP im 5-GHz-Betrieb ist von AutoWDS unberührt und besitzt höhere Priorität. Die DFS-Radarerkennung kann bewirken, dass der AP während des Betriebs einen plötzlichen Kanalwechsel durchführt oder das WLAN bei Ausfall der möglichen Frequenzen – aufgrund mehrerer Radarerkennungen auf verschiedenen Kanälen – für einige Zeit komplett deaktiviert. Der betroffene AP kann somit für Störungen des gesamten AutoWDS-Verbundes verantwortlich sein oder eine Zeit lang gar keine SSIDs aufspannen. Innerhalb von Gebäuden haben Sie die Möglichkeit,

evtl. auftretenden Störungen durch Aktivieren des Indoor-Modus entgegenzuwirken.

Hinweis:

Wenn Sie AutoWDS auf einem Gerät mit einer einzigen physikalischen WLAN-Schnittstelle einsetzen, drittelt sich im Betrieb deren Datenrate, da das Gerät eingehende/ausgehende Daten mehrfach senden muss: An die WLAN-Clients, an einen Master-AP und ggf. an einen Slave-AP. Um diesen Effekt zu mildern, sollten Sie ausschließlich Geräte mit mehreren physikalischen WLAN-Schnittstellen einsetzen und auf diesen eine Trennung des Datenverkehrs vornehmen. Dazu reservieren Sie eine physikalische WLAN-Schnittstelle für die Anbindung der APs und eine physikalische WLAN-Schnittstelle für die Anbindung der Clients.

MultiHop auf ein und derselben WLAN-Schnittstelle aktivieren Sie bei Bedarf in der AutoWDS-Profil-Konfiguration, da dieses aufgrund der Performance-Verluste standardmäßig deaktiviert ist.

13.6.1 Hinweise zur Nutzung von AutoWDS

Die Einsatzmöglichkeiten von AutoWDS unterliegen technischen Beschränkungen, wodurch sich die Funktion ausschließlich für bestimmte Anwendungsszenarien eignet. Bitte beachten Sie daher aufmerksam die in diesem Kapitel beschriebenen allgemeinen Hinweise, um möglichen Komplikationen vorzubeugen. Die hier gelisteten Punkte sind als Ergänzung zu den Hinweisen des übrigen AutoWDS-Kapitels zu verstehen, wobei Überschneidungen möglich sind.

- APs müssen bei Radarerkennung (5-GHz-Band, Outdoor bzw. DFS) den Kanal wechseln. Dadurch sind kurzzeitige Unterbrechungen des WLANs durch notwendigen Kanalwechsel möglich.
- Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.
- Bei Verwendung von AutoWDS auf ausschließlich einem Funkkanal treten Mehrfachübertragungen und Hidden-Station-Probleme auf. Empfehlenswert ist daher der Einsatz von APs mit zwei physikalischen WLAN-Schnittstellen (Dual Radio) auf separaten Funkkanälen.

- AutoWDS unterstützt keine Netztrennung von SSIDs auf VLANs über eine statische Konfiguration oder eine dynamische VLAN-Zuweisung über RADIUS. Soll eine Netztrennung von SSIDs erfolgen, müssen Sie diese durch Layer-3-Tunnel separieren.

Wichtig: Betreiben Sie DFS in Kombination mit AutoWDS, konfigurieren Sie für den autarken Weiterbetrieb (Continuation-Time) des AutoWDS-Profils mindestens 2 Minuten. So bleibt dem CAPWAP-Layer nach der Downtime einer P2P-Verbindung aufgrund eines DFS-Scans von einer Minute eine zusätzliche Minute Zeit, die CAPWAP-Verbindung zum WLC über die P2P-Verbindung nach dem DFS-Scan wieder herzustellen.

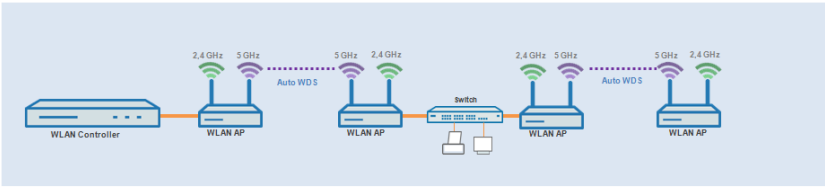
Wichtig: Achten Sie nach Möglichkeit darauf, dass alle beteiligten APs je physikalischer WLAN-Schnittstelle (WLAN-1, WLAN-2) durchgehend das gleiche Frequenzband (2,4GHz oder 5GHz) verwenden, um so eventuelle Probleme bei der automatischen Topologie-Konfiguration auszuschließen.

Nachfolgend finden Sie eine Bewertung der **Eignung von AutoWDS** für bestimmte von Anwendungsszenarien.

Gut geeignet:

Nutzung einer **dedizierten** physikalischen WLAN-Schnittstelle für die P2P-Strecken.

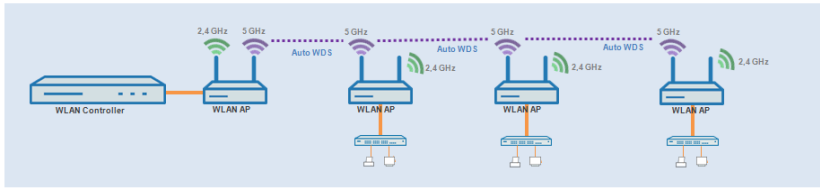
- Verwendung von unterschiedlichen Kanälen für die P2P-Strecken (Indoor)
- Verwendung von AutoWDS auf bis zu 3 Hops



Bedingt geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus), wobei alle P2P-Strecken den gleichen Funkkanal verwenden.

- Verwendung für Betrieb ohne DFS (Indoor)
- Verwendung von AutoWDS auf bis zu 3 Hops



Mögliche auftretende Probleme sind z. B. das sogenannte Hidden-Station-Phänomen oder die Durchsatz-Reduzierung durch Mehrfachübertragung.

- **Hidden-Station-Phänomen**: Bei größeren Entfernungen können sich weit entfernte APs des selben Netzwerkes u. U. nicht mehr gegenseitig sehen, da die Empfangsradien nicht ausreichen. In diesem Fall steigt die Wahrscheinlichkeit, dass mehrere APs gleichzeitig senden und sich in der Übertragung gegenseitig stören. Diese Kollisionen führen zu Mehrfachübertragungen und Performanz-Einbußen.

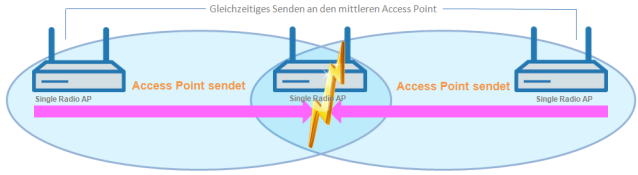


Abbildung 14: Gleichzeitiges senden an den mittleren AP: Die beiden äußeren APs erkennen die Kollision nicht.

- **Durchsatz-Reduzierung durch Mehrfachübertragung**: Überträgt ein AP Datenpakete auf dem gleichen Kanal mehrfach, reduziert sich in der Praxis der maximal erreichbare Durchsatz (Halbierung pro Hop).

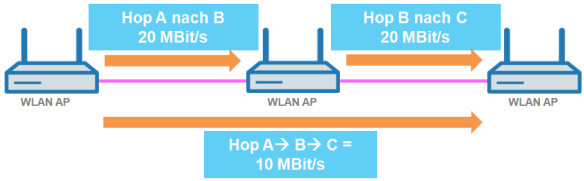
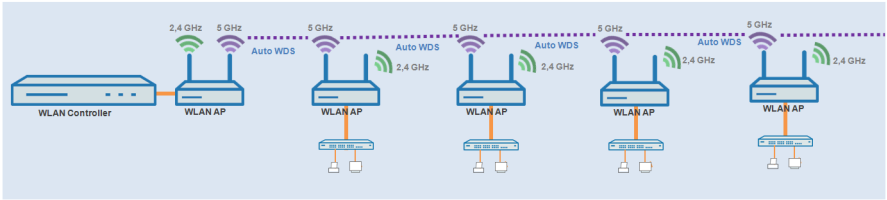


Abbildung 15: Übertragung der Datenpakete auf jedem Hop

Nicht geeignet:

Nutzung einer physikalischen WLAN-Schnittstelle **gleichzeitig** für AutoWDS-Uplink und -Downlink (Repeater-Modus) bei Outdoor-Betrieb mit mehr als 1 Hop im 5-GHz-Band.



Im Repeater-Modus nimmt die physikalische WLAN-Schnittstelle eine Doppelrolle ein: In Richtung des WLCs agiert die Schnittstelle als Master, in Richtung eines Nachbar-APs hingegen als Slave. Hierzu arbeiten alle APs notwendigerweise auf dem selben Funkkanal. Bei der Erkennung von DFS-Signalen dürfen die APs jedoch nicht mehr auf den entsprechenden Frequenzen senden. Somit kann Seitens der APs keine Meldung an den WLC über die DFS-Erkennung erfolgen und der WLC kann seinerseits keinen Frequenzwechsel für das Netz einleiten. Im Ergebnis sind die betroffenen APs ggf. permanent vom Netz getrennt.

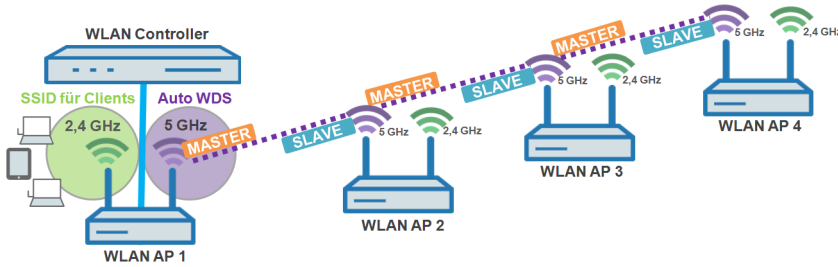


Abbildung 16: Verbindungssperre bei DFS-Erkennung

13.6.2 Funktionsweise

Aufspannen des AutoWDS-Basisnetzes

AutoWDS stellt verschiedene Integrationsmodi bereit, über die das Management von P2P-Strecken zum Errichten vermaschter Netze erfolgen kann. Den Großteil der Konfiguration nehmen Sie auf dem WLC vor, der die einzelnen logischen WLAN-Netze verwaltet. Dazu verknüpfen Sie ein aktives AutoWDS-Profil mit einem eingerichteten WLAN-Profil Ihres gemanagten WLANs. Das AutoWDS-Profil gruppiert die Einstellungen und Grenzwerte für die Gestaltung der P2P-Topologie und des AutoWDS-Basisnetzes.

Das AutoWDS-Basisnetz bzw. die dazugehörige SSID (Vorgabename: **AutoWDS-Rollout**) ist ein reines Managementnetz: Es dient ausschließlich der Authentifizierung eines AP bei der vorkonfigurierten Integration sowie dem Aufbau des WLC-Tunnels für den Konfigurationsaustausch. Auf diese Weise lassen sich hinzukommende APs bei der Integration in das gemanagte WLAN vom operativen Betrieb isolieren. Sobald eine P2P-Verbindung zu einem Master-AP besteht, gilt ein hinzukommender AP als integriert und wickelt die weitere Kommunikation über die Bridge auf Layer 2 ab. Ähnlich wie bei klassischen P2P-Verbindungen spannen die P2P-Partner dazu eine Management-SSID auf, über die sie den Datenverkehr und den CAPWAP-Tunnel zum WLC abwickeln (siehe *Update der AP-Konfiguration und Aufbau der P2P-Strecke* auf Seite 1348).

Hinweis: Für WLAN-Clients wie Smartphones, Laptops, etc. ist das AutoWDS-Basisnetz nicht benutzbar. Für sie muss innerhalb der WLAN-Infrastruktur eine eigene SSID aufgespannt sein.

Nachdem Sie Ihrem gemanagten WLAN ein aktives AutoWDS-Profil zugewiesen haben, spannen die betreffenden (Zugangs-)APs das AutoWDS-Basisnetz auf und senden in ihren Beacons (sofern Sie im AutoWDS-Profil 'SSID-Broadcast' aktiviert haben) und Probe-Responses eine zusätzliche, herstellerspezifische Kennung aus. Diese auch als "AutoWDSInfoFlags" bezeichnete Kennung signalisiert hinzukommenden AutoWDS-fähigen APs die generelle Unterstützung der Funktion und teilt ihnen mit, …

- ob AutoWDS für die erkannte SSID aktiv/inaktiv ist;
- ob der AP der betreffenden SSID eine aktive/inaktive WLC-Verbindung besitzt;
- ob der WLC hinzukommende APs im Express-Modus akzeptiert oder verbietet; und
- ob sich APs für die Integration mit der äquivalenten physikalischen WLAN-Schnittstelle des Zugangs-AP verbinden müssen (strikte Schnittstellen-Paarung, d. h. mit WLAN-1 auf WLAN-1 sowie mit WLAN-2 auf WLAN-2) oder gemischte Schnittstellen-Paarungen erlaubt sind.

Ein gemanagter AP funktioniert automatisch als AutoWDS-AP, sobald er sich einmal initial mit einem WLC per LAN-Kabel gepaart und ein gültiges Zertifikat sowie ein AutoWDS-Profil mit der weiteren AP-Konfiguration korrekt übertragen hat. Ein konfigurierter AutoWDS-AP funktioniert automatisch als hinzukommender AP, sobald eine CAPWAP-Verbindung zu einem WLC nach einer vordefinierten Zeit nicht gelingt, weil z. B. keine kabelgebundene LAN Verbindung existiert. Der betreffende AP wechselt die Betriebsart daraufhin temporär in den **Client**-Modus und scannt solange die einzelnen WLANs, bis er einen geeigneten Zugangs-AP erkennt. Der Scan erfolgt sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzband.

Sofern Ihr Gerät über zwei physikalische WLAN-Schnittstellen verfügt und beide aktiv sind, scannen beide WLAN-Schnittstellen gleichzeitig nach einem geeigneten AutoWDS-Basisnetz. Erkennt eine physikalische WLAN-Schnittstelle eine geeignete SSID, assoziiert sie sich mit dem Zugangs-AP, sofern es die oben erwähnte Schnittstellen-Paarung erlaubt. Die andere physikalische WLAN-Schnittstelle scannt für den Fall weiter, dass die bereits assoziierte physikalische WLAN-Schnittstelle die Verbindung wieder verliert. Die andere physikalische WLAN-Schnittstelle verbindet sich aber bis dahin mit keinem weiteren AutoWDS-Basisnetz. Sobald Ihr Gerät die WLC-Konfiguration erhalten hat, verhalten sich beide physikalischen WLAN-Schnittstellen wie im Profil festgelegt und spannen die Ihnen zugewiesenen SSIDs und das AutoWDS-Basisnetz auf.

Der Ablauf des Suchvorgangs nach einem AutoWDS-Basisnetz ist identisch mit dem der Rekonfiguration bei Verlust der WLAN-Verbindung (siehe *Verlust der Konnektivität und Rekonfiguration* auf Seite 1349).

Unterschiede der Integrationsmodi

Bei der Integration von hinzukommenden APs in Ihr gemanagtes WLAN haben Sie die Wahl zwischen zwei verschiedenen Integrationsmodi. Der Integrationsmodus legt die Bedingungen fest, unter denen Ihr WLC einen hinzukommenden AP akzeptiert:

- Die **vorkonfigurierte Integration** stellt den kontrollierten und bevorzugten Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus gestattet der WLC ausschließlich die Integration von APs, die über eine lokal vorkonfigurierte SSID und gültige WPA2-Passphrase für das AutoWDS-Basisnetz verfügen.

  Der Modus eignet sich für sämtliche Produktivumgebungen und dient dazu, einen vorgegebenen Bezug zwischen einem hinzukommenden AP und einem AutoWDS-Basisnetz herzustellen. Sobald der betreffende AP eine Konfiguration vom WLC erhält, priorisiert der AP diese Konfiguration höher als die lokale AutoWDS-Konfiguration, bis der WLC via CAPWAP die Konfiguration widerruft oder Sie den AP resetten.

- Die **Express-Integration** stellt den schnellen Weg dar, einen hinzukommenden AP über eine Funkstrecke in ein gemanagtes WLAN zu integrieren. In diesem Modus erlaubt der WLC sowohl die Integration vorkonfigurierter Geräte als auch die Integration vollkommen unkonfigurierter Geräte. Unkonfigurierte APs verfügen weder über eine eingetragene SSID noch über eine individuelle WPA2-Passphrase für ein AutoWDS-Basisnetz. Für die Authentifizierung an einem beliebigen AutoWDS-Basisnetz nutzen die Geräte stattdessen einen fest in die Firmware implementierten Pre-Shared-Key.

  Der Modus eignet sich zur einfachen Integration neuer APs in ein gemanagtes WLAN. Die Wahl eines AutoWDS-Basisnetzes geschieht hierbei automatisch und entzieht sich Ihrer Kontrolle. Sobald die betreffenden APs vom WLC eine Konfiguration erhalten, speichern die Geräte die Einstellungen als voreingestellte Werte, bis der WLC via CAPWAP die Konfiguration widerruft, das Gerät nach einem Verbindungsabbruch die Express-*Rekonfiguration* ausführt oder Sie das Gerät resetten.

Wichtig: Achten Sie bei der Express-Integration darauf, dass sich keine anderen AutoWDS-Basisnetze in Reichweite befinden. Andernfalls ist es möglich, dass ein fremder WLC Ihren AP übernimmt und so Ihrem weiteren Fernzugriff entzieht. Ein aktivierter Express-Modus erweitert die Angriffsmöglichkeiten. Deshalb ist es ratsam, den Express-Modus zu deaktivieren, wenn er nicht unbedingt notwendig ist.

Wichtig: Hirschmann empfiehlt aus o. g. Sicherheitsgründen vornehmlich die vorkonfigurierte Integration. Über das Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Mehr dazu erfahren Sie im Abschnitt *Vorkonfigurierte Integration durch Pairing beschleunigen* auf Seite 1357.

Nach erfolgreicher Authentifizierung am AutoWDS-Basisnetz und dem Beziehen einer IP-Adresse scannen die hinzukommenden APs das Netz nach einem WLC. Sobald sie einen WLC erkannt haben, versuchen sie, sich mit ihm zu verbinden und eine Konfiguration zu beziehen. Im LANmonitor erscheinen diese APs als neue Geräte, deren Aufnahme in das gemanagte WLAN der Administrator noch bestätigen und ihnen noch ein WLAN-Profil zuweisen muss. Die Zuweisung unterscheidet sich dabei nicht von der Aufnahme normaler APs. Alternativ kann die Zuweisung durch den WLC erfolgen, wenn Sie

- ein Default-WLAN-Profil eingerichtet und die automatische Zuweisung dessen aktiviert haben; oder
- den betreffenden AP in die Access-Point-Tabelle eingetragen und mit einem WLAN-Profil verknüpft haben.

Wichtig: Durch gleichzeitiges Setzen der automatischen Annahme hinzukommender APs durch den WLC ("Auto Accept") lässt sich die Integration hinzukommender APs automatisieren. Für die Express-Integration sollten Sie diese Einstellung jedoch unbedingt deaktivieren, um ein Mindestmaß an Sicherheit zu erhalten und Rogue-AP-Intrusion zu erschweren.

Hinweis: Der Ablauf der Zertifikatserstellung und die Zertifikatsprüfung sowie die automatische Annahme oder Verweigerung von Verbindungsanfragen

durch den WLC gleichen dem eines WLAN-Szenarios mit kabelgebundenen APs.

Gestaltung der Topologie

Mit der Zuweisung des WLAN-Profils durch den WLC erhalten die Slave-APs gleichzeitig Informationen darüber, wie Ihre P2P-Strecken der Topologie des vermaschten Netzes aufzubauen sind. Die Topologie ergibt sich unmittelbar aus der Hierarchie der unter den APs aufgebauten P2P-Verbindungen. Für deren Gestaltung bietet Ihnen der WLC folgende Management-Modi an:

- **Automatisch**: Der WLC generiert automatisch eine P2P-Konfiguration. Manuell festgelegte P2P-Strecken ignoriert das Gerät.
- **Halb-automatisch**: Der WLC generiert ausschließlich dann eine P2P-Konfiguration, wenn keine manuelle P2P-Konfiguration für den hinzukommenden AP existiert. Andernfalls verwendet der WLC die manuelle Konfiguration.
- **Manuell**: Der WLC generiert selbständig keine P2P-Konfiguration. Wenn eine manuelle P2P-Konfiguration existiert, wird diese verwendet. Andernfalls überträgt der WLC keine P2P-Konfiguration zum AP.

Standardmäßig übernimmt der WLC automatisch die Berechnung der Topologie, bei der sich ein Slave-AP i. d. R. mit dem nächstgelegenen Master-AP verbindet. Die in Echtzeit berechnete Topologie protokolliert der WLC in der Status-Tabelle **AutoWDS-Auto-Topology**. Sofern Sie das halb-automatische oder manuelle Management verwenden, definieren Sie die statischen P2P-Strecken innerhalb der Setup-Tabelle **AutoWDS-Topology**. Dazu legen Sie die Beziehungen zwischen den einzelnen Master-APs und Slave-APs ähnlich einer normalen P2P-Verbindung fest. Mehr dazu finden Sie im Abschnitt *Manuelles Topologie-Mangement* auf Seite 1361.

Hinweis: Die automatische Berechnung einer P2P-Konfiguration (z. B. bei Initial- oder Wiederverbindung eines AP) ersetzt einen in der AutoWDS-Auto-Topology-Tabelle ggf. bereits vorhandenen Eintrag.

Hinweis: Die automatisch generierten Topologie-Einträge sind nicht boot-persistent. Die Tabelle leert sich bei einem Neustart des WLC.

Hinweis: Bei der manuellen Topologie-Konfiguration ist es wichtig, dass sich ein konfigurierter P2P-Master-AP innerhalb der Topologie näher am WLC befindet als ein entsprechender P2P-Slave-AP, da bei einer kurzzeitigen Unterbrechung der P2P-Verbindung der Slave-AP nach dem Master-AP scannt.

Update der AP-Konfiguration und Aufbau der P2P-Strecke

Hat ein hinzukommender AP vom WLC via CAPWAP das WLAN-Profil mit sämtlichen darin enthaltenen Einstellungen empfangen, versucht er, als Slave eine P2P-Strecke zu dem ihm zugewiesenen Master-AP aufzubauen. Bei diesem Prozess wechselt der AP gleichzeitig seine WLAN-Betriebsart von **Client** zurück zu **Managed**.

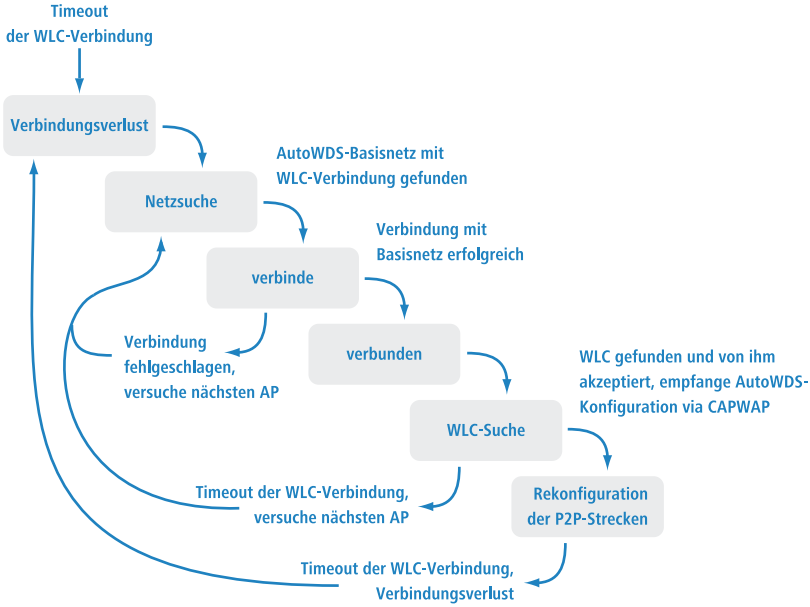
Da der Master-AP bereits im Managed-Modus agiert, erhält er vom WLC via CAPWAP lediglich ein Update seiner P2P-Konfiguration. Diese teilt dem AP neben der WPA2-Passphrase die Peer-Identifikation des AP mit. Bei einer automatisch generierten P2P-Konfiguration entspricht die Peer-Identifikation der MAC-Adresse; bei einer manuellen P2P-Konfiguration dem Namen des Slave-AP. Der Master-AP kennzeichnet derartige SSIDs mit der Kennung ***** P2P Info *****.

Sobald beide APs eine P2P-Verbindung aufgebaut haben, ist der AutoWDS-Integrationsprozess abgeschlossen. Der hinzukommende AP ist dann für Clients (Smartphones, Laptops, andere APs im Client-Modus auf der Suche nach einem Master, etc.) benutzbar.

Hinweis: Solange sich der hinzukommende AP im Client-Modus befindet, ist das Bridging zwischen einer physikalischen WLAN-Schnittstelle und einer LAN-Schnittstelle oder einer anderen physikalischen Funkschnittstelle während des gesamten Integrationsprozesses deaktiviert. Dazu legt das Gerät die physikalischen WLAN-Schnittstellen automatisch auf verschiedene Bridges. Erst nach dem erfolgreichen Aufbau der P2P-Verbindung schaltet der AP das Bridging wieder in den Ursprungszustand zurück.

Verlust der Konnektivität und Rekonfiguration

Sobald Sie AutoWDS auf einem hinzukommenden AP aktivieren, die Anmeldung an einem Zugangs-AP fehlschlägt oder ein eingebundener AP die Verbindung zum WLC verliert, setzt dies einen automatischen (Re-)Konfigurationsprozess in Gang, der gemäß dem abgebildeten Schema verläuft:



Ein AP durchläuft den (Re-)Konfigurationsprozess nicht, wenn er im Client-Modus zwar eine Verbindung zu einem Zugangs-AP, jedoch nicht zum WLC aufbauen kann. Der AP wartet 5 Minuten ab Verbindung zum AutoWDS-Basisnetz, ob der WLC eine Konfiguration des Gerätes durchführt. Erfolgt in dieser Zeit keine Konfiguration (z. B. weil kein Administrator den AP akzeptiert), trennt sich der AP vom AutoWDS-Basisnetz und scannt nach weiteren passenden SSIDs. Ist nur eine SSID in Reichweite, wählt der AP diese erneut für den Integrationsvorgang.

Wichtig: Sofern Verbindung zu einem LAN besteht, versucht der AP während der kompletten Downtime zusätzlich, per Broadcast den WLC über LAN zu erreichen. Findet der AP den WLC via LAN, erfolgt kein Aufsetzen einer

neuen P2P-Strecke und der WLC löscht sämtliche automatisch generierten P2P-Strecken, die den AP als Slave festlegten.

Konfigurations-Timeouts

Sowohl die initiale Konfiguration als auch die Rekonfiguration eines hinzukommenden APs werden durch den Ablauf einzelner Zähler ausgelöst, deren Zusammenspiel das Verhalten des Gerätes steuert. Hierzu gehören, sofern festgelegt:

1. die Zeit für den autarken Weiterbetrieb der P2P-Strecke bei Verlust der CAPWAP-Verbindung (ausschließlich Rekonfiguration);
2. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration; sowie
3. die Wartezeit bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration.

Die Weiterbetriebszeit bezeichnet die Lebensdauer einer jeden P2P-Strecke für den Fall, dass der AP die CAPWAP-Verbindung zum WLC verliert. Erkennt der AP einen Verlust der CAPWAP-Verbindung, versucht er, die Verbindung innerhalb der festgelegten Weiterbetriebszeit wiederherzustellen. Während dieser Zeiten bleiben Verbindungen zu den P2P-Partnern und eingebuchten WLAN-Clients bestehen. Gelingt dem AP die Wiederherstellung nicht und ist die Weiterbetriebszeit abgelaufen, verwirft das Gerät den P2P-Teil der WLC-Konfiguration. Wenn die autarke Weiterbetriebszeit mit `0` festgelegt ist, verwirft der AP den betreffenden Konfigurationsteil sofort.

Anschließend beginnt das Gerät damit, anhand des verbliebenen Konfigurationsteils – der SSID des AutoWDS-Basisnetzes, der dazugehörigen WPA2-Passphrase sowie der Wartezeiten für die vorkonfigurierte und Express-Integration – die eingestellte Zeit bis zum Beginn der automatischen (Re-)Konfiguration für die vorkonfigurierte Integration herabzuzählen. Nach Ablauf dieser Wartezeit schaltet das Gerät seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus um und scannt die verfügbaren SSIDs nach dem zuletzt erkannten AutoWDS-Basisnetz. Parallel dazu beginnt der Zähler bis zum Beginn der automatischen (Re-)Konfiguration für die Express-Integration herabzuzählen.

Hat das Gerät bei Ablauf des Express-Zählers das ihm bekannte AutoWDS-Basisnetz nicht gefunden, stellt das Gerät automatisch auf Express-Integration

um. Anschließend sucht der AP solange nach einem beliebigen AutoWDS-fähigen Netz, bis schließlich ein geeigneter Zugangs-AP erkannt ist.

Durch intelligentes Zusammenspiel der einzelnen Wartezeiten haben Sie die Möglichkeit, das Gerät auf unvorhergesehene Ereignisse flexibel reagieren zu lassen. So lässt sich z. B. eine Fallback-Lösung für den Fall realisieren, dass Sie den Pre-Shared-Key für das AutoWDS-Basisnetz ändern, die Änderung am hinzukommenden AP jedoch fehlschlägt und sich das Gerät aufgrund einer ungültigen Konfiguration nicht mehr erreichen lässt. Bitte beachten Sie dabei die unter *Unterschiede der Integrationsmodi* auf Seite 1345 aufgeführten Hinweise.

Die betreffenden Zähler konfigurieren Sie sowohl auf dem AP (z. B. via LANconfig) als auch auf dem WLC (ausschließlich im Setup-Menü). Auf dem AP werden die Zähler ausschließlich dann beachtet, wenn noch keine WLC-Konfiguration vorliegt (initiale Konfiguration). Sobald eine Konfiguration vorliegt, sind die im AutoWDS-Profil festgelegten Zählerwerte maßgebend (Rekonfiguration). Näheres zur Prioritätensetzung der Konfigurationen finden Sie unter *Unterschiede der Integrationsmodi* auf Seite 1345.

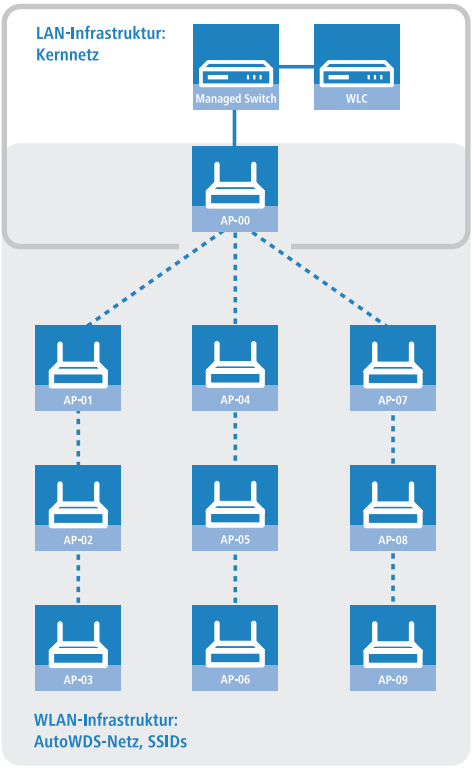
Wichtig: Wenn Sie den Express- oder den Vorkonfigurations-Zähler deaktivieren, überspringt das Gerät den entsprechenden Integrationsschritt. Durch Deaktivieren beider Zähler lässt sich die automatische Rekonfiguration ausschalten. Das Gerät ist dann nach einem entsprechend langen Verbindungsabbruch nicht mehr mittels AutoWDS zu erreichen. Das Gerät bleibt aber über die LAN-Schnittstelle erreichbar und sucht im LAN nach einem WLC, sofern eine entsprechende Verbindung besteht.

Wichtig: Der Prozess zur vorkonfigurierten Integration startet nicht, wenn die Angaben für das AutoWDS-Basisnetz (SSID, Passphrase) unvollständig sind oder der Vorkonfigurations-Zähler bei `0` liegt.

Beispiel: Ausfall eines AP

Die CAPWAP-Verbindung eines jeden AP sichert sich in einem festgelegten Intervall durch Echo-Requests zum WLC ab. Fällt ein AP aus oder ist seine Anbindung gestört, läuft ein solcher Request ins Leere. Erhalten die betreffenden APs nach mehrmaliger Wiederholung des Echo-Requests keine Antwort

des WLC, gilt die CAPWAP-Verbindung als verloren und die betreffenden APs beginnen mit dem unter *Verlust der Konnektivität und Rekonfiguration* auf Seite 1349 beschriebenen Rekonfigurationsprozess.



Für die oben abgebildete Infrastruktur hätte ein Ausfall von AP-01 die nachfolgenden Auswirkungen, sofern das automatische Topologie-Management aktiviert ist:

1. AP-01 ist defekt.
2. AP-02 und AP-03 wiederholen ihre Echo-Requests; alle Wiederholungen schlagen fehl.
3. AP-02 und AP-03 gehen in den autarken Weiterbetrieb (sofern konfiguriert) und versuchen weiterhin, den WLC zu erreichen (sowohl über WLAN als auch LAN, sofern Konnektivität besteht).
4. AP-02 und AP-03 beenden den autarken Weiterbetrieb für die P2P-Verbindungen.

5. AP-02 und AP-03 zählen die Wartezeit für den Beginn der vorkonfigurierten Integration herunter.
6. AP-02 und AP-03 schalten nach Ablauf der Wartezeit in den Client-Modus und scannen das WLAN nach dem letzten bekannten AutoWDS-Basisnetz.
7. AP-02 und AP-03 finden einen neuen Zugangs-AP (z. B. AP-05 oder AP-06) und buchen sich als Client ein.
8. AP-02 und AP-03 stellen über den **WLC-TUNNEL-AUTOWDS** die CAPWAP-Verbindung wieder her und melden dem WLC den neuen Zugangs-AP sowie die verwendeten physikalischen WLAN-Schnittstellen.
9. Der WLC generiert für die betroffenen physikalischen WLAN-Schnittstellen eine P2P-Strecke und übermittelt den APs die Konfiguration via CAPWAP.
10. Die APs setzen die neue P2P-Strecke zu den Ihnen zugewiesenen Master-APs auf und kommunizieren mit dem WLC nicht mehr über den **WLC-TUNNEL-AUTOWDS**, sondern ins LAN gebridged.

13.6.3 Einrichtung mittels vorkonfigurierter Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die vorkonfigurierte Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

In diesem Szenario erweitert ein Unternehmen seine Geschäftsräume um einen weiteren Gebäudekomplex. Das Unternehmen will die neuen Geschäftsräume in sein bestehendes gemanagtes WLAN integrieren. Dazu sollen die betreffenden APs ausschließlich per Funkstrecke verbunden sein. Zwischen Gebäude A (alt) und Gebäude B (neu) ist keine kabelgebundene Netzverbindung erwünscht.

Um die Konfiguration einfach zu halten, konfiguriert das Unternehmen alle APs mit einem einzelnen WLC. Die genaue Anzahl der APs in Gebäude A und Gebäude B ist nebensächlich. Besonderheiten wie mehrere physikalische WLAN-Schnittstellen berücksichtigt der WLC beim Topologie-Management automatisch.

Die Konfiguration selbst gliedert sich in zwei Teile:

1. Konfiguration des WLC in Gebäude A
2. Konfiguration aller APs in Gebäude B

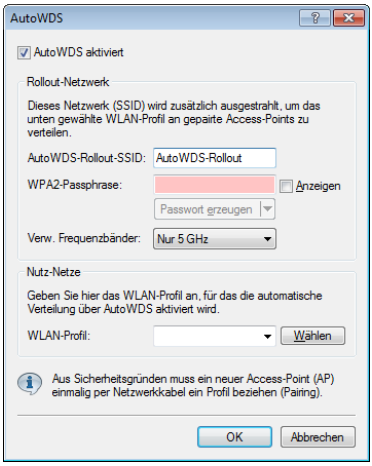
Hinweis: Das Anwendungsbeispiel setzt eine gültige WLAN-Konfiguration mit gültigen Zertifikaten im WLC voraus. Wie Sie ein gemanagtes WLAN einrichten, entnehmen Sie bitte dem Kapitel zum WLAN-Management.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die vorkonfigurierte Integration.

Hinweis: Achten Sie darauf, dass die AutoWDS-APs, die sich als WLAN-Client in das Netzwerk integrieren, über das WLC-TUNNEL-AUTOWDS-Interface einen DHCP-Server erreichen. Ohne IP-Adresse werden die APs nicht nach dem WLC suchen und keine Konfiguration vom WLC erhalten.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **Profile** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **AutoWDS-Rollout-SSID** den Namen des AutoWDS-Basisnetzes ein. Standardmäßig verwendet LANconfig die Bezeichnung `AutoWDS-Rollout`.

Die hier festgelegte SSID agiert als Managementnetz für sämtliche ein AutoWDS-Netz suchenden APs und ist – bis auf die Passphrase – nicht weiter konfigurierbar. Der WLC verbindet die angegebene SSID intern automatisch mit einem WLC-Tunnel (**WLC-TUNNEL-AUTOWDS**). Normale WLAN-Clients sind nicht in der Lage, dieses Managementnetz zu benutzen.

Wichtig: Vergeben Sie hier zweckmäßigerweise eine vom LANconfig-Standard abweichende individuelle AutoWDS-Rollout-SSID.

Hinweis: Die Einrichtung des AutoWDS-Basisnetzes reduziert die Anzahl der SSIDs, die Ihr Gerät über eine physikalische WLAN-Schnittstelle maximal aufspannen kann, um den Wert 1.

4. Geben Sie unter **WPA2-Passphrase** einen Schlüssel ein, mit dem Sie das AutoWDS-Basisnetz absichern.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen.

5. Geben Sie unter **Verw. Frequenzbänder** das Frequenzband an, in dem die APs das AutoWDS-Basisnetz ausstrahlen.
6. Wählen Sie das **WLAN-Profil** aus, dessen SSIDs Sie mittels AutoWDS erweitern wollen.

   Die APs des betreffenden WLAN-Profils fungieren als Zugangs-APs und spannen das AutoWDS-Basisnetz auf. Gleichzeitig erhalten via AutoWDS eingebundene APs dieses WLAN-Profil als Standardkonfiguration, unter der sie nach erfolgreicher Integration die dazugehörige SSID aussenden.

7. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Der WLC weist nun allen gemanagten AutoWDS-fähigen APs in Ihrem WLAN die AutoWDS-Einstellungen zu, woraufhin diese das AutoWDS-Basisnetz aufspannen. Für künftige Rekonfigurationsprozesse verwenden die APs ausschließlich die hier hinterlegte SSID und Passphrase, sofern nicht anders konfiguriert (siehe *Unterschiede der Integrationsmodi* auf Seite 1345).

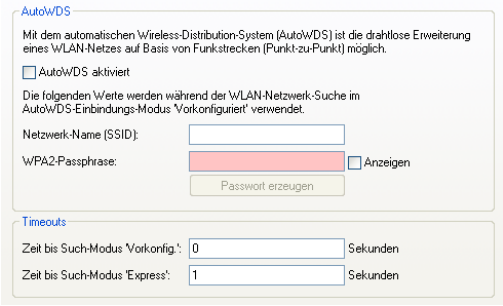
Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die vorkonfigurierte Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

Hinweis: Die Konfiguration eines APs ist nicht notwendig, wenn der AP sich initial bereits mit einem WLC gepaired hat. Die manuelle Eingabe der SSID und der Passphrase ist optional für Geräte, die sich außerhalb der Reichweite des WLC befindet und damit ein Pairing unmöglich ist.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Geben Sie unter **Netzwerk-Name (SSID)** den Namen des AutoWDS-Basisnetzes ein, das Sie auf dem WLC konfiguriert haben (z. B. `AutoWDS-Rollout`).
4. Geben Sie unter **WPA2-Passphrase** den Schlüssel des AutoWDS-Basisnetzes ein, den Sie auf dem WLC konfiguriert haben.
5. Ändern Sie die Timeout-Werte für die **Zeit bis Such-Modus 'Vorkonfig'** auf `1` und die **Zeit bis Such-Modus 'Express'** auf `0`.

6. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
7. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach dem eingetragenen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie im *Kapitel zur Funktionsweise*.

13.6.4 Vorkonfigurierte Integration durch Pairing beschleunigen

Über das einmalige Pairing von WLC und APs haben Sie die Möglichkeit, den Aufwand für die vorkonfigurierte Integration weiter zu reduzieren. Beim Pairing verbinden Sie im Vorfeld einen zurückgesetzten AP via LAN mit dem WLC, auf dem Sie Ihr gemanagtes WLAN inklusive AutoWDS eingerichtet haben. Im zurückgesetzten Zustand befindet sich der AP nach dem Einschalten automatisch im Managed-Modus. Findet der AP den WLC und akzeptiert der WLC den AP, erhält der AP automatisch sämtliche relevanten Zertifikate und Konfigurationsteile, welche die notwendigen Parameter im Gerät konfigurieren. Das Pairing ist dann abgeschlossen. Am Einsatzort installiert ein Mitarbeiter den AP und schaltet ihn ein. Das Gerät sucht dann automatisch nach dem vorkonfigurierten AutoWDS-Basisnetz.

Die nachfolgenden Schritte fassen die Vorgehensweise beim Pairing zusammen. Zusätzlich beinhalten Sie die Schritte zur automatischen Konfigurationszuweisung, um das Pairing bei einer hohen Anzahl von APs weiter zu vereinfachen.

1. Starten Sie LANconfig und richten Sie auf Ihrem WLC ein gemanagtes WLAN mit einem gültigen WLAN-Profil ein, sofern noch nicht geschehen. In LANconfig konfigurieren Sie ein solches Profil unter **WLAN-Controller** > **Profile** > **WLAN-Profile**.
2. Aktivieren Sie für dieses WLAN-Profil die AutoWDS-Funktion, wie im Abschnitt *Konfiguration des WLC* auf Seite 1354 beschrieben.
3. Legen Sie unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** über die Schaltfläche **Default** ein für sämtliche APs allgemein

gültiges Profil an. Weisen Sie diesem Profil dabei das zuvor eingerichtete **WLAN-Profil** zu

4. Aktivieren Sie unter **WLAN-Controller** > **Allgemein** die Option **APs automatisch eine Default-Konfiguration zuweisen**.
5. **Optional:** Um die Annahme hinzukommender APs in LANmonitor nicht manuell zu bestätigen, sondern dies durch den WLC zu automatisieren, aktivieren Sie in dem Dialog zusätzlich die Option **Automatische Annahme neuer APs aktiviert (Auto-Accept)**.

   Wichtig: Aus Sicherheitsgründen sollten Sie diese Option lediglich dann aktivieren, wenn Sie die hinzukommenden APs über eine LAN-Schnittstelle mit dem WLC verbunden haben. Achten Sie darauf, dass keine weiteren Geräte mit dem WLC verbunden sind, um ein mögliches Rogue-AP-Intrusion auszuschließen.

6. Übertragen Sie die Konfiguration zum WLC.
7. Resetten Sie den hinzukommenden AP und schließen Sie das Gerät via LAN an den WLC an.
   Das Gerät beginnt automatisch damit, nach einem WLC zu suchen.
8. Akzeptieren Sie im LANmonitor unter **Wireless LAN** > **Neue APs** den AP, sofern Sie keine automatische Annahme eingerichtet haben.
   Das Gerät erhält daraufhin vom WLC die benötigten Konfigurationsteile für den zukünftigen gemanagten Betrieb. Nach erfolgreicher Konfiguration listet LANmonitor das Gerät im Zweig **Aktive APs**.

Das Pairing ist damit abgeschlossen und der AP für den zukünftigen AutoWDS-Betrieb einsatzbereit.

13.6.5 Einrichtung mittels Express-Integration

Die nachfolgenden Abschnitte zeigen Ihnen, wie Sie ein AutoWDS-Netz über die Express-Integration einrichten. Die Konfiguration verwendet dabei das automatische Topologie-Management des WLC.

Das Ausgangsszenario gleicht dem der *vorkonfigurierten Integration*.

Hinweis: Auf einem zurückgesetzten AP ist AutoWDS standardmäßig deaktiviert, sodass Sie zunächst einen kabelgebundenen Zugriff wählen müssen, um die Funktion zu aktivieren.

Wichtig: Die Express-Konfiguration unterliegt sicherheitsrelevanten Besonderheiten. Lesen Sie sich daher das Kapitel *Unterschiede der Integrationsmodi* auf Seite 1345 aufmerksam durch.

Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines zentralen WLC für die Express-Integration.

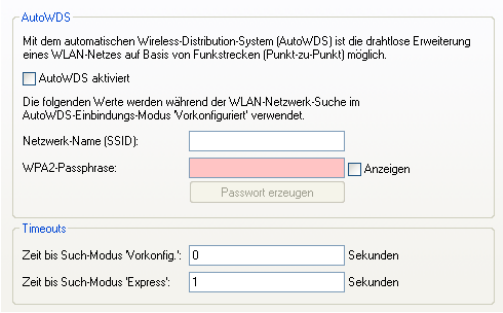
1. Führen Sie die einzelnen Handlungsschritte unter *Konfiguration des WLC* auf Seite 1354 für die vorkonfigurierte Integration aus.
2. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
3. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
4. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
5. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **ja** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Die Konfiguration des WLC ist damit abgeschlossen. Fahren Sie nun mit der Konfiguration der APs fort.

Konfiguration der APs

Die nachfolgenden Handlungsanweisungen beschreiben die AutoWDS-Konfiguration eines AP für die Express-Integration. Die Konfigurationsschritte sind für sämtliche hinzukommenden APs identisch.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **Wireless-LAN** > **AutoWDS**, um zum AutoWDS-Einstellungsfenster zu gelangen.



2. Klicken Sie **AutoWDS aktiviert**, um die Funktion auf dem Gerät generell zu aktivieren.
3. Stellen Sie unter **Wireless LAN** > **Allgemein** > **Physikalische WLAN-Einst.** sicher, dass sich mindestens eine physikalische WLAN-Schnittstelle in der Betriebsart **Managed** befindet.
   Andernfalls sucht das Gerät zu keiner Zeit nach einem AutoWDS-Basisnetz.
4. Schließen Sie das Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.

Nach erfolgreichem Konfigurations-Update schaltet der AP seine physikalische(n) WLAN-Schnittstelle(n) in den Client-Modus und sucht nach einem beliebigen AutoWDS-Basisnetz. Weitere Informationen zum Ablauf erhalten Sie unter *Aufspannen des AutoWDS-Basisnetzes* auf Seite 1343.

13.6.6 Umschalten von Express- zu vorkonfigurierter Integration

Um nach einem Netz-Rollout mittels Express-Integration auf eine vorkonfigurierte Integration umzuschalten, deaktivieren Sie die Express-Integration auf dem WLC. Ein gezieltes Umschalten der APs entfällt, da die APs im Rahmen der Express-Integration bereits eine AutoWDS-Konfiguration erhalten haben, die ein AutoWDS-Netz für spätere Rekonfigurationsprozesse vorkonfiguriert.

1. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
2. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
3. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.

4. Ändern Sie den Parameter **Erlaube-Express-Integration** auf **nein** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.

Damit haben Sie die Express-Integration für weitere hinzukommende APs deaktiviert.

13.6.7 Manuelles Topologie-Mangement

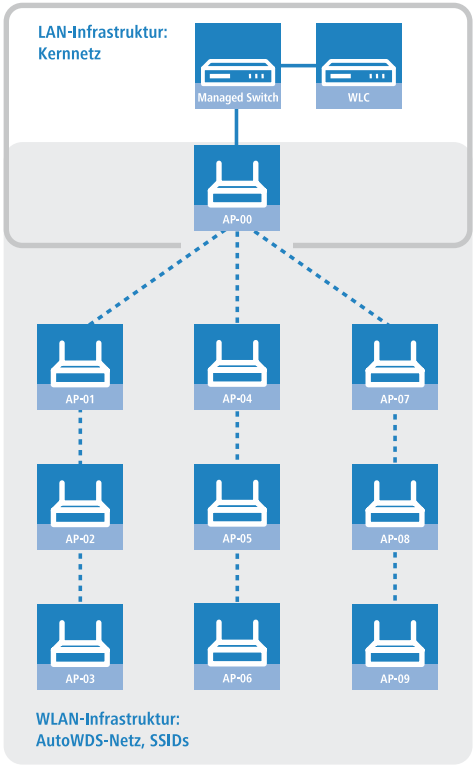
Die Einrichtungsbeispiele für AutoWDS verfolgen das automatische Topologie-Management durch den WLC, um die Konfiguration zu vereinfachen. Je nach Einsatzszenario kann es jedoch erforderlich sein, einzelne oder sämtliche P2P-Strecken manuell zu definieren.

Der nachfolgende Abschnitt zeigt Ihnen, wie Sie das automatische Topologie-Management auf dem WLC deaktivieren und eine manuelle P2P-Konfiguration anlegen. Für die Konfiguration der P2P-Strecken ordnen Sie den APs zunächst eindeutige Namen zu, die Sie anschließend mit der Topologiekonfiguration und den verwendeten physikalischen WLAN-Schnittstellen verknüpfen. Das Kapitel geht davon aus, dass Sie die unter *Einrichtung mittels vorkonfigurierter Integration* auf Seite 1353 beschriebenen Schritte für den WLC bereits ausgeführt haben, um die Basis-Konfiguration abzuschließen und AutoWDS auf dem WLC generell zu aktivieren.

Hinweis: Generell ist ein AutoWDS-Betrieb von bis zu maximal 3 Hops empfehlenswert.

Änderungen am Ausgangsszenario

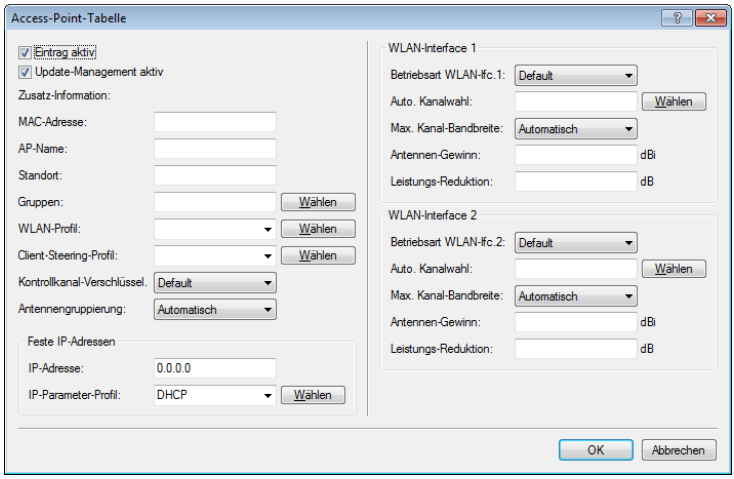
Das Ausgangsszenario gleicht dem der vorkonfigurierten Integration. Für die gesamte WLAN-Infrastruktur kommen ausschließlich Dual-Radio-APs zum Einsatz, die entsprechend der untenstehenden Grafik angeordnet sind. Das gemanagte WLAN besteht zu Beginn aus einem einzigen AP, der den hinzukommenden APs als initialer Zugangs-AP dient.



Konfiguration des WLC

Die nachfolgenden Handlungsanweisungen beschreiben die Deaktivierung des automatischen Topologie-Managements und die Konfiguration manueller P2P-Strecken gemäß des unter *Manuelles Topologie-Mangement* auf Seite 1361 beschriebenen Szenarios.

1. Öffnen Sie den Konfigurationsdialog in LANconfig und klicken Sie **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle**, um zur Liste der verwalteten APs zu gelangen.



2. Geben Sie für jeden hinzukommenden AP die **MAC-Adresse** und unter **AP-Name** einen eindeutigen Namen an. Auf diesen Namen referenzieren Sie später in der Topologie-Konfiguration.

Für das Beispielszenario lauten die einzelnen Konfigurationseinträge wie folgt:

Eintrag	*MAC-Adresse*	*AP-Name*
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08

Eintrag	*MAC-Adresse*	*AP-Name*
10	00-a0-57-33-e1-05	AP-09

Tabelle 26: Konfiguration der hinzukommenden APs in der Access-Point-Tabelle

Hinweis: Der Tabelleneintrag AP-00 bezieht sich auf Ihren bereits vorhandenen AP, welchen die hinzukommenden APs als Zugangs-AP nutzen.

3. Wählen Sie das **WLAN-Profil** aus, für das Sie AutoWDS aktiviert haben. Über das betreffende WLAN-Profil erhalten die APs automatisch die Einstellungen für AutoWDS und damit auch die P2P-Konfiguration zugewiesen.
4. Schließen Sie die geöffneten Dialogfenster mit **OK** und schreiben Sie die Konfiguration zurück auf das Gerät.
5. Melden Sie sich über WEBconfig oder die Konsole an Ihrem Gerät an.
6. Wechseln Sie innerhalb des Setup-Menüs in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Profile**.
7. Klicken Sie auf den Eintrag **DEFAULT**, um das AutoWDS-Standardprofil zu bearbeiten.
8. Ändern Sie den Parameter **Topology-Management** auf **Manuell** und speichern Sie die Einstellung mit einem Klick auf **Setzen**.
9. Wechseln Sie in die Tabelle **WLAN-Management** > **AP-Konfiguration** > **AutoWDS-Topology** und klicken Sie **Hinzufügen**.
10. Legen Sie für jedes P2P-Paar eine manuelle P2P-Konfiguration an. Die festgelegte P2P-Strecke gilt stets aus Sicht des Slave-AP.
    a) Geben Sie im Feld **AutoWDS-Profil** das AutoWDS-Profil an, für das die manuelle P2P-Konfiguration gilt, z. B. `DEFAULT`.
    b) Setzen Sie die **Priorität** der P2P-Konfiguration auf `0` (höchste Priorität).
    c) Geben Sie für **Slave-AP-Name** und **Master-AP-Name** den Namen der APs entsprechend der von Ihnen gewählten Hierarchie ein.

    Für das Beispielszenario lauten die einzelnen Konfigurationseinträge bei strikter Schnittstellen-Paarung wie folgt:

Eintrag	*Slave-AP-Name*	*Slave-AP-WLAN-Ifc.*	*Master-AP-Name*	*Master-AP-WLAN-Ifc.*
01	AP-01	WLAN-1	AP-00	WLAN-1

Eintrag	*Slave-AP-Name*	*Slave-AP-WLAN-Ifc.*	*Master-AP-Name*	*Master-AP-WLAN-Ifc.*
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

Tabelle 27: Konfiguration der P2P-Paare in der AutoWDS-Topology-Tabelle

d) Geben Sie unter **Schluessel** die WPA2-Passphrase an, mit der die P2P-Partner die P2P-Strecke verschlüsseln.

   Wählen Sie dazu einen möglichst komplexen Schlüssel mit mindestens 8 und maximal 63 Zeichen. Für eine angemessene Verschlüsselung sollte der Schlüssel mindestens 32 Zeichen umfassen. Wenn Sie das Eingabefeld leer lassen, erzeugt das Gerät automatisch eine Passphrase mit einer Länge von 32 Zeichen.

e) Schalten Sie den Eintrag **Aktiv** auf **Ja**.
f) Speichern Sie den jeweiligen Eintrag mit einem Klick auf **Setzen**.

Waren bereits APs angeschlossen, übermittelt der WLC die neue Konfiguration an die APs und löst damit einen Rekonfigurationsprozess auf diesen aus. Waren noch keine APs angeschlossen, überträgt der WLC die P2P-Konfiguration beim ersten Verbindungsaufbau der hinzukommenden APs.

13.6.8 Redundante Strecken mittels RSTP

Das manuelle Topologie-Management eröffnet Ihnen in Kombination mit dem Rapid Spanning Tree Protocol (RSTP) die Möglichkeit, redundante P2P-Strecken einzurichten, um die Ausfallsicherheit Ihres gesamten AutoWDS-Basisnetzes zu verbessern. Hierzu müssen Sie RSTP zunächst im Setup-Menü eines jeden APs aktivieren, da sich die Management-Einstellungen des WLC nicht auf diesen Konfigurationsteil erstrecken. Um den Konfigurations-

aufwand zu reduzieren, ist der Einsatz eines Skripts empfehlenswert, welches Sie über das Skript-Management des WLC an sämtliche APs übertragen.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie dabei vorgehen. Die Schritte implizieren, dass Sie ein AutoWDS-Basisnetz bereits erfolgreich eingerichtet haben. Nach seiner Aktivierung führt RSTP die Pfadsuche vollautomatisch durch.

1. Erstellen Sie eine Textdatei mit dem Namen `WLC_Script_1.lcs`.
2. Kopieren die folgenden Codezeilen in die Textdatei und speichern Sie.

```
# Script (9.000.0000 / 15.07.2014)

lang English
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version        Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation   Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating               yes

flash Yes

# done
exit
```

3. Melden Sie sich an der WEBconfig-Oberfläche Ihres WLCs an und wählen Sie **Dateimanagement** > **Zertifikat oder Datei hochladen**.
4. Wählen Sie in der Auswahlliste **Dateityp** den Eintrag **CAPWAP - WLC_Script_1.lcs** und über die Schaltfläche **Durchsuchen** die zuvor angelegte Skriptdatei aus. Klicken Sie anschließend auf **Upload starten**. Den erfolgreichen Upload des Skripts in den WLC prüfen Sie z. B. über das Status-Menü unter **Dateisystem** > **Inhalt**.
5. Wechsel Sie im Setup-Menü zum Menüpunkt **WLAN-Management** > **Zentrales-Firmware-Management** > **Skriptverwaltung** und klicken Sie **Hinzufügen**.
6. Geben Sie als **Profil** Ihr entsprechendes WLAN-Profil an und als **Name** `WLC_Script_1.lcs` ein, um das AutoWDS-Profil mit dem Skriptnamen zu verbinden und an die APs auszurollen.
7. Weisen Sie – wie in Kapitel *Konfiguration des WLC* auf Seite 1362 beschrieben – den APs im WLC eindeutige Namen zu und richten Sie die manuellen P2P-Strecken ein.

Damit haben Sie die Konfiguration erfolgreich abgeschlossen.

13.7 Wireless-IDS – Erkennung von Angriffen auf Ihre Wireless-Infrastruktur

Informationen zum Thema "Wireless-IDS" finden Sie im Kapitel *Wireless-IDS* auf Seite 1223.

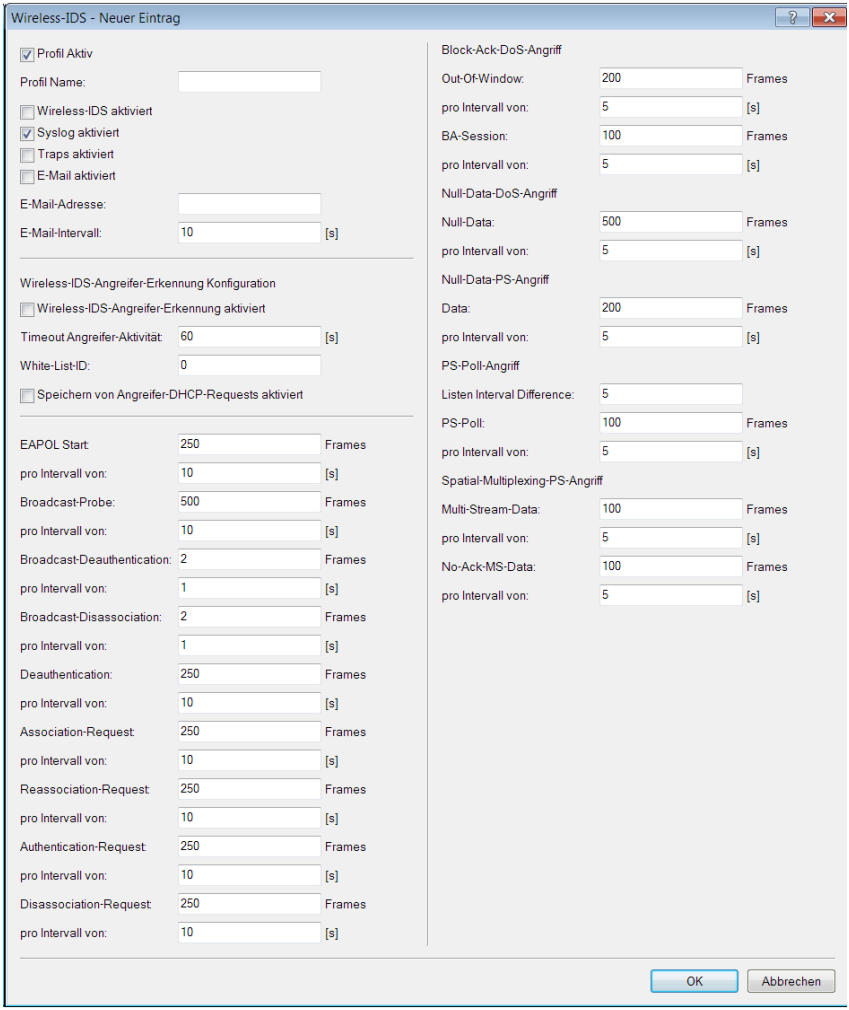
13.7.1 Tutorial: Konfiguration des Wireless-IDS mit dem WLAN-Controller

Die voreingestellten Grenzwerte sind Richtwerte, die für Ihren Anwendungsfall ungeeignet sein können. Die Grenzwerte für Ihren Anwendungsfall hängen von den Umgebungsbedingungen Ihres APs ab. Führen Sie daher zuerst eine Referenzmessung mittels eines Testlaufs des Wireless-IDS am Einsatzort Ihres WLANs durch.

Zusätzliche Referenzwerte erhalten Sie durch Mitschnitte mittels eines kostenfreien Programms wie beispielsweise Wireshark. Für das Abhören des Funkverkehrs und das Speichern sowie das Verarbeiten der daraus gewonnenen Daten benötigen Sie in vielen Ländern die Erlaubnis der Regulierungsbehörde. Das unerlaubte Mitschneiden und das unerlaubte Speichern der Daten sowie deren Weitergabe steht in vielen Ländern unter Strafe.

Um das Wireless-IDS mit dem WLAN-Controller zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Ansicht **WLAN-Controller** > **Profile** > **Wireless-IDS** > **Hinzufügen**.



2. Geben Sie unter **Profil Name** einen Namen für das Wireless-IDS-Profil ein.
3. Aktivieren Sie die Option **Wireless-IDS aktiviert**.

Hinweis: Wenn Sie Wireless-IDS über den WLC aktivieren, werden lokale Wireless-IDS-Konfigurationen auf den APs überschrieben. Direkte

Konfigurationen des Wireless-IDS auf vom WLC gesteuerten APs werden verworfen und führen zu einer Fehlermeldung.

4. Wählen Sie die gewünschte Art der Protokollierung. Wireless-IDS protokolliert per Default im **Syslog**. Um Wireless-IDS über Traps zu protokollieren, aktivieren Sie die Option **Traps aktiviert**.

   Hinweis: Die spezifischen Einstellungen für SNMP-Traps können mit dem WLC-Controller nicht direkt vorgenommen, sondern müssen mit einem zusätzlichen Skript auf die APs ausgerollt werden. Weitere Infos zu Skripten finden Sie im Abschnitt *Skript-Management-Tabelle* auf Seite 1374.

5. Um E-Mail-Benachrichtigungen zu erhalten, aktivieren Sie die Option **E-Mail aktiviert** und geben Sie die gewünschte E-Mail-Adresse ein.

   Hinweis: Die spezifischen Einstellungen für das nötige SMTP-Konto können mit dem WLC-Controller nicht direkt vorgenommen, sondern müssen mit einem zusätzlichen Skript auf die APs ausgerollt werden. Weitere Infos zu Skripten finden Sie im Abschnitt *Skript-Management-Tabelle* auf Seite 1374.

6. Um Informationen über den Angreifer zu erhalten, aktivieren Sie die Option **Wireless-IDS-Angreifer-Erkennung aktiviert**.

   Hinweis: Wenn Sie die Wireless-IDS-Angreifer-Erkennung über den WLC aktivieren, werden lokale Wireless-IDS-Angreifer-Erkennungs-Konfigurationen auf den APs überschrieben. Direkte Konfigurationen der Wireless-IDS-Angreifer-Erkennung auf vom WLC gesteuerten APs werden verworfen und führen zu einer Fehlermeldung..

7. Setzen Sie den **Timeout Angreifer-Aktivität**.
8. Um Stationen von der Angreifer-Erkennung auszunehmen, legen Sie eine **White-List-ID** für das Wireless-IDS-Profil fest.
9. Um Informationen über die Angreifer-DHCP-Requests zu erhalten, aktivieren Sie die Option **Speichern von Angreifer-DHCP-Requests aktiviert**.

10. Setzen Sie die Grenzwerte für die Frames und die Intervalle entsprechend Ihrer Referenzmessung.
11. Klicken Sie die Schaltfläche **OK**.
12. Um Stationen von der Angreifer-Erkennung auszunehmen, wechseln Sie in die Ansicht **WLAN-Controller** > **Profile** > **White-List-Tabelle** und fügen Sie die gewünschten Stationen hinzu. Gruppieren Sie die auszunehmenden Stationen mittels der White-List-ID (siehe Punkt 8. dieses Tutorials) in White-Listen für das jeweilige Wireless-IDS-Profil.
13. Wechseln Sie in die Ansicht **WLAN-Controller** > **Profile** > **WLAN-Profile**.
14. Fügen Sie im zugehörigen WLAN-Profil das **Wireless-IDS-Profil** hinzu.
15. Klicken Sie die Schaltfläche **OK**.

Sie haben das Wireless-IDS aktiviert und konfiguriert.

13.8 Zentrales Firmware- und Skript-Management

Mit einem WLC kann die Konfiguration von mehreren APs von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

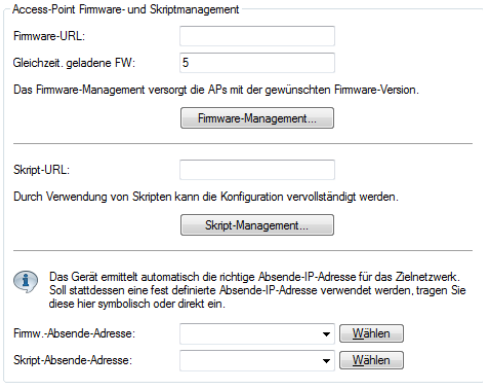
Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLC prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion den Bestand und vergleicht die verfügbaren Dateien mit den Versionen in den Geräten – alternativ kann dieser Vorgang auch über einen Cron-Job z. B. nachts erledigt werden. Wenn ein Update durchgeführt werden kann oder nicht die gewünschte Version auf dem AP läuft, lädt der WLC diese vom Webserver herunter und spielt sie in die entsprechenden APs ein.

Mit der Konfiguration des Firmware- und Skript-Managements kann die Distribution der Dateien gezielt gesteuert werden. So kann die Nutzung von bestimmten Firmware-Versionen z. B. auf bestimmte Gerätetypen oder MAC-Adressen beschränkt werden.

Das Update kann in zwei möglichen Zuständen ausgeführt werden:

- Beim Verbindungsaufbau, danach startet der AP automatisch neu.

- Wenn der AP schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der AP manuell über die Menüaktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisierte-APs-neustarten** oder zeitgesteuert per Cron-Job neu gestartet.
- Mit der Aktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisiere-Firmware-und-Skript-Information** können Skript- und Firmwareverzeichnisse aktualisiert werden.



Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **WLAN-Controller** > **AP-Update**

WEBconfig: **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management**

13.8.1 Allgemeine Einstellungen für das Firmware-Management

- **Firmware-URL**

  Pfad zum Verzeichnis mit den Firmware-Dateien.

  - Mögliche Werte: URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`
  - Default: leer

- **Gleichzeitig geladene FW**

Anzahl der gleichzeitig im Arbeitsspeicher des WLCs vorgehaltenen Firmware-Versionen.

Hinweis: Die hier vorgehaltenen Fimrware-Versionen werden nur einmal vom Server geladen und anschließend für alle passenden Update-Prozesse genutzt.

- Mögliche Werte: 1 bis 10
- Default: 5

▶ **Firmware-Absende-IP-Adresse**

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

Mögliche Werte:

- Name eines definierten IP-Netzwerks.
- 'INT' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
- 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- Name einer Loopback-Adresse.
- Beliebige andere IP-Adresse.

Default:

- leer

Hinweis: Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'INT' oder 'DMZ' vorhanden ist, wird die IP-Adresse des IP-Netzwerks bzw. der Loopback-Adresse mit dem Namen 'INT' bzw. 'DMZ' verwendet.

Firmware-Management-Tabelle

In dieser Tabelle wird hinterlegt, welche Geräte (MAC-Adresse) und Gerätetypen mit welcher Firmware betrieben werden sollen.

Gerätetypen

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Alle oder Auswahl aus der Liste der verfügbaren Gerätetypen.
- Default: Alle

MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Gültige MAC-Adresse.
- Default: Leer

Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll.

- Mögliche Werte: Firmware-Version in der Form `X.XX`
- Default: Leer

Datum

Das Datum ermöglicht ein Downgrade auf eine spezifische Firmware-Version innerhalb einer Release, z. B. von einem Release-Upgrade (RU) auf ein früheres Upgrade.

- Mögliche Werte: 8 Zeichen aus 0123456789. Der Eintrag muss dem Format des UPX-Headers entsprechen, also z. B. "01092014" für den 01.09.2014.
- Default: Leer

Allgemeine Einstellungen für das Skript-Management

- **Skript-URL**

  Pfad zum Verzeichnis mit den Skript-Dateien.

  - Mögliche Werte: URL in der Form `Server/Verzeichnis` oder `http://Server/Verzeichnis`
  - Default: Leer

- **Skript-Absende-IP-Adresse**

  Hier können Sie optional eine Absendeadresse konfigurieren, die statt der automatisch für die Zieladresse gewählten Absendeadresse verwendet wird.

  Mögliche Werte:

  - Name eines definierten IP-Netzwerks.
  - 'INT' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.
  - 'DMZ' für die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
  - Name einer Loopback-Adresse.
  - Beliebige andere IP-Adresse.

  Default:

  - leer

  Hinweis: Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'INT' oder 'DMZ' vorhanden ist, wird die IP-Adresse des IP-Netzwerks bzw. der Loopback-Adresse mit dem Namen 'INT' bzw. 'DMZ' verwendet.

Skript-Management-Tabelle

In dieser Tabelle werden Skripte anhand ihres Dateinamens einem WLAN-Profil zugeordnet.

Die Konfiguration eines APs in der Betriebsart "Managed" erfolgt über WLAN-Profile. Mit einem Skript können auch diejenigen Detail-Parameter der gemanagten Geräte eingestellt werden, die nicht im Rahmen der vorgegebenen Parameter eines WLAN-Profils verwaltet werden. Dabei erfolgt die Zuordnung ebenfalls über die WLAN-Profile, um für die APs mit gleicher WLC-Konfiguration auch das gleiche Skript zu verwenden.

Da für jedes WLAN-Profil nur eine Skript-Datei angegeben werden kann, ist hier keine Versionierung möglich. Bei der Zuweisung eines Skripts zu einem AP wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLC bei einer neuen oder geänderten Skript-Datei mit gleichem Dateinamen feststellen, ob die Skript-Datei erneut übertragen werden muss.

- **Skript-Dateiname**

  Name der zu verwendenen Skript-Datei.

  - Mögliche Werte: Dateiname in der Form *.lcs
  - Default: leer

- **WLAN-Profil**

  Wählen Sie hier aus, für welches WLAN-Profil die in diesem Eintrag spezifizierte Skript-Datei verwendet werden soll.

  - Mögliche Werte: Auswahl aus der Liste der definierten WLAN-Profile.
  - Default: Leer

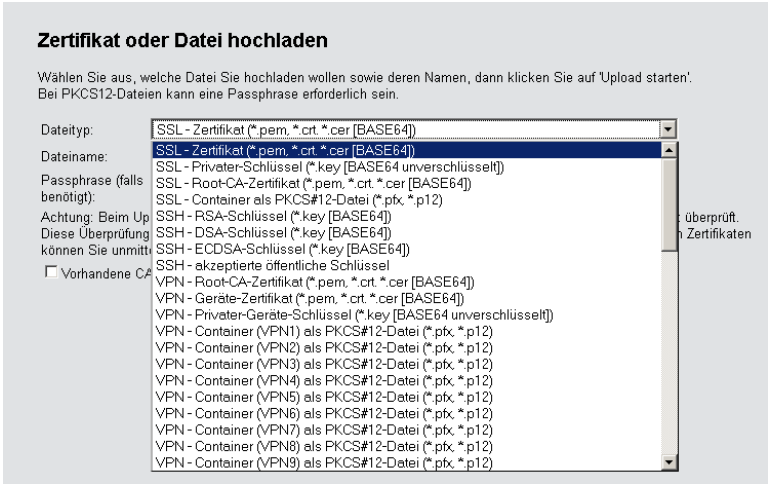
Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLCs können drei Skripte mit maximal je 64kB Größe gespeichert werden. Wenn der Bedarf für Skripte nicht über dieses Volumen hinausgeht, kann die Einrichtung eines HTTP-Servers für diesen Zweck entfallen.

Die Skript-Dateien werden dazu einfach über WEBconfig auf den vorgesehenen Speicherplatz geladen. Nach dem Upload muss die Liste der verfügbaren Skripte mit der Aktion **Setup** > **WLAN-Management** > **Zentrales-Firmware-Management** > **Aktualisiere-Firmware-und-Skript-Information** aktualisiert werden.

Aus der Skript-Management-Tabelle können diese internen Skripte den entsprechenden Namen referenziert werden (WLC_Script_1.lcs, WLC_Script_2.lcs oder WLC_Script_3.lcs).

Hinweis: Bitte beachten Sie bei der Angabe der Script-Namen die Groß- und Kleinschreibung!

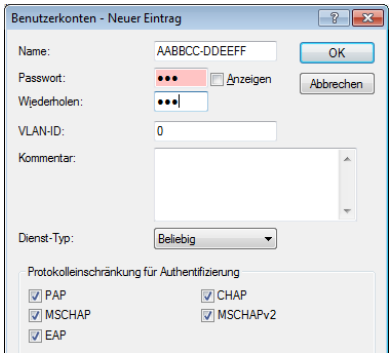


13.9 RADIUS

13.9.1 Prüfung der WLAN-Clients über RADIUS (MAC-Filter)

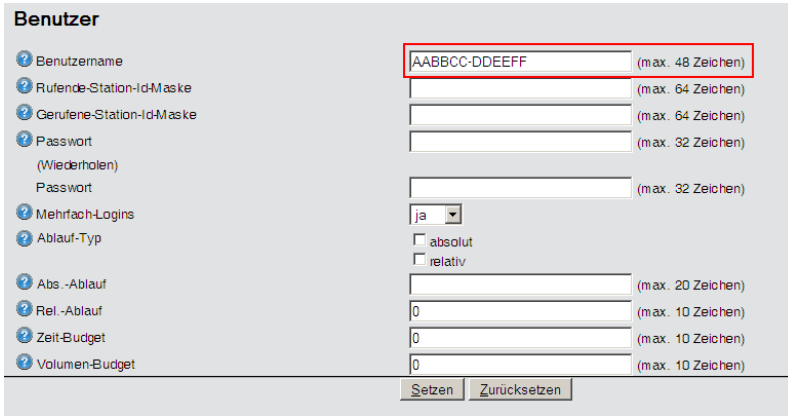
Bei der Nutzung von RADIUS zur Authentifizierung der WLAN-Clients kann neben einem externen RADIUS-Server auch die interne Benutzertabelle der WLC genutzt werden, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank im Konfigurationsbereich **RADIUS-Server** auf der Registerkarte **Allgemein** ein. Verwenden Sie dabei die MAC-Adresse als **Name** und ebenso als **Passwort** und wählen Sie als Authentifizierungsmethode **Alle**.



Alternativ tragen Sie die zugelassenen MAC-Adressen über WEBconfig ein unter **HiLCOS-Menübaum** > **Setup** > **RADIUS** > **Server** > **Benutzer**.

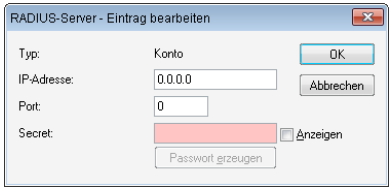
Hinweis: Als **Benutzername und Passwort** wird jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF' eingetragen.



13.9.2 Externer RADIUS-Server

Standardmäßig übernimmt der WLC die Weiterleitung von Anfragen für die Konto- bzw. Zugangsverwaltung an einen RADIUS-Server. Damit die APs den RADIUS-Server direkt ansprechen können, müssen entsprechenden Server-Informationen hier definiert werden. Somit funktioniert die RADIUS-Anwendung auch dann noch, wenn der WLC nicht erreichbar ist. Allerdings

müssen dafür Einstellungen für jeden einzelnen AP im adressierten RADIUS-Server vorgenommen werden und die managed APs müssen den RADIUS-Server aus ihrem Management-Netz heraus erreichen können. Ist der RADIUS-Server in einem anderen IP-Netz, muss über das IP-Parameter-Profil insbesondere das Gateway definiert werden.



LANconfig: **WLAN Controller** > **Stationen** > **RADIUS-Server**

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN Management** > **RADIUS-Server**

- **Typ**: Type der RADIUS Anwendung.

  Mögliche Werte:

  Konto oder Zugang

  Default:

  Die Einträge Konto, Zugang, Backup-Konto und Backup-Zugang sind fest eingestellt und können nicht verändert werden.

- **IP-Adresse**: IP-Adresse des Radius Servers, die den AP mitgeteilt wird, um den RADIUS-Server zu erreichen. Wird hier kein Wert angegeben, wird automatisch die IP-Adresse des Controllers genommen.

  Mögliche Werte:

  Gültige IP-Adresse.

  Default:

  leer

- **Port**: Port-Nummer, die den AP mitgeteilt wird, um den RADIUS Server zu erreichen. Der Port muss mit dem im RADIUS-Server konfigurierten Wert übereinstimmen. Dieser Wert wird ignoriert, wenn keine IP-Adresse konfiguriert ist, da dann der WLC selbst als RADIUS-Server benutzt wird.

  Mögliche Werte:

Gültige Port-Nummer, im Allgemeinen 1812 für Zugangs- und 1813 für Kontoverwaltung.

Default:

0

- **Secret**: Passwort für den RADIUS Dienst. Der Schlüssel (Secret) muss mit dem im RADIUS-Server konfigurierten Wert übereinstimmen. Dieser Wert wird ignoriert, wenn keine IP-Adresse konfiguriert ist, da dann der WLC selbst als RADIUS-Server benutzt wird.

  Mögliche Werte:

  max. 31 ASCII-Zeichen.

  Default:

  leer

13.9.3 Dynamische VLAN-Zuweisung

In einer größeren WLAN-Struktur ist es oft sinnvoll, den einzelnen WLAN-Clients ein bestimmtes Netzwerk zuzuweisen. Solange sich die WLAN-Clients immer in der Reichweite des gleichen APs befinden, kann diese Zuweisung über die SSID in Verbindung mit einem bestimmten IP-Netzwerk realisiert werden. Wechseln die WLAN-Clients hingegen häufig die Position und buchen sich dann bei unterschiedlichen APs ein, befinden sie sich je nach Konfiguration in einem anderen IP-Netzwerk.

Um die WLAN-Clients **unabhängig** von dem WLAN-Netzwerk, in dem sie sich gerade eingebucht haben, in ein bestimmtes Netzwerk zu leiten, können dynamisch zugewiesene VLANs genutzt werden. Anders als bei den statisch konfigurierten VLAN-IDs für eine bestimmte SSID wird die VLAN-ID dabei dem WLAN-Client von einem RADIUS-Server direkt zugewiesen.

Beispiel:

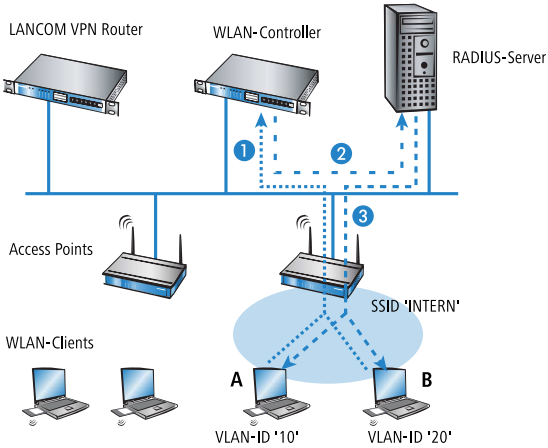
- Die WLAN-Clients der Mitarbeiter buchen sich über einen AP in das WPA2-gesicherte WLAN mit der SSID 'INTERN' ein. Bei der Anmeldung werden die RADIUS-Anfragen der WLAN-Clients an den AP gestellt. Wenn sich das entsprechende WLAN-Interface in der Betriebsart 'Managed' befindet, werden die RADIUS-Anfragen automatisch an den WLC weitergereicht. Dieser leitet die Anfragen seinerseits an den konfigurierten RADIUS-Server

weiter. Der RADIUS-Server kann die Zugangsberechtigung der WLAN-Clients prüfen. Darüber hinaus kann er allerdings auch z. B. anhand der MAC-Adresse eine bestimmte VLAN-ID für die jeweilige Abteilung zuweisen. Dabei erhält z. B. der WLAN-Client aus dem Marketing die VLAN-ID '10' und WLAN-Client aus der Entwicklung die '20'. Wenn für den Benutzer keine VLAN-ID definiert ist, wird die Haupt-VLAN-ID der SSID verwendet.

- Die WLAN-Clients der Gäste buchen sich über den gleichen AP in das nicht gesicherte WLAN mit der SSID 'PUBLIC' ein. Diese SSID ist statisch auf die VLAN-ID '99' gebunden und leitet die Gäste so in einen bestimmtes Netzwerk. Statische und dynamische VLAN-Zuweisung können also sehr elegant parallel genutzt werden.

Hinweis: Die Zuweisung der VLAN-ID kann im RADIUS-Server auch anhand von anderen Kriterien erfolgen, z. B. über die Kombination aus Benutzername und Kennwort. Auf diese Weise kann z. B. den unbekannten MAC-Adressen der Besucher in einer Firma eine VLAN-ID zugewiesen werden, die für den Gastzugang z. B. nur die Internetnutzung erlaubt, jedoch keinen Zugang zu anderen Netzwerkressourcen.

Hinweis: Alternativ zu einem externen RADIUS-Server kann den WLAN-Clients auch über den internen RADIUS-Server oder die Stationstabelle im WLC eine VLAN-ID zugewiesen werden.



1. Aktivieren Sie das VLAN-Tagging für den WLC. Tragen Sie dazu als Management-VLAN-ID in den physikalischen Parametern des Profils einen Wert größer als '0' ein.
2. Für eine Authentifizierung über 802.1x wählen Sie in den Verschlüsselungseinstellungen für das logische WLAN-Netzwerk des Profils eine Einstellung, die eine Authentifizierungsanfrage auslöst.
3. Für eine Prüfung der MAC-Adressen aktivieren Sie für das logische WLAN-Netzwerk des Profils die MAC-Prüfung.

   Hinweis: Sowohl für die Authentifizierung über 802.1x als auch für die Prüfung der MAC-Adressen ist bei der Verwaltung von WLAN-Modulen über einen WLC ein RADIUS-Server erforderlich. Der WLC trägt sich dabei automatisch in den von ihm verwalteten APs als RADIUS-Server ein – alle RADIUS-Anfragen an die APs werden daher direkt an den WLC weitergeleitet, der die Anfragen entweder selbst bearbeiten oder sie alternativ an einen externen RADIUS-Server weiterleiten kann.

4. Für eine Weiterleitung der RADIUS-Anfragen an einen anderen RADIUS-Server tragen Sie dessen Adresse über LANconfig in die Liste der Forwarding-Server im Konfigurationsbereich 'RADIUS-Server' auf der Registerkarte **Forwarding** ein. Alternativ tragen Sie die externen RADIUS-Server über WEBconfig ein unter **Menübaum** > **HiLCOS-Setup** > **RADIUS** > **Server** > **Weiterleit-Server**. Stellen Sie außerdem den Standard-Realm sowie den leeren Realm ein, um auf unterschiedliche Benutzerinformationen (mit unbekanntem oder ganz ohne Realm) gezielt reagieren zu können.
5. Konfigurieren Sie die Einträge im RADIUS-Server entsprechend, damit den anfragenden WLAN-Clients anhand bestimmter Merkmale die richtigen VLAN-IDs zugewiesen werden.

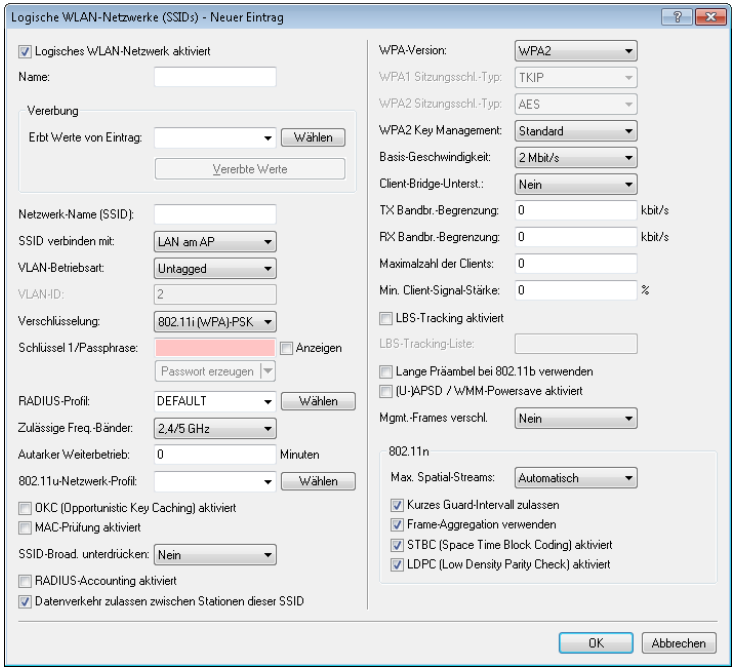
Hinweis: Weitere Information zu RADIUS finden Sie in der Dokumentation Ihres RADIUS-Servers.

13.9.4 RADIUS-Accounting im WLAN-Controller für logische WLANs aktivieren

Die Konfiguration der logischen WLAN-Netzwerke finden Sie in folgendem Menü:

LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**



▶ **RADIUS-Accounting aktiviert**

Stellen Sie hier ein, ob das RADIUS-Accounting in diesem logischen WLAN-Netzwerk aktiviert werden soll.

Mögliche Werte:

– ja, nein

Default:

– nein

Hinweis: Die APs, die der WLC mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine HiLCOS-Version 8.00 oder höher verwenden.

13.10 Anzeigen und Aktionen im LANmonitor

Über den LANmonitor haben Sie einen schnellen Überblick über die WLC im Netzwerk und die APs in der WLAN-Struktur. LANmonitor zeigt dabei u. a. die folgenden Informationen:

- Aktive WLAN-Netzwerke mit den eingebuchten WLAN-Clients sowie der Bezeichnung des APs, bei dem der WLAN-Client eingebucht ist.
- Anzeige der neuen APs mit IP- und MAC-Adresse
- Anzeige der fehlenden APs mit IP- und MAC-Adresse
- Anzeige der gemanagten APs mit IP- und MAC-Adresse, verwendetem Frequenzband und Kanal

Hinweis: Falls der AP wegen einer älteren Firmware diese Daten nicht überträgt, entnimmt der WLC den Kanal und die Frequenz aus der Status-Tabelle **Aktive-Radios** unter **Status** > **Aktive-Radios** > **WLAN-Management** > **AP-Status**.

Über die rechte Maustaste kann auf den APs ein Kontext-Menü geöffnet werden, in dem folgende Aktionen zur Auswahl stehen:

- **Neuen Access Point zu Profil zuordnen**

  Bietet die Möglichkeit, einem neuen AP eine Konfiguration zuzuordnen und ihn so in die WLAN-Struktur aufzunehmen.

- **Access Point trennen**

  Trennt die Verbindung zwischen AP und WLC. Der AP sucht dann erneut nach einem zuständigen WLC. Diese Aktion wird z. B. verwendet, um APs nach einem Backup-Fall vom Backup-WLC zu trennen und wieder auf den eigentlichen WLC zu leiten.

- **Aktualisieren**

  Aktualisiert die Anzeige des LANmonitors.

13.11 Funkfeldoptimierung

Mit der Auswahl des Kanals in der Kanal-Liste wird der Teil des Frequenzbandes festgelegt, den ein AP für seine logischen WLANs verwendet. Alle WLAN-Clients, die sich mit einem AP verbinden wollen, müssen den gleichen Kanal im gleichen Frequenzband verwenden. Im 2,4-GHz-Band stehen je nach Land die Kanäle 1 bis 13, im 5-GHz-Band die Kanäle 36 bis 64 zur Verfügung. Auf einem Kanal kann dabei zeitgleich jeweils nur ein AP Daten übertragen. Um in der Funkreichweite eines anderen APs ein WLAN mit maximaler Bandbreite betreiben zu können, muss jeder AP einen separaten Kanal nutzen – anderenfalls müssen sich die WLANs die Bandbreite des Kanals teilen.

Hinweis: Bei einer völlig offenen Kanalliste werden die APs möglicherweise automatisch Kanäle wählen, die sich gegenseitig teilweise überlappen und so die Signalqualität reduzieren. Außerdem könnten die APs evtl. Kanäle wählen, welche die WLAN-Clients aufgrund der Ländereinstellung nicht nutzen können. Um die APs gezielt auf bestimmte Kanäle zu leiten, können z. B. die überlappungsfreien Kanäle 1, 6, 11 in der Kanalliste aktiviert werden.

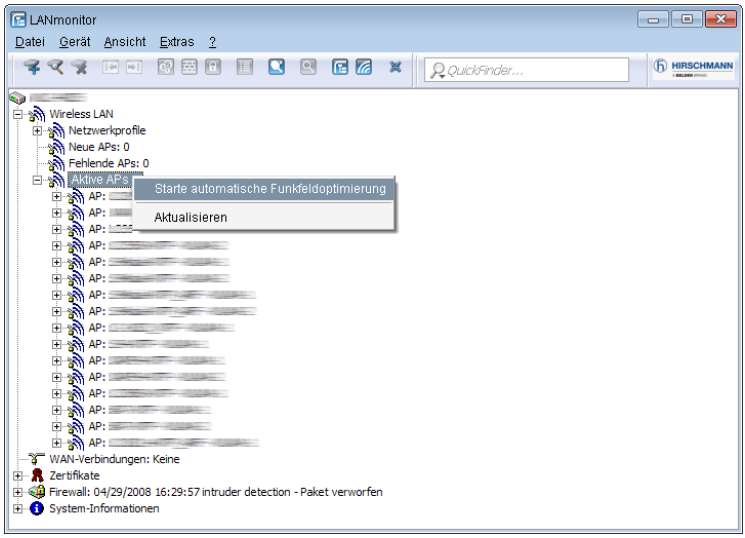
In größeren Installationen mit mehreren APs ist es manchmal schwierig, für jeden AP einen geeigneten Kanal einzustellen. Mit der automatischen Funkfeldoptimierung bieten die WLCs ein Verfahren, um die optimalen Kanäle der APs für das 2,4-GHz- und 5-GHz-Band automatisch einzustellen.

Hinweis: Für APs, die im 5-GHz-Band funken, muss sichergestellt sein, dass der "Indoor-Only"-Modus aktiviert ist.

WEBconfig: **Setup** > **WLAN-Management** > **Starte-automatische-Funkfeldoptimierung**

Hinweis: Sie können die Optimierung auch gezielt für einen einzelnen AP starten, indem Sie die MAC-Adresse als Parameter für die Aktion eintragen.

LANmonitor: Klicken Sie mit der rechten Maustaste auf die Liste der aktiven APs oder auf ein bestimmtes Gerät und wählen Sie danach im Kontextmenü **Starte automatische Funkfeldoptimierung**.



Die Optimierung läuft dann in den folgenden Schritten ab:

1. Der WLC weist allen APs den gleichen Kanal zu. Hierbei verwendet er den Kanal, der von den meisten APs genutzt wird.
2. Die APs führen einen "Background-Scan" durch und melden das Ergebnis an den WLC.
3. Der WLC bestimmt für jeden AP auf Basis der im "Background-Scan" erkannten Geräte einen Interferenzwert.
4. Anschließend löscht er die AP-Kanalliste aller APs. Da die Kanalliste nun leer ist, erhalten die APs über ein Konfigurations-Update die neue Kanalliste ihres jeweiligen Profils.
5. Der WLC deaktiviert die Funkmodule aller APs.
6. Die einzelnen APs durchlaufen nun nacheinander die folgenden Schritte. Es beginnt der AP mit dem höchsten Interferenzwert, um sicherzustellen, dass dieser AP zuerst einen Kanal wählen kann.
7. In der Reihenfolge der Interferenzwerte aktiviert der WLC die Funkmodule der APs, die daraufhin die automatische Einmessung starten. Der jeweilige AP sucht selbstständig den für ihn besten Kanal aus der ihm zugewiesenen Kanalliste. Zur Bestimmung des am besten geeigneten Kanals führt der AP jeweils eine Interferenz-Messung durch, so dass er Signalstärken und Kanäle anderer APs entsprechend berücksichtigen kann. Da die bisherige Liste in der Konfiguration des WLCs gelöscht wurde, ist dies nun die Pro-

filkanalliste. Wenn die Profilkanalliste leer ist, hat der AP die freie Auswahl aus den nicht durch andere Funk-Module belegten Kanälen. Der gefundene Kanal wird zurück an den WLC gesendet und dort in der AP-Kanalliste gespeichert. Somit erhält der AP beim nächsten Verbindungsaufbau wieder diesen Kanal. Die AP-Kanalliste hat so gesehen ein höheres Gewicht als die Profilkanalliste.

Hinweis: Verfügt ein AP über mehrere WLAN-Module, so durchläuft jedes WLAN-Modul nacheinander diesen Vorgang.

Hinweis: Die Funkfeldoptimierung ist Bestandteil von *HirschmannActive Radio Control (ARC)*

13.11.1 Gruppenbezogene Funkfeldoptimierung

Ein WLC erlaubt eine Gruppierung von APs anhand von Standortinformationen, Geräteeigenschaften oder Netzgliederungen. Auf Basis dieser Gruppenzugehörigkeit lässt sich auch eine Funkfeldoptimierung durchführen. Statt also entweder für alle oder nur für einen AP eine Funkfeldoptimierung durchzuführen, können Sie z. B. alle AP innerhalb eines Gebäudetrakts mit einer speziellen Bezeichnung oder mit einer bestimmten Firmware-Version adressieren.

Die entsprechende Gruppe lässt sich sowohl über WEBconfig als auch die Konsole mit dem Gruppen-Parameter ansprechen:

```
do /Setup/WLAN-Management/start optimization <Gruppe>
```

Die APs sind über folgende Optionen des Gruppen-Parameters filterbar:

`-g <Gruppenname>`

APs, die der Gruppe angehören. Mehrere Gruppennamen sind durch Komma getrennt möglich.

`-l <Standort>`

APs, deren Standort entsprechend festgelegt ist.

Hinweis: Die Kombination von `-l` und einer der Standort-Optionen `-c` bis `-r` ist nicht sinnvoll.

-c <Land>

APs mit der entsprechenden Landesangabe.

-i <Stadt>

APs mit der entsprechenden Stadtangabe.

-s <Straße>

APs mit der entsprechenden Straßenangabe.

-b <Gebäude>

APs mit der entsprechenden Gebäudeangabe.

-f <Etage>

APs mit der entsprechenden Etagenangabe.

-r <Raum>

APs mit der entsprechenden Raumangabe.

-d <Gerätename>

APs mit den entsprechenden Gerätenamen.

-a <Antennen>

APs mit der entsprechenden Anzahl an Antennen.

Hinweis: Eine Kombination aus den Optionen -d und -a ist nicht sinnvoll.

-v <Firmware>

APs, die genau diese Firmwareversion besitzen.

-x <Firmware>

APs, deren Firmwareversion niedriger als die angegebene Version ist.

-y <Firmware>

APs, deren Firmwareversion niedriger oder gleich der angegebenen Version ist.

`-z <Firmware>`

APs, der Firmwareversion höher als die angegebene Version ist.

`-t <Firmware>`

APs, deren Firmwareversion höher oder gleich der angegebenen Version ist.

Hinweis: Kombinationen sind möglich, um z. B. APs mit einer Firmwareversion zwischen zwei Versionsständen zu adressieren.

`-n <Intranet-Adresse>`

APs, die sich im Intranet mit der angegebenen Adresse befinden.

`-p <Profilname>`

APs, die sich im angegebenen WLAN-Profil befinden.

13.12 Client Steering über den WLC

Das Client Steering ermöglicht den APs, die im Sendebereich befindlichen WLAN-Clients anhand bestimmter Kriterien zu veranlassen, sich immer mit dem für sie idealen AP zu verbinden. Die Kriterien sind zentral im WLC definiert. Die verwalteten APs melden ständig die aktuellen Werte an den WLC, der aufgrund der Kriterien entscheidet, welche APs die Anfragen von WLAN-Clients beantworten dürfen. Deshalb ist das Client Steering auch nur mit APs möglich, die ein WLC zentral verwaltet.

In gemanagten Netzen zentralisiert ein WLC das Client Steering aller angeschlossenen APs. Das Client Steering läuft in diesem Fall wie folgt ab:

1. Der WLC sammelt die Daten über die angemeldeten WLAN-Clients von den angeschlossenen APs. Aus diesen Daten erstellt der WLC die Bewertung für das Client Steering.
2. Alle APs sind so konfiguriert, dass das Client Steering über den WLC erfolgt.

3. Ein hinzukommender WLAN-Client sendet einen Probe-Request an die APs in seiner Reichweite.
4. Die APs übermitteln diese Anfrage zusammen mit der Signalstärke des WLAN-Clients via CAPWAP an den WLC.
5. Der WLC berechnet für jeden AP im Bereich des WLAN-Clients einen Wert, der sich aus drei Bestandteilen zusammensetzt:

   - Signalstärke-Wert
   - Wert aus der Anzahl der am AP angemeldeten Clients
   - Frequenzband-Wert

   Zusammen mit der jeweiligen Gewichtung, mit der der WLC jeden einzelnen Wert multipliziert, ergibt sich der endgültige Wert.
6. Der WLC sendet den APs mit dem höchsten oder einem maximal um ein Toleranz-Level davon abweichenden Wert die Nachricht, dass dieser den WLAN-Client beim nächsten Anmeldeversuch annehmen darf.
7. Versucht der WLAN-Client, sich noch vor der Antwort des WLC mit einem AP zu verbinden, weist ihn dieser zurück, solange die Antwort vom WLC aussteht.
8. Versucht ein WLAN-Client nicht, sich trotz einer bestehenden Verbindung mit niedriger Qualität an einem anderen AP mit höherer Verbindungsqualität zu verbinden ("Sticky Client"), kann der WLC den aktuellen AP dazu veranlassen, den WLAN-Client abzumelden. Der WLAN-Client ist daraufhin gezwungen, sich mit dem AP zu verbinden, der die bessere Verbindung anbietet.

Hinweis: Wenn ein AP die Verbindung zu dem WLC verliert, der für das Client Steering verantwortlich ist, lässt der AP alle Verbindungen von berechtigten WLAN-Clients zu.

Wichtig: Für die optimale Funktionsweise des gemanagten Client-Steerings muss auf sämtlichen APs HiLCOS 9.00 oder höher installiert sein. Wenn Sie im Mischbetrieb APs mit einer älteren LCOS-Version einsetzen, kann in Ihrem WLAN keine sinnvolle Verteilung der Clients erfolgen.

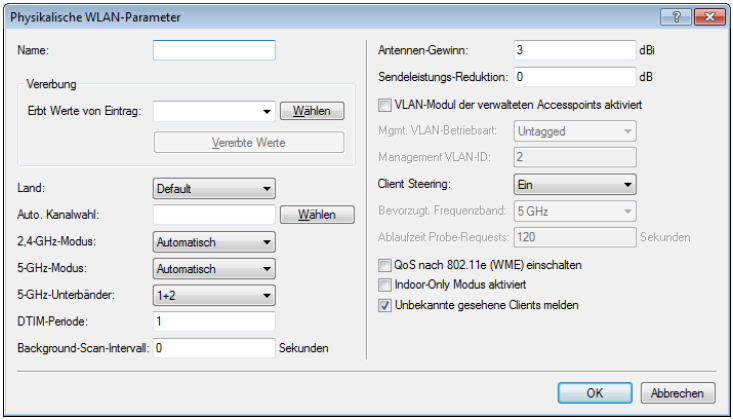
Wichtig: In Szenarien mit zeitkritischem Roaming, z. B. bei VoIP-Telefonen, sollten Sie Client Steering nicht einsetzen, da Client Steering den Einbuchvorgang eines Clients verzögern kann.

13.12.1 Konfiguration

Mit LANconfig konfigurieren Sie das Client Steering wie folgt:

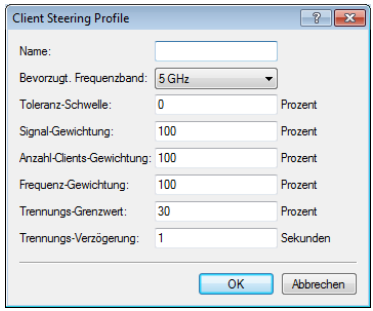
1. Aktivieren Sie zunächst im WLC das Client Steering für einen AP unter **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter** über die Auswahlliste **Client Steering**.

   - **Aus**: Das Client Steering ist deaktiviert.
   - **AP-basiertes Band Steering**: Der AP leitet den WLAN-Client eigenständig auf ein bevorzugtes Frequenzband.
   - **Ein**: Der AP lässt das Client Steering vom WLC durchführen.



2. Im Menü **WLAN-Controller** > **AP-Konfiguration** > **Client Steering Profile** sind bereits zwei Standard-Profile vorkonfiguriert (High-Density, Default), die für die meisten Anwendungsfälle genügen. Optional erstellen Sie dort mit einem Klick auf **Hinzufügen** ein neues Client Steering-Profil.

   Client Steering-Profile legen die Bedingungen fest, nach denen der WLC entscheidet, welche APs beim nächsten Anmeldeversuch einen Client annehmen.



Die Einträge haben folgende Bedeutung:

Name

Bezeichnung des Client Steering-Profils.

Bevorzugt. Frequenzband

Gibt das Frequenzband vor, auf welches der WLC den WLAN-Client leitet.

- **2,4GHz**: Der WLC leitet den AP auf das Frequenzband 2,4 GHz.
- **5GHz**: Der WLC leitet den AP auf das Frequenzband 5 GHz.

Toleranz-Schwelle

Um diesen Prozentwert darf der errechnete Wert für einen AP vom maximal errechneten Wert abweichen, so dass der AP die Erlaubnis erhält, den Client beim nächsten Anmeldeversuch anzunehmen.

Signal-Gewichtung

Gibt an, mit wie viel Prozent der Signalstärke-Wert in den endgültigen Wert eingeht.

Anzahl-Clients-Gewichtung

Gibt an, mit wie viel Prozent der Wert für die Anzahl angemeldeter Clients bei einem AP in den endgültigen Wert eingeht.

Frequenzband-Gewichtung

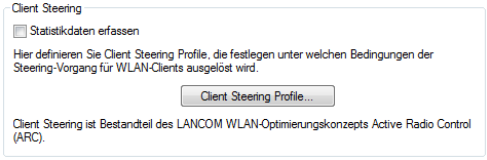
Gibt an, mit wie viel Prozent der Wert für das Frequenzband in den endgültigen Wert eingeht.

Trennungs-Grenzwert

Gibt den Prozentwert vom maximal gesehenen Signalstärkewert an, unter den der aktuelle Wert sinken muss, bevor der AP die Verbindung zum Client trennt.

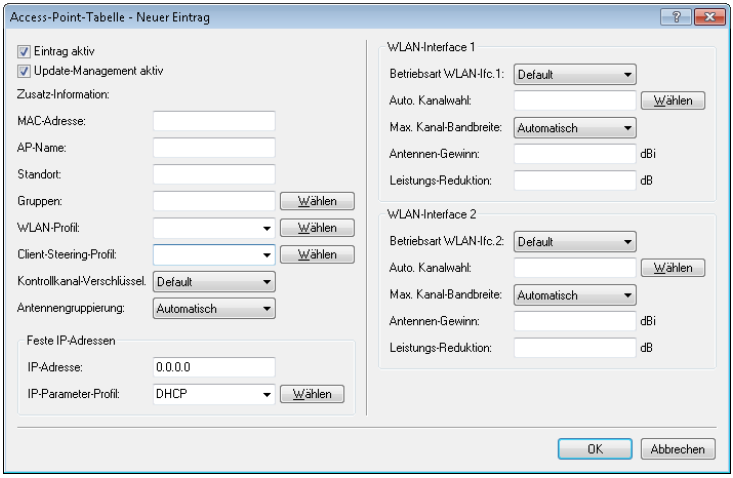
Trennungs-Verzögerung
Gibt die Anzahl der Sekunden an, in denen keine Datenübertragung zwischen AP und Client stattfinden darf, bevor der AP den Client trennt.

3. Optional: Aktivieren Sie über den Parameter **Statistikdaten erfassen** die Aufzeichnung von Client Steering-Statistiken. Die Statistikdaten lassen sich anschließend z. B. mittels LANmonitor auswerten.

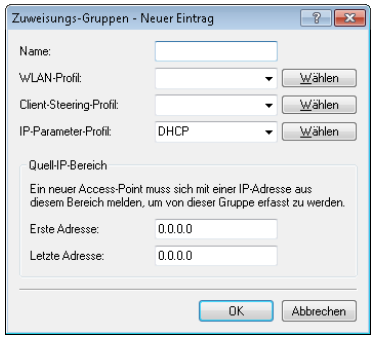


Hinweis: Die Statistikaufzeichnung erhöht die Last auf dem WLC. Hirschmann empfiehlt daher, die Statistikaufzeichnung nicht dauerhaft zu aktivieren.

4. Weisen Sie jetzt unter **WLAN-Controller** > **AP-Konfiguration** > **Access-Point-Tabelle** dem entsprechenden AP eines der Client Steering-Profile zu.



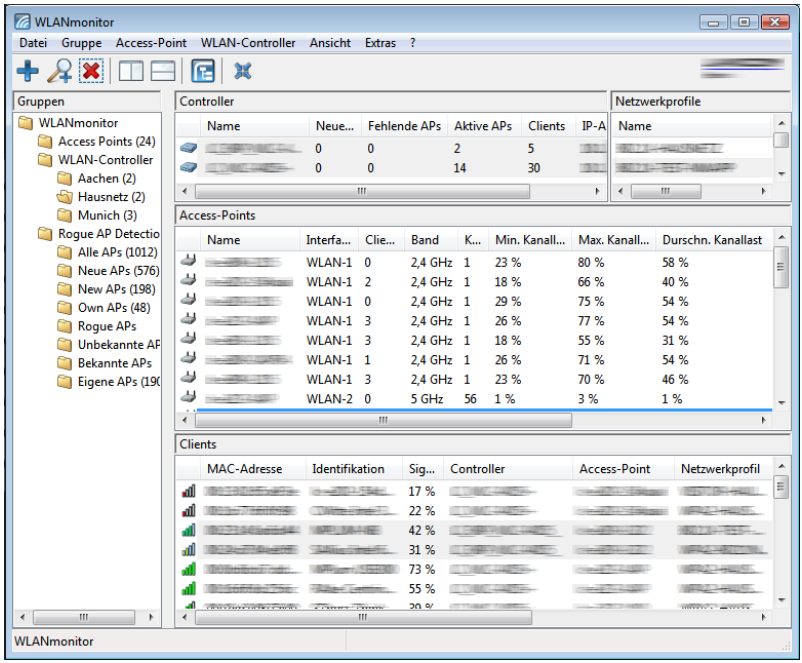
5. Optional: Ordnen Sie ggf. definierten Zuweisungs-Gruppen ein entsprechendes Client Steering-Profil zu.



Damit haben Sie die Konfiguration des Client-Steerings abgeschlossen.

13.13 Kanallastanzeige im WLC-Betrieb

Für die von einem WLC verwalteten APs wird die Last auf den verwendeten Kanälen in drei Werten als minimale, maximale und durchschnittliche Kanallast angezeigt. Die angezeigten Werte werden in einem Messintervall von drei Minuten ermittelt. Die ersten Werte werden demnach auch erst nach drei Minuten angezeigt.



13.14 Sicherung der Zertifikate

Ein WLC erzeugt beim ersten Systemstart die grundlegenden Zertifikate für die Zuweisung der Zertifikate an die APs – darunter die Root-Zertifikate für die CA (Certification Authority) und die RA (Registration Authority). Auf der Grundlage dieser beiden Zertifikate stellt der WLC die Geräte-Zertifikate für die APs aus.

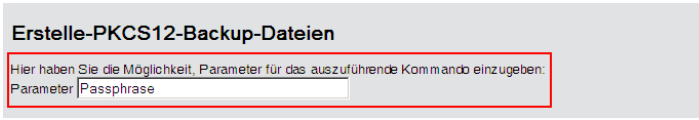
Wenn mehrere WLCs in der gleichen WLAN-Infrastruktur parallel eingesetzt werden (Load-Balancing) oder wenn ein Gerät ersetzt bzw. neu konfiguriert werden muss, sollten immer die gleichen Root-Zertifikate verwendet werden, um einen reibungslosen Betrieb der verwalteten APs zu gewährleisten.

13.14.1 Backup der Zertifikate anlegen

Für die Wiederherstellung der CA bzw. der RA werden die jeweiligen Root-Zertifikate mit den privaten Schlüsseln benötigt, die beim Systemstart automatisch vom WLC erzeugt werden. Außerdem sollten folgende noch weitere Dateien mit Informationen über die ausgestellten Geräte-Zertifikate gesichert werden. Damit diese vertraulichen Daten auch beim Export aus dem Gerät heraus geschützt bleiben, werden sie zunächst in einen PCKS12-Container gespeichert, der mit einer Passphrase geschützt ist.

WEBconfig

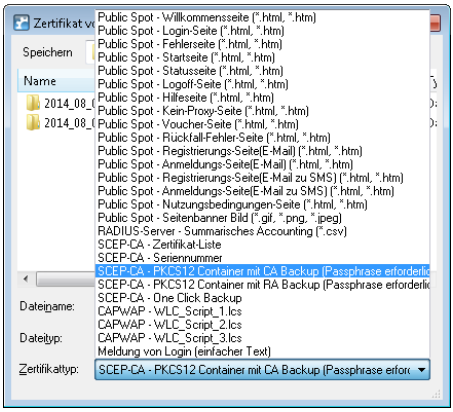
1. Öffnen Sie die Konfiguration des WLCs mit WEBconfig im Bereich **HiLCOS-Menübaum** > **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**.
2. Wählen Sie den Befehl **Erstelle-PKCS12-Backup-Dateien** und geben Sie als Parameter die Passphrase für die PKCS12-Container an.



Mit dieser Aktion werden die Zertifikate und privaten Schlüssel in die PKCS12-Dateien gespeichert und können dann aus dem Gerät heruntergeladen werden.

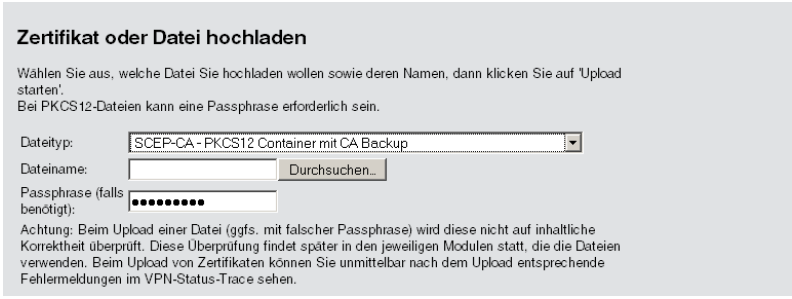
LANconfig

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern.**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container aus und klicken Sie auf **Speichern**.



13.14.2 Zertifikats-Backup in das Gerät einspielen

1. Wählen Sie **Dateimanagement** > **Zertifikat oder Datei hochladen**.
2. Wählen Sie dann als Dateityp nacheinander die beiden Einträge für die SCEP-CA:
   - PKCS12-Container mit CA-Backup
   - PKCS12-Container mit RA-Backup
3. Geben Sie dazu jeweils den Dateinamen mit Speicherort an und die Passphrase, die beim Erstellen der Sicherungsdateien definiert wurde. Bestätigen Sie mit **Upload starten**:



4. Nach dem Einspielen der CA Sicherung muss die Datei `controller_rootcert` im Verzeichnis **Status** > **File-System** > **Contents** gelöscht werden.

Geben Sie dazu an der Konsole die folgenden Befehle ein:

```
cd /Status/File-System/Contents
del controller_rootcert
```

5. Löschen Sie nach dem Zurückspielen des Backups alle Dateien, die mit `controller_` oder `eaptls_` beginnen.
6. Danach muss im Verzeichnis **Setup** > **Certificates** > **SCEP-Client** der Befehl `Reinit` aufgerufen werden:

```
cd /Setup/Certificates/SCEP-Client
do Reinit
```

13.14.3 Sichern und Wiederherstellen weiterer Dateien der SCEP-CA

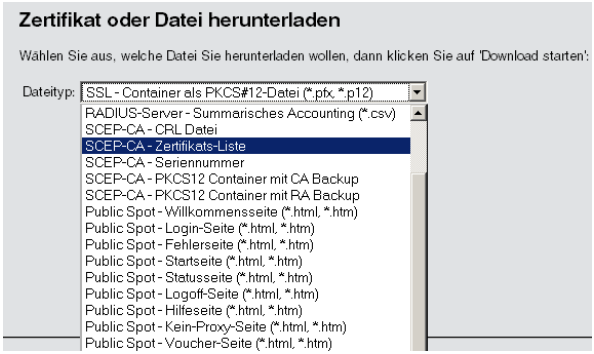
Um die SCEP-CA vollständig wiederherstellen zu können, sind auch die Informationen über die von der SCEP-CA ausgestellten Geräte-Zertifikate für die einzelnen APs wichtig.

Hinweis: Wenn nur die Root-Zertifikate gesichert werden, können die ausgestellten Geräte-Zertifikate nicht mehr zurückgerufen werden!

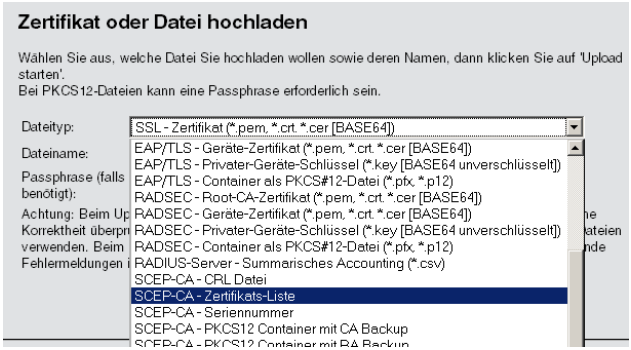
Daher müssen Sie neben den Zertifikaten selbst noch folgende Dateien sichern:

- SCEP-Zertifikatsliste: Liste aller von der SCEP-CA jemals ausgestellten Zertifikate.
- SCEP-Seriennummern: Enthält die Seriennummer für das nächste Zertifikat.

1. Wählen Sie **Dateimanagement** > **Zertifikat oder Datei herunterladen**.
2. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge und bestätigen Sie mit **Download starten**.



3. Zum Einspielen dieser Dateien in das Gerät wählen Sie auf der Startseite von WEBconfig den Befehl **Zertifikat oder Datei hochladen**.
4. Wählen Sie dann als Dateityp nacheinander die oben aufgeführten Einträge, geben Sie dazu jeweils den Dateinamen mit Speicherort an und bestätigen Sie mit **Upload starten**.



Hinweis: Nach dem Einspielen einer neuen Zertifikatsliste werden abgelaufene Zertifikate entfernt und eine neue CRL erstellt. Weiterhin reinitialisiert sich die CA automatisch, wenn nach dem Einspielen der Zertifikatsbackups erfolgreich Zertifikate und Schlüssel extrahiert wurden.

13.14.4 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt

Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im HiLCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem HiLCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das HiLCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des HiLCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA - One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA - One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

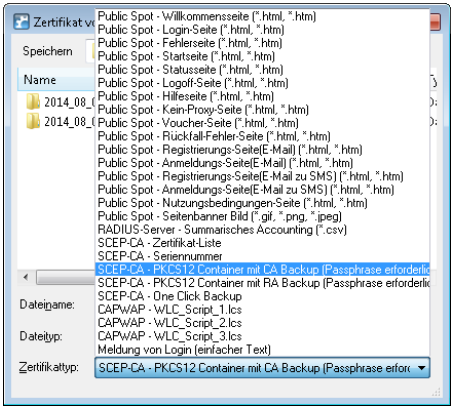
Hinweis: Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion 2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

13.14.5 Backup und Einspielen der Zertifikate über LANconfig

Um die Zertifikate über LANconfig zu speichern und hochzuladen, gehen Sie wie folgt vor:

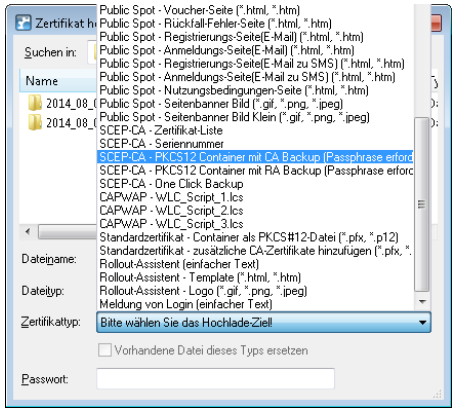
Speichern

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus und klicken Sie auf **Speichern**.



Hochladen

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat oder Datei hochladen**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus.
3. Navigieren Sie anschließend zur gewünschten Datei, geben Sie ggf. ein Passwort an und klicken Sie auf **Öffnen**.



One Click Backup

Für das One Click Backup wählen Sie aus der Dialogliste jeweils den Eintrag "SCEP-CA - One Click Backup" aus.

13.15 Backuplösungen

WLCs verwalten eine große Zahl von APs, bei denen wiederum zahlreiche WLAN-Clients eingebucht sein können. Die WLC haben daher eine zentrale Bedeutung für die Funktionsfähigkeit der gesamten WLAN-Struktur – die Einrichtung einer Backup-Lösung für den vorübergehenden Ausfall eines WLCs ist daher in vielen Fällen unverzichtbar.

In einem Backup-Fall soll sich ein gemanagter AP mit einem anderen WLC verbinden. Da diese Verbindung nur gelingen kann, wenn das Zertifikat des APs von dem Backup-Controller authentifiziert wird, müssen alle WLCs in einer Backup-Lösung auf jeden Fall identische Root-Zertifikate verwenden.

13.15.1 WLC-Cluster

Sofern Sie in Ihrem Netz mehrere WLCs einsetzen, haben Sie die Möglichkeit, diese Geräte zu einem geschlossenen Verbund (Cluster) zusammenfassen. Die APs eines gemanagten WLANs werden dann nicht mehr von einem einzigen, zentralen WLC verwaltetet, sondern von mehreren miteinander synchro-

nisierten WLCs. Ein solcher WLC-Cluster bietet Ihnen vor allem in größeren Netzen diverse Vorteile:

- Automatische Verteilung der Netzlast zwischen den einzelnen APs und WLCs (“Load-Balancing”).
- Erhöhte Ausfallsicherheit durch die Bereitstellung von Backup-WLCs (“Hot Standby”) und automatische Neuverteilung der APs im Falle eines WLC-Ausfalls.
- Aufbau einer Zertifikatshierarchie: Verwaltung der Zertifikate durch eine zentrale Zertifizierungsstelle (CA), dargestellt wahlweise durch einen Master-WLC oder eine externe Stelle (z. B. einen Server).

Ab HiLCOS 8.90 erhält die Cluster-Funktion angeführten Verbesserungen, die im Folgenden näher beschrieben sind.

CAPWAP im WLC gezielt (de)aktivieren

Um mehrere WLCs in einem Verbund (Cluster) zu betreiben, müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies ist auf einem WLC standardmäßig jedoch nicht der Fall, da dieser bestimmte Konfigurationsbestandteile (wie Zertifikate) automatisch generiert. Durch Deaktivieren von CAPWAP auf allen Geräten bis auf einem haben Sie die Möglichkeit, in Ihrem WLC-Cluster einen Master-Controller zu definieren, dessen Konfiguration sich anschließend auf die übrigen WLCs spiegeln lässt.

WLC-Tunnel für die interne Kommunikation

Der Einsatz von WLC-Tunneln ist ein essentieller Bestandteil eines WLC-Clusters. Die am WLC-Cluster beteiligten WLCs nutzen diese Tunnel zur Kommunikation untereinander, um die verteilten Statusinformationen im Verbund abzugleichen. Im Rahmen der Funktionserweiterungen ab HiLCOS 8.90 verbessert sich daher auch der HiLCOS-interne Umgang mit WLC-Tunneln:

- WLCs sind dazu in der Lage, sich untereinander automatisch zu finden.
- Sie haben die Möglichkeit, WLC-Tunnel statisch zu konfigurieren.
- WLCs trennen einen WLC-Tunnel erst nach Ablauf eines Timeouts.
- WLC-Tunnel lassen sich global ein- oder ausschalten.

Die Einstellungen für die WLC-Tunnel und die weiteren WLCs (Remote-WLCs) nehmen Sie in LANconfig im Abschnitt **WLAN-Controller** > **Allgemein** >

WLC-Cluster vor. Über die Einstellung **WLC-Tunnel aktiv** deaktivieren Sie den Einsatz von WLC-Tunneln, was de facto ein Abschalten der Clustering-Funktion bewirkt.

Ermittlung des idealen WLC

Die im HiLCOS implementierten Algorithmen ermöglichen die intelligente Verteilung von APs auf einzelne WLCs. Dies erlaubt den APs, innerhalb von WLC-Clustern die Netzlast gleichmäßig auf alle WLCs aufzuteilen oder nach Ausfall eines WLCs ein alternatives Gerät zu wählen. Hierzu sendet ein AP zunächst einen Discovery Request ins Netz, um sämtliche verfügbaren WLCs zu ermitteln. Die WLCs antworten ihrerseits mit einem Discovery Response, anhand dessen ein AP eine Liste von WLCs erstellt. Diese Liste priorisiert ein der AP anhand verschiedener Kritieren.

Ein AP arbeitet dabei die einzelnen Kriterien sequentiell ab: Sofern nach der Anwendung eines Kriteriums mehrere WLCs für den idealen WLC in Frage kommen, zieht der AP das nächste Kriterium zur Priorisierung heran. Dieser Prozess endet, wenn im Rahmen der nachfolgend beschriebenen Priorisierung schließlich ein WLC als idealer WLC verbleibt.

Kriterien zur Priorisierung

- **Spezifität der AP-Konfiguration**: Ein AP wertet aus, ob ein WLC für den AP eine Konfiguration bereithält und ob diese ein spezifisches AP-Profil oder ein Default-Profil umfasst. Ein spezifisches AP-Profil priorisiert der AP am höchsten, gefolgt von einem Default-Profil. Ein fehlendes Profil erhält die niedrigste Priorität.
- **Höhe des Präferenzwerts**: Der AP wertet aus, welchen Präferenzwert Sie einem WLC zugewiesen haben. Je höher die betreffende Zahl zwischen 0 und 255 liegt, desto höher priorisiert der AP den WLC.

Sofern immer noch mehrere WLCs für die Rolle des idealen WLCs in Frage kommen, hängt der weitere Priorisierungsprozess vom Verbindungsstatus und der Art des Auswahlprozesses (automatisch vs. manuell initiiert) ab:

- Bei der **erstmaligen Ermittlung** bildet ein AP für jeden verbliebenen WLC einen gewichteten Wert aus der Zahl der verbundenen sowie der maximal möglichen APs (**Lizenzauslastung**). Als idealen WLC wählt ein AP schließlich den WLC mit der geringsten Lizenzauslastung.

Hinweis: Hat ein WLC die maximal mögliche Anzahl von AP-Verbindungen erreicht (Lizenzkontingent erschöpft), berücksichtigt ein AP den betreffenden WLC nicht mehr für den aktuellen Auswahlprozess.

- Bei der **automatischen Überprüfung** der idealen AP-Verteilung verbleibt ein AP bei dem mit ihm verbundenen WLC, sofern sich dieser WLC in der Liste der verbliebenen WLCs befindet. Andernfalls sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass der AP einen beliebigen AP auswählt.
- Bei der **manuell ausgelösten Überprüfung** der idealen AP-Verteilung sorgt ein **zufallsgesteuerter Algorithmus** dafür, dass die einzelnen APs die im Netz verfügbaren Lizenzkontingente möglichst gleichmäßig ausnutzen.

Ermittlung der idealen AP-Verteilung

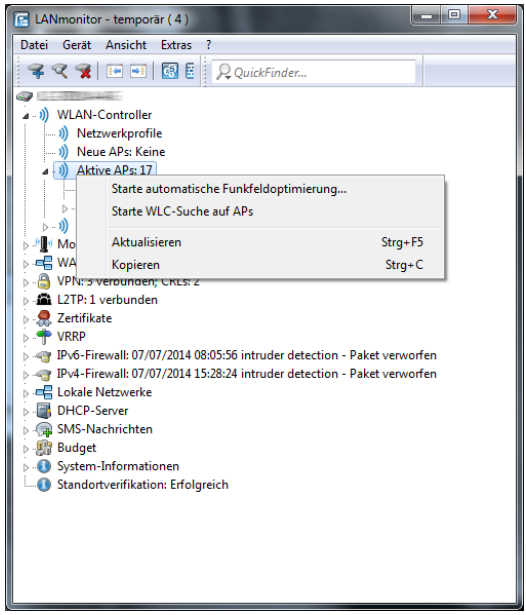
Die Ermittlung der idealen AP-Verteilung in einem WLC-Cluster und eine dadurch ggf. ausgelöste Umverteilung erfolgt grundsätzlich automatisch. Dazu durchläuft ein jeder AP in unregelmäßigen Abständen von 30 bis 60 Minuten den Prozess zur *Ermittlung des idealen WLC*. Gewinnt bei diesem Vorgang der WLC, zu dem bereits eine Verbindung besteht, erfolgt keine Umverteilung. Weist jedoch ein anderer WLC eine höhere Priorisierung auf, so versucht der AP, sich mit diesem WLC zu verbinden.

Sie haben aber auch als Administrator die Möglichkeit, via LANmonitor die Ermittlung der idealen AP-Verteilung und eine ggf. daraus resultierende Umverteilung der APs manuell auszulösen (siehe *Ideale AP-Verteilung manuell initiieren* auf Seite 1404).

Ideale AP-Verteilung manuell initiieren

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die Berechnung der idealen Verteilung manuell starten und dadurch ggf. eine Neuverteilung auslösen.

1. Starten Sie LANmonitor und wählen Sie einen WLC aus.
2. Wechseln Sie in den Menüzweig **Wireless LAN** > **Aktive APs**.
3. Öffnen Sie das Kontextmenü auf einem beliebigen AP und wählen Sie **Starte WLC-Suche auf APs**.



Die betreffenden Access Points bestimmen den für sie optimalen WLC und verteilen sich entsprechend der Vorgaben über den WLC-Verbund.

Einrichten einer CA-Hierarchie

Um mehrere WLC im Verbund zu betreiben (WLC-Cluster), müssen alle beteiligten Geräte eine identische Konfiguration aufweisen. Dies umfasst auch die innerhalb des WLC-Clusters eingesetzten Zertifikate. Die Lösung liegt in dem Aufbau einer Zertifikats- bzw. CA-Hierarchie: Hierbei definieren Sie die CA eines WLC als Root-CA, von welcher die übrigen WLCs das Zertifikat für ihre (Sub-)CA beziehen.

Das nachfolgende Szenario zeigt Ihnen, welche Konfigurationsschritte für den Aufbau einer CA-Hierarchie notwendig sind. Die Konfiguration erfolgt exemplarisch anhand zweier WLCs:

- WLC-MAIN stellt das Gerät mit der Root-CA dar;
- WLC-SUB stellt das Gerät dar, welches bei der Root-CA ein Zertifikat bezieht, um als Sub-CA weitere Zertifikate ausstellen zu können.

Konfiguration der Root-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Root-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Kommandozeile am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-MAIN CA/O=HIRSCHMANN/C=DE`

3. Wechsel Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **Ja**.

Damit haben Sie die Konfiguration der Root-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat.

Konfiguration der Sub-CA

Der nachfolgende Abschnitt beschreibt die Einrichtung einer Sub-CA auf einem WLC. Die einzelnen Handlungsschritte gehen von einem zurückgesetzten Gerät aus, bei dem Sie die Standard-Inbetriebnahme durchgeführt und die korrekte Uhrzeit gesetzt haben.

1. Melden Sie sich via WEBconfig oder über die Kommandozeile am Gerät an.
2. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Root-CA** auf **Nein**.
3. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate**. Passen Sie hier die Namen für die Certificate Authority (CA) und die Registration Authority (RA) über die Parameter **CA-Distinguished-Name** und **RA-Distinguished-Name** an.

   Beispiel: `/CN=WLC-SUB CA/O=HIRSCHMANN/C=DE`

4. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** > **Sub-CA** und tragen Sie für den Parameter **CADN** den Distinguished Name der Root-CA ein.

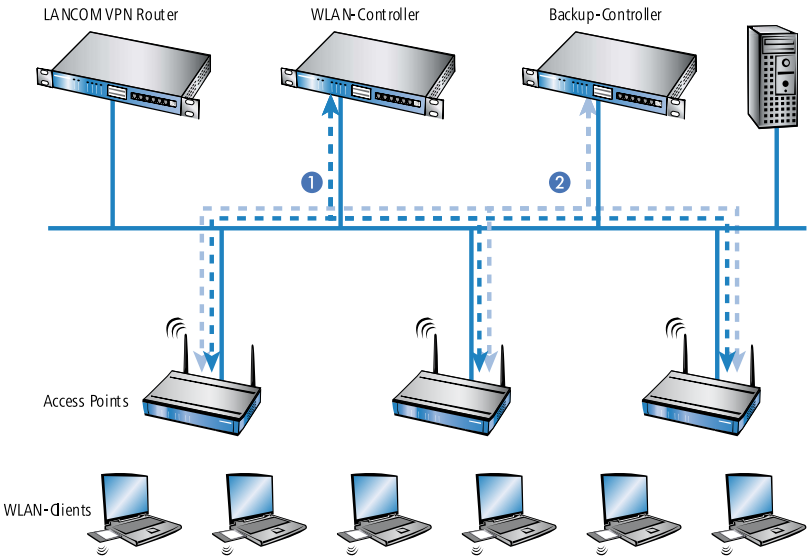
   Beispiel: `/CN=WLC-MAIN CA/O=HIRSCHMANN/C=DE`

5. Tragen Sie für den Parameter **Challenge-Pwd** das Challenge-Passwort ein, das auf WLC-MAIN unter **Setup** > **Zertifikate** > **SCEP-CA** hinterlegt ist.
6. Hinterlegen im Parameter **CA-Url-Adresse** die URL (Adresse) zur Root-CA.
   Stellt ein anderer WLC mit HiLCOS-Betriebssystem die Root-CA zur Verfügung, müssen Sie lediglich die IP-Adresse im Default-Wert durch jene Adresse austauschen, unter der das entsprechende Gerät zu erreichen ist. Beispiel: `http://192.168.1.1/cgi-bin/pkiclient.exe`.
7. Optional: Spezifizieren Sie die **Ext-Key-Usage** und **Cert-Key-Usage**, um die Funktionen der Sub-CA einzuschränken. Weitere Informationen hierzu finden Sie in der CLI-Reference.
8. Setzten Sie den Parameter **Auto-generiert-Request** auf **ja**, um die Sub-CA zu aktivieren..
9. Wechseln Sie in das Menü **Setup** > **Zertifikate** > **SCEP-CA** und setzten Sie den Parameter **Aktiv** auf **ja**, um den CA-Server mit SCEP zu aktivieren.

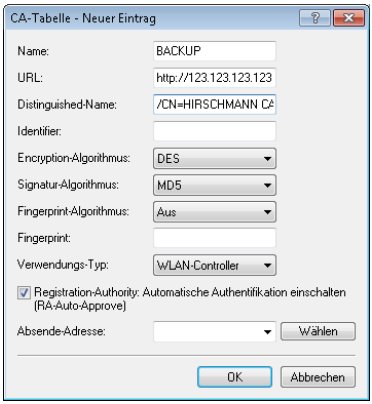
Damit haben Sie die Konfiguration der Sub-CA abgeschlossen. Mit dem Befehl `show ca cert` an der Kommendozeile lässt sich überprüfen, ob der WLC das Zertifikat korrekt erstellt hat. Die Hierarchie der Zertifikate muss hierbei sichtbar sein: Als erstes zeigt der WLC das Zertifikat der Root-CA an, dann das Zertifikat der Sub-CA.

13.15.2 Backup mit redundanten WLAN-Controllern

Diese Form des Backups bietet sich an, wenn Sie einen WLC durch einen zweiten WLC absichern und dabei jederzeit die volle Kontrolle über alle gemanagten APs behalten möchten. Der Backup-WLC wird dabei so konfiguriert, dass er die benötigten Zertifikate über SCEP vom abgesicherten Haupt-WLC bezieht.

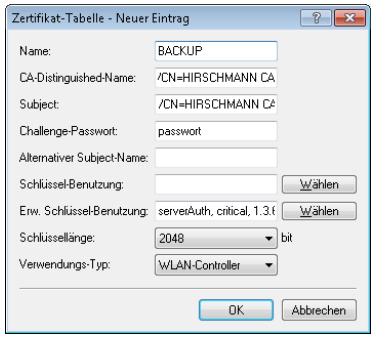


1. Stellen Sie auf beiden WLCs **1** und **2** die gleiche Uhrzeit ein.
2. Schalten Sie die CA auf dem Backup-WLC aus (WEBconfig: HiLCOS-Menübaum > Setup > Zertifikate > SCEP-CA > Aktiv).
3. Erstellen Sie in der Konfiguration des SCEP-Clients im Backup-WLC einen neuen Eintrag in der CA-Tabelle (in LANconfig unter **Zertifikate** > **SCEP-Client** > **CA-Tabelle**). Darin wird die CA des Haupt-WLC eingetragen.



4. Geben Sie als URL die IP-Adresse oder den DNS-Namen des Haupt-WLCs ein gefolgt vom Pfad zur CA `/cgi-bin/pkiclient.exe`, also z. B. `10.1.1.99/cgi-bin/pkiclient.exe`.
   - **Distinguished-Name**: Standardname der CA (/CN=HIRSCHMANN CA/O=HIRSCHMANN/C=DE) bzw. der Name der auf dem primären Controller vergeben wurde
   - **RA-Auto-Approve** einschalten
   - **Verwendungs-Typ**: WLAN-Controller

5. Erstellen Sie dann einen neuen Eintrag in der Zertifikats-Tabelle mit folgenden Angaben:



   - **CA-Distinguished-Name**: Der Standardname, der bei der CA eingetragen wurde, also z. B. /CN=HIRSCHMANN CA/O=HIRSCHMANN/C=DE
   - **Subject**: Angabe der MAC-Adresse des Haupt-WLAN-Controllers in der Form: /CN=00:a0:57:01:23:45/O=HIRSCHMANN/C=DE
   - **Challenge**: Das allgemeine Challenge-Passwort der CA auf dem primären WLAN-Controller oder ein extra für den Controller manuell vergebenes Passwort.
   - **Erweiterte Schlüsselbenutzung**: critical,serverAuth,1.3.6.1.5.5.7.3.18
   - **Schlüssellänge**: 2048 Bit
   - **Verwendungs-Typ**: WLAN-Controller

6. Wenn im Backup-Controller zuvor schon eine SCEP-Konfiguration aktiv war, müssen folgende Aktionen unter WEBconfig ausgeführt werden (**Experten-Konfguration** > **Setup** > **Zertifikate** > **SCEP-Client**):
   - Bereinige-SCEP-Dateisystem

- Aktualisieren (2x: beim ersten Mal holt sich der SCEP-Client nur die neuen CA/RA Zertifikate, beim zweiten Mal wird das Gerätezertifikat aktualisiert)

7. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit allen Profilen und der zugehörigen AP-Tabelle. Die APs bauen dann die Verbindung zum ersten WLC auf. Die APs erhalten von diesem WLC ein gültiges Zertifikat und eine Konfiguration für die WLAN-Module.
8. Übertragen Sie die Konfiguration des ersten WLCs **1** z. B. mit LANconfig auf den Backup-Controller **2**. Dabei werden auch die Profile und die AP-Tabellen mit den MAC-Adressen der APs auf den Backup-WLC übertragen. Alle APs bleiben in diesem Zustand weiterhin beim ersten WLC angemeldet. Ist die Übertragung der Konfiguration erfolgt, ist es erforderlich, dass Sie dem Backup-Controller eine neue IP-Adresse zuweisen.

Fällt der erste WLC **1** aus, suchen die APs automatisch nach einem anderen WLC und finden dabei den Backup-WLC **2**. Da dieser über die gleichen Root-Zertifikate verfügt, kann er die Zertifikate der APs auf Gültigkeit überprüfen. Da die APs außerdem mit ihrer MAC-Adresse in der AP-Tabelle des Backup-WLCs eingetragen sind, übernimmt der Backup-WLC vollständig die Verwaltung der APs. Änderungen in den WLAN-Profilen des Backup-WLCs wirken sich direkt auf die gemanagten APs aus.

Hinweis: Die APs bleiben in diesem Szenario so lange in der Verwaltung des Backup-WLCs, bis dieser entweder selbst einmal nicht erreichbar ist oder bis sie manuell getrennt werden.

Hinweis: Mit der Einstellung des autarken Weiterbetriebs können die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb bleiben, und die WLAN-Clients bleiben eingebucht.

13.15.3 Backup mit primären und sekundären WLAN-Controllern

Mit einer zweiten Form des Backups können Sie für eine größere Anzahl von "primären" WLCs einen gemeinsamen, "sekundären" Backup-WLC bereitstellen. Beim Ausfall eines WLCs bleiben die APs zwar in Betrieb, arbeiten allerdings mit der aktuellen Konfiguration der WLAN-Module weiter. Der Backup-

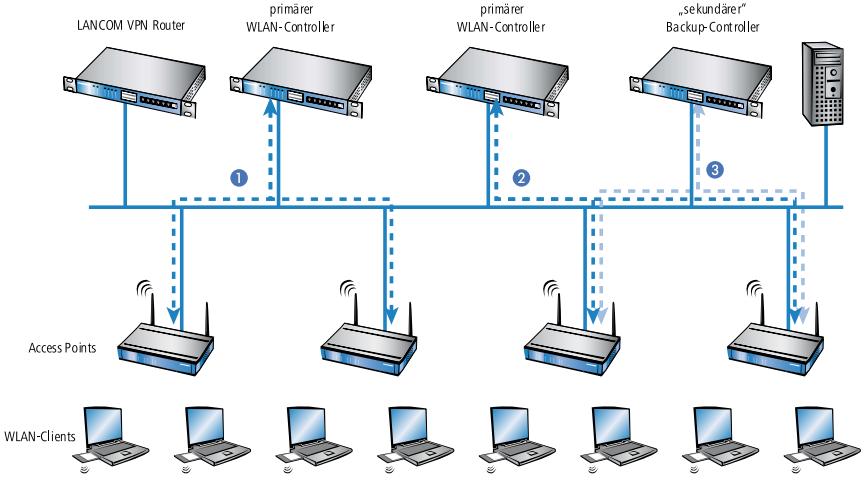
WLC kann als sekundärer WLC den APs keine veränderte Konfiguration zuweisen.

13.15.4 Primäre und sekundäre Controller

Der Verbindungsaufbau zwischen WLC und AP wird immer vom AP initiiert. Ein AP im Managed-Modus sucht in einem LAN nach einem WLC, der ihm eine Konfiguration zuweisen kann. Bei dieser Suche kann der AP unterschiedliche geeignete WLCs finden:

- Der WLC kann das **Zertifikat** des APs authentifizieren und hat für die MAC-Adresse des suchenden APs eine **Konfiguration** gespeichert. Einen solchen WLC bezeichnet man als "primären" WLC.
- Ein WLC kann das **Zertifikat** des APs authentifizieren, hat aber für die MAC-Adresse des suchenden APs **keine Konfiguration** gespeichert und auch **keine Default-Konfiguration**. Einen solchen WLC bezeichnet man als "sekundären" WLC.

Beispiel einer Backup-Lösung mit drei WLCs für 50 gemanagte APs: Zwei der WLCs verwalten jeweils 25 APs, der dritte steht als Backup-WLC bereit:



Hinweis: Ein WLC kann nun in seiner AP-Tabelle die fünffache Anzahl der von ihm selbst maximal verwalteten APs aufnehmen. Für jeweils fünf WLCs (mit gleicher Ausstattung) reicht also ein zusätzlicher WLC aus, um eine vollständige Absicherung bei Ausfall eines Gerätes zu realisieren.

1. Stellen Sie auf allen WLCs **1** und **2** und **3** die gleiche Uhrzeit ein.
2. Übertragen Sie die CA- und RA-Zertifikate aus dem ersten primären WLC **1** in den zweiten, primären **2** und den sekundären "Backup-WLC" **3**.
3. Konfigurieren Sie den ersten WLC **1** wie gewünscht mit den Profilen und der zugehörigen AP-Tabelle für eine Hälfte der APs. Dieser WLC wird somit zum primären WLC für die bei ihm eingetragenen APs.

Hinweis: Bei einer Backup-Lösung über einen sekundären WLC muss die Zeit für den autarken Weiterbetrieb auf jeden Fall so eingestellt werden, dass der AP während dieser Zeitspanne einen Backup-WLC findet, da der Backup-WLC dem AP keine neue Konfiguration zuweisen kann.

Sobald der AP eine Verbindung zu einem sekundären WLC hergestellt hat, wird der Ablauf der Zeit für den autarken Weiterbetrieb unterbrochen. Der AP bleibt also mit seinen WLAN-Netzwerken auch über diese eingestellte Zeit hinaus aktiv, solange er eine Verbindung zu einem WLC hat.

1. Konfigurieren Sie den zweiten WLC **2** für die andere Hälfte der APs, welche dann diesen WLC als primären WLC betrachten.
2. Der Backup-WLC **3** bleibt bis auf die Uhrzeit und die Root-Zertifikate ohne weitere Konfiguration.
3. Die APs suchen nach dem Start über eine Discovery-Message nach einem WLC. In diesem Fall antworten alle drei WLCs auf diese Nachricht – die APs wählen jeweils "ihren" primären WLC für die folgende DTLS-Verbindung. Die eine Hälfte der APs entscheidet sich für WLC **1**, die andere Hälfte für WLC **2**. Da WLC **3** für keinen der APs als primärer WLC fungiert, meldet sich kein AP bei ihm an.
4. Fällt z. B. der erste WLC **2** aus, suchen die APs automatisch nach einem anderen WLC. Sie finden die WLC **A** und **C**, wobei **A** schon mit seinen 25 APs vollständig ausgelastet ist. Backup-Controller **C** kann die Gültigkeit der Zertifikate prüfen, die APs also authentifizieren und als gemanagte APs annehmen. Da die APs jedoch **nicht** mit ihrer MAC-Adresse in der AP-Tabelle des Backup-WLCs eingetragen sind, kann der Backup-WLC die APs nicht weiter verwalten, sie werden nur mit der jeweiligen aktuellen WLAN-Konfiguration weiterbetrieben.

Hinweis: Sollte WLC **A** nicht ausgelastet sein, weil z. B. einige "seiner" APs ausgeschaltet sind, so könnten sich auch einige der suchenden APs bei diesem anmelden. WLC **A** bleibt für diese APs aber ein "sekundärer" WLC, da

er nicht über Konfigurationsprofile für diese Geräte verfügt. Wird in diesem Fall einer der AP wieder eingeschaltet, der über einen Eintrag in der AP-Tabelle von WLC **A** verfügt, nimmt **A** diesen reaktivierten AP wieder auf und trennt sich dafür von einem der APs im Backup-Fall.

Hinweis: Mit der Einstellung des autarken Weiterbetriebs bleiben die APs auch während der Suche nach einem Backup-WLC mit der aktuellen WLAN-Konfiguration in Betrieb, die WLAN-Clients können weiterhin alle Funktionen nutzen.

13.15.5 Automatische Suche nach alternativen WLCs

Ab HiLCOS 8.90 versucht ein AP nicht mehr, sich bei einem Verbindungsabbruch mit dem zuletzt bekannten WLC neu zu verbinden. Stattdessen sucht der AP im Netz nach einem erreichbaren WLC, der den Kriterien für die *Ermittlung des idealen WLC* entspricht.

13.15.6 One Click Backup der SCEP-CA

Um das Backup der im WLC vorliegenden CA zu vereinfachen, bietet Ihnen das Gerät die Möglichkeit, mit einer einzigen Aktion einen kompletten Zertifikats-Datensatz zu erzeugen (One Click Backup). Dieser Datensatz erlaubt Ihnen die vollständige Sicherung und Wiederherstellung der CA und vermeidet das Auftreten von Zertifikats-Konflikten.

Derartige Konflikte können dann auftreten, wenn Sie die einzelnen PKCS12-Container separat vom Gerät heruntergeladen haben und anschließend wieder einspielen: Hat der WLC in der Zwischenzeit eine neue CA aufgesetzt und neue Zertifikate ausgestellt, führen die abweichenden CAs temporär zu Authentisierungsproblemen bei den verschiedenen Diensten im HiLCOS. Sofern nicht gewartet werden kann, bis die einzelnen Dienste neue Zertifikate anfordern, erfordert die manuelle Konfliktlösung ein Löschen der SCEP-Dateien aus dem HiLCOS-Dateisystem und eine Reinitialisierung des SCEP-Clienten. Mit dem Zurückspielen eines One Click Backups dagegen führt das HiLCOS die notwendigen Schritte automatisch aus.

Erstellen einer Backup-Datei

Um einen Zertifikats-Datensatz zu erzeugen, führen Sie die Aktion **Erstelle-PKCS12-Backup-Dateien** unter **Setup** > **Zertifikate** > **SCEP-CA** > **CA-Zertifikate** aus. Diese Aktion erzeugt eine Zip-Datei innerhalb des HiLCOS-Dateisystems, die alle notwendigen Dateien enthält. Zum Schutz der enthaltenen Zertifikate und Schlüssel ist die Zip-Datei automatisch mit dem Gerätepasswort geschützt, sofern Sie kein gesondertes Passwort angeben. Die erzeugte Zip-Datei lässt sich anschließend z. B. im WEBconfig über **Dateimanagement** > **Zertifikat oder Datei herunterladen** > **SCEP-CA - One Click Backup** herunterladen.

Zurückspielen der Backup-Datei

Um einen Zertifikats-Datensatz zurückzuspielen, laden Sie die gesicherte Zip-Datei unter Angabe der Passphrase direkt in das Gerät. Im WEBconfig z. B. erfolgt dies über die Auswahl **Dateimanagement** > **Zertifikat oder Datei hochladen** > **SCEP-CA - One Click Backup**. Setzen Sie dabei die Option **Vorhandene CA Zertifikate ersetzen**, damit das Gerät den Zertifikats-Datensatz nach dem Hochladen automatisch zurückspielt.

Hinweis: Sofern Sie die Option nicht setzen oder die Backup-Datei auf andere Weise ins Gerät laden, müssen Sie nach dem Hochladen die Aktion 2.39.2.2.11 Zertifikate-aus-Backup-wiederherstellen ausführen, damit das Gerät den Zertifikats-Datensatz zurückspielt.

14 Public Spot

14.1 Einführung

Dieses Kapitel gibt Antworten auf die beiden folgenden Fragen:

- Was ist ein "Public Spot"?
- Welche Funktionen und Eigenschaften zeichnen das Public Spot-Modul aus?

14.1.1 Was ist ein "Public Spot"?

Public Spots, auch HotSpots genannt, sind Orte, an denen sich Benutzer mit ihren Endgeräten – z. B. einem Smartphone, Tablet-PC oder Notebook – in ein öffentlich zugängliches Netzwerk einwählen können. Üblicherweise stellen diese Netzwerke einen Zugang ins Internet bereit, doch kann ein Public Spot auch auf ein lokes Netzwerk beschränkt sein; z. B. um Besuchern einer musealen Einrichtung oder eines Messegeländes via Intranet zusätzliche Informationen bereitzustellen. Der Begriff wird dabei synonym zu den Geräten benutzt, über welche die Benutzer den Netzzugang schließlich herstellen, weshalb auch dieses Handbuch meistens nicht zwischen der Lokalität und dem Gerät unterscheidet.

Weit verbreitet ist der Zugang via WLAN, doch auch der Zugang über ein kabelgebundenes LAN ist in einem Public Spot-Szenario möglich. Der Wunsch nach dieser Form von Netzwerkanbindung bestand ursprünglich vor allem bei Geschäftsreisenden, die am Flughafen, im Hotel oder an vergleichbaren Orten mit dem eigenen Endgerät auf Online-Inhalte zugreifen wollten. An solchen Orten sind festinstallierte Modem-, ISDN- oder Breitbandanschlüsse nur selten für den öffentlichen Gebrauch vorgesehen. Inzwischen erfreut sich jedoch auch die freizeitliche Nutzung eines Public Spots durch Privatpersonen einer wachsenden Beliebtheit.

Die Lösung: (W)LAN-Technologie

Für Public Spot-Szenarios bieten sich die bewährten (W)LAN-Technologien nach den internationalen IEEE 802.11/802.3-Standards an:

- Der Zugang über WLAN ermöglicht den schnellen und unkomplizierten Zugang über Funk: Der Anwender benötigt für sein mobiles Gerät lediglich einen WLAN-Adapter, der bei modernen Endgeräten üblicherweise zur Standardausrüstung gehört oder sich – z. B. über die USB-Schnittstelle – kostengünstig nachrüsten lässt. Die Bandbreite reicht dabei für die wichtigsten Anwendungen aus, selbst wenn zahlreiche Anwender gleichzeitig an einem Public Spot angemeldet sind.
- Der Zugang über LAN ist – bei automatischer Adressvergabe via DHCP – ähnlich unkompliziert: Der Anweder benötigt für sein Endgerät in diesem Fall lediglich einen LAN-Adapter und ein entsprechendes Verbindungskabel, um sich über eine Anschlussdose mit den Public Spot-Netzwerk zu verbinden.

Beim Zugang über LAN verliert der Anwender zwar seine stationäre und unterbrechungsfreie Flexibilität. Allerdings ermöglicht diese Zugangsform – eine entsprechende Infrastruktur vorausgesetzt – selbst bei hoher Netzlast (z. B. durch Multimedia-Inhalte wie Video-on-Demand) und hoher Nutzerzahl (z. B. in einem großen Hotel) einen stabilen Netzbetrieb, wo Verbindungen via WLAN evtl. früher an ihre Grenzen stoßen. Ebenso ist es über einen Public Spot via LAN auch möglich, eine bereits bestehende, kabelgebundene Infrastruktur (z. B. in einer Hochschule) relativ kostengünstig um ein Public Spot-Angebot zu erweitern.

Besonderheiten beim Zugang über (W)LAN

Zwei Aspekte erschweren den Einsatz von herkömmlichen WLAN-Access-Points oder LAN-Routern als Public Spot:

- Die Benutzer-Authentifizierung ist nur über RADIUS/802.1x möglich und erfordert daher eine entsprechende Konfiguration.
- Es gibt keine Möglichkeit, die Benutzung abzurechnen (fehlendes Accounting).

Aus diesem Grund ist der Einsatz von Geräten ohne Public Spot-Funktion nicht praktikabel, da diese Geräte nicht in der Lage sind, zwischen befugten

und unbefugten Nutzern öffentlich zugänglicher Netze zu trennen und deren spezifische Netznutzung entsprechend zu protokollieren.

Benutzer-Autorisierung und -Authentifizierung

Sobald sich eine Person mit einem Endgerät in Reichweite eines Access Points befindet, kann sie zu diesem Access Point auch eine spontane Verbindung herstellen. Ähnliches gilt für frei zugängliche LAN-Anschlüsse. Daraus ergibt sich immer dann ein Problem, wenn der Zugang nicht jedermann, sondern nur bestimmten Benutzern zur Verfügung stehen soll. Genau diese Einschränkung ist beim Einsatz von Public Spots typisch.

Ein Public Spot muss daher in der Lage sein, den (W)LAN-Zugang auf BenutzerEbene zu kontrollieren. Bei einfachen Public Spot-Installationen reicht es dabei aus, wenn die Benutzerdaten lokal im Router oder Access Point – oder alternativ in einem WLAN-Controller – gespeichert und verwaltet werden. Komplexere Installationen verwenden stattdessen für ein detaillierteres Accounting oder eine direkte Verwaltung Datenbankanbindungen an zentrale Authentifizierungs-Server. Solche zentralen Server arbeiten üblicherweise nach dem RADIUS-Verfahren.

Logging

Zum Betrieb öffentlicher Telekommunikationsdienste müssen entsprechend nationaler Gesetzgebung bestimmte Nutzungs-Informationen gespeichert und auf Anfrage den Strafverfolgungsbehörden zur Verfügung gestellt werden können.

Das Public Spot-Modul stellt mittels RADIUS-Accounting und SYSLOG geeignete Schnittstellen zur Speicherung der Nutzungsdaten zur Verfügung.

Hinweis: Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften.

14.1.2 Das Public Spot-Modul im Überblick

Die Ansprüche an Geräte im Public Spot-Betrieb sind so unterschiedlich, wie die Umgebungen, in denen sie eingesetzt wird. Ein Public Spot verfügt über Funktionen für die unterschiedlichsten Bedürfnisse, die in den folgenden Abschnitten genauer beschrieben sind.

Open User Authentication (OUA)

Die Open User Authentication (OUA) stellt eine web-basierte Authentisierung über ein Formular bereit und eignet sich deshalb optimal für Public Spot-Installationen.

Typischer Ablauf einer Online-Sitzung mit OUA

1. Der Benutzer eines (W)LAN-fähigen Endgerätes befindet sich in Reichweite eines Access Points bzw. einer Netzwerkdose im Public Spot-Betrieb.

   - WLAN: Nach dem Systemstart meldet sich der WLAN-Adapter automatisch an betreffenden Access Point an.
   - LAN: Nach dem Systemstart stellt der Benutzer über ein geeignetes Kabel den Netzanschluss her und lässt sich vom DHCP-Server eine Adresse zuweisen.

   Ein Internetzugang oder der Zugriff auf einen kostenpflichtigen Service ist in dieser Phase noch nicht möglich.
2. Der Benutzer startet seinen Web-Browser. Das den Public Spot-Service anbietende Gerät führt den Benutzer automatisch auf die Anmeldeseite des Public Spots. Auf dieser Seite findet er detaillierte Informationen zum angebotenen Service.

   In der Regel hat der Benutzer seine Anmeldedaten in Form eines Vouchers für einen zeitlich begrenzten Zugang zum Public Spot erhalten. Es sind aber auch andere Anmeldeformen denkbar, wie z. B. die Anmeldung nach Bestätigen der Nutzungsbestimmungen des Betreibers oder die selbstständige Anforderung der Zugangsdaten via E-Mail oder SMS.
3. Im Falle einer Voucher-Anmeldung trägt der Benutzer auf der Anmeldeseite seine Zugangsdaten (Benutzerkennung und Passwort) ein. Je nach Konfiguration prüft entweder der geräteinterne oder ein externer RADIUS-Server die eingegebenen Anmeldedaten. Im Erfolgsfall erhält der Benutzer den

Zugang zum Public Spot, ansonsten erscheint eine Fehlermeldung. Falls die Verwendung von Zeitkontingenten gewünscht ist (PrePaid-Modell), überträgt der RADIUS-Server dem Public Spot zusätzlich Informationen zum verfügbaren Zeitguthaben des Benutzers.

4. Der Benutzer kann sich jederzeit beim Public Spot abmelden. Unabhängig davon beendet der Public Spot eine Sitzung selbstständig bei vollständigem Ablauf des Zeitguthabens, bei Erreichen eines festgelegten Ablaufdatums oder bei längerem Kontaktabbruch.

   Während und beim Beenden der Sitzung liefert der Public Spot dem Benutzer eine Übersicht über die Sitzungsdaten. Auf Wunsch meldet der Public Spot parallel dazu alle wichtigen Abrechnungsinformationen des Benutzers an den zuständigen RADIUS-Accounting-Server. Dies kann entweder der geräteinterne oder ein extern konfigurierter Server sein.

OUA ist universell einsetzbar

Der besondere Vorteil des OUA-Verfahrens ergibt sich durch den ausschließlichen Einsatz von Standardprotokollen. Es garantiert, dass OUA universell einsetzbar ist. Es funktioniert mit beliebigen (W)LAN-Adaptern, lässt sich unkompliziert in bestehende Netzwerk-Infrastrukturen einfügen und ermöglicht den Einsatz erweiterter Funktionen, im Falle von WLAN z. B. Roaming zwischen verschiedenen Zellen.

Sicherheit im (W)LAN

Bei der Betrachtung von (W)LANs entstehen oft erhebliche Sicherheitsbedenken. Solche Bedenken existieren im Zusammenhang mit Public Spots sowohl beim Betreiber als auch beim Benutzer.

Sicherheit für den Betreiber

Für den Betreiber eines Public Spots steht die Absicherung seiner Netzwerk-Infrastruktur im Vordergrund. Das Public Spot-Modul stellt dem Betreiber deshalb eine Reihe von Sicherungstechnologien und -methoden zur Verfügung:

- **Multi-SSID** (nur WLAN)**, VLAN und virtuelle Router**

- Die sichere Abgrenzung des öffentlichen Zugangs kann durch eine oder mehrere separate Funkzellen eines Access Points erfolgen (Multi-SSID).
- VLAN-Technik kann den öffentlichen Zugang vom privaten Netz des Betreibers trennen.
- Die virtuelle Routing-Technologie ARF (Advanced Routing and Forwarding) versieht eine SSID mit eigenen Sicherheits- und QoS-Einstellungen und routet darüber nur bestimmte Ziele.

So kann der Gastzugang über einen Public Spot – sicher und effektiv vom Produktivnetz getrennt – die gemeinsame Infrastruktur mitnutzen. Die geräteinterne Firewall kann dabei z. B. die für Public Spot-Nutzer verfügbare Bandbreite im WAN auf max. 50 % begrenzen und nur auf Webseitenzugriffe (HTTP, Port 80) und Namensauflösungen (UDP 53) einschränken.

- **Traffic-Limit**

  Um Denial-of-Service- (DoS-) und Brute-Force-Angriffe auf den Public Spot zu verhindern, können Sie den zulässige Datentransfer noch nicht authentisierter Public Spot-Teilnehmer auf ein ungefährliches Volumen begrenzen.

- **Sperren des Konfigurationszugangs**

  Sie können den Web-Zugriff auf die Gerätekonfiguration (z. B. Ihres Access Points, WLAN Controllers oder Routers) aus dem Public Spot-Netzwerk heraus sperren, so dass der Konfigurationszugang nur über andere festgelegte Management-Schnittstellen möglich ist.

Sicherheit für den Benutzer

Für den Benutzer eines Public Spots steht die Vertraulichkeit der übertragenen Daten im Vordergrund. Zudem wünscht er die Sicherung seiner Benutzerdaten gegen Missbrauch. Ihn schützen folgende Sicherungstechnologien:

- **Intra-Cell Blocking** (nur WLAN)

  Unterbinden Sie in Ihrem Public Spot-Netzwerk die Kommunikation der WLAN-Clients untereinander. Diese Maßnahme erschwert – über die nutzerseitig evtl. ohnehin schon bestehenden Schutzmechanismen – den Zugriff auf die Ressourcen Ihrer Public Spot-Benutzer.

- **Verschlüsselung während der Anmeldephase**

  Sofern Sie über ein digitales Zertifikat verfügen, können Sie dieses in Ihr Gerät laden, um über das verschlüsselte HTTPS-Verfahren Benutzernamen und Kennwörter sicher zu schützen. Das digitale Zertifikat sollte dabei von einer anerkannten öffentlichen Stelle signiert sein, damit ein Browser es als vertrauenswürdig einstuft und Ihren Nutzern keine Sicherheitswarnung ausgibt. Ohne ein Zertifikat erfolgt die Übertragung der Anmeldedaten unverschlüsselt.

  Hinweis: Das Zertifikat sichert lediglich den Anmeldevorgang ab; innerhalb eines Public Spot-Netzwerks werden die Daten in der Regel unverschlüsselt übertragen. Dies gilt sowohl für Verbindungen über LAN als auch über WLAN. Sofern Ihre Nutzer also den normalen Datenverkehr absichern möchten, sind sie auf eigene Verschlüsselungsmechanismen angewiesen!

  Ausgenommen davon sind WLAN-Verbindungen, die über Hotspot 2.0 erfolgen: Da der Hotspot-2.0-Standard auf WPA2 (802.1X/802.11i), EAP und 802.11u basiert, werden Datenpakete sowohl bei der Autorisierung als auch während der Sitzung stets verschlüsselt übertragen.

  Hirschmann empfiehlt dringend, sensitive Nutzdaten immer über verschlüsselte Verbindungen zu übertragen, z. B. durch IPSec-basierte VPN-Tunnel mit dem LANCOM Advanced VPN Client oder durch normale HTTPS-gesicherte Datenverbindungen. Außerdem sollte der Public Spot-Benutzer auf die Aktivierung einer Personal Firewall auf seinem Endgerät achten.

Assistent zur Einrichtung eines Public Spots

Der Setup-Assistent **Public Spot einrichten** unterstützt Sie bei der Einrichtung und ersten Konfiguration Ihres Public Spots. Mit seiner Hilfe gelingt es Ihnen, mit wenigen Klicks ein funktionsfähiges Public Spot-Netzwerk bereitzustellen. Der Assistent gruppiert dazu die dafür notwendigen Einstellungen (z. B. Zuweisen einer Schnittstelle, Vergeben eines IP-Bereichs, Festlegen von Zugangform und Anmeldungsverfahren, Protokollierung) und bietet Ihnen darüber hinaus die Option, einen Administrator mit beschränkten Rechten anzulegen, dem ausschließlich die Einrichtung und ggf. Verwaltung von Public Spot-Nutzern erlaubt ist.

Assistent zum Einrichten und Verwalten von Benutzern

Mit Hilfe des Setup-Wizards **Public-Spot-Benutzer einrichten** (Benutzer-Erstellungs-Assistent) erstellen Sie über WEBconfig zeitlich begrenzte Zugänge zu einem Public Spot-Netzwerk mit wenigen Mausklicks. Dabei bestimmen Sie im einfachsten Fall lediglich die Dauer des Zugangs; der Assistent vergibt Benutzername und Kennwort automatisch und speichert den Zugang in der Benutzerdatenbank des geräteinternen RADIUS-Servers. Der Anwender erhält abschließend ein ausdruckbares, personalisiertes Ticket (Voucher), mit dem er sich im Public Spot-Netzwerk ab sofort bis zur definierten Ablaufzeit anmelden kann.

Alternativ lassen sich Voucher auch auf Vorrat anlegen und ausdrucken, um z. B. in Stoßzeiten die Voucher-Ausgabe zu beschleunigen oder Mitarbeitern ohne Gerätezugriff die Voucher-Ausgabe zu ermöglichen. Hierzu geben Sie im Benutzer-Erstellungs-Assistenten an, dass die Nutzungsdauer erst ab dem ersten Login des Anwenders beginnt. Außerdem definieren Sie eine maximale Gültigkeitsdauer für den Zugang – nach dieser Zeit löscht der Public Spot den Zugang automatisch, auch wenn die Nutzungsdauer noch nicht abgelaufen ist.

Der Setup-Wizard **Public-Spot-Benutzer verwalten** (Benutzer-Verwaltungs-Assistent) stellt alle eingetragenen Public Spot-Zugänge auf einer eigenen Webseite in einer tabellarischen Übersicht dar. So haben Sie mit einem Klick die wichtigsten Daten Ihrer Nutzer im Blick und können auf komfortable Weise die Gültigkeit des Zugangs verlängern / verkürzen oder das betreffende Benutzerkonto komplett löschen. Zusätzlich lassen sich über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, der Authentifizierungsstatus, die IP-Adresse, die gesendeten / empfangenen Datenmengen oder etwaige Beschränkungen, die für das Benutzerkonto gelten.

Verwalten mehrere Administratoren die Public Spot-Zugänge, haben Sie die Möglichkeit, die Anzeige der angelegten Accounts auf den jeweiligen Administrator zu beschränken. Als Folge erscheinen in der tabellarischen Übersicht lediglich die angelegten Zugänge des gerade angemeldeten Administrators.

Hinweis: Diese Beschränkung zeigt keine Wirkung, falls ein Administrator-Zugang existiert, dessen kompletter Name Bestandteil der übrigen Adminis-

tratoren-Accounts ist. "PSpot_Admin" sieht z. B. die Einträge von "PSpot_Admin1" und "PSpot_Admin2". "PSpot_Admin" fungiert in diesem Szenario als Super-Admin. Alle anderen Administratoren ("PSpot_AdminX") dagegen sehen die Einträge der anderen nicht.

14.2 Einrichtung und Betrieb

Dieses Kapitel enthält die wichtigsten Informationen zu Einrichtung und Betrieb eines Public Spots.

- **1. Schritt: Grundkonfiguration**

  Zunächst beschreiben wir die Grundkonfiguration. Nach Abschluss der Grundkonfiguration ist der Public Spot betriebsbereit und für einfaches Anwendungsszenario (Anmeldung über Voucher) vorkonfiguriert.

- **2. Schritt: Sicherheitseinstellungen**

  Dieses Kapitel geht explizit auf sicherheitsrelevanten Einstellungen ein, mit denen Sie Angriffe auf Ihr Public Spot-Netzwerk erschweren und den stabilen Betrieb verbessern. Sofern Sie die hier beschriebenen Einstellungen nicht bereits nicht im Rahmen anderer Einrichtungsschritte getätigt haben, sollten Sie den nachfolgenden Seiten erhöhte Aufmerksamkeit schenken.

- **3. Schritt: Erweiterte Funktionen und Einstellungen**

  Schließlich richtet sich der Blick auf zahlreiche erweiterte Funktionen und Einstellungsoptionen. In detaillierten Beschreibungen erfahren Sie, wie Sie Ihr Gerät individuell an Aufgabe und Umfeld anpassen. Außerdem lernen Sie, wie Sie sich während des Betriebes einen Überblick über Zustand und Aktivitäten des Public-Spots verschaffen.

Hinweis: Bitte beachten Sie, dass der Betrieb eines Public Spots (manchmal auch als "HotSpot" bezeichnet) in Ihrem Land rechtlichen Regulierungen unterliegen kann. Bitte informieren Sie sich vor der Einrichtung eines Public Spots über die jeweils geltenden Vorschriften.

14.2.1 Grundkonfiguration

Die Anleitung der Grundkonfiguration ist in mehrere separate Abschnitte aufgeteilt:

- Der erste Abschnitt beschreibt die Einrichtung eines funktionsfähigen Public Spots am Beispiel eines Wireless Routers.

  Hinweis: Um einen Public Spot für ein einfaches Anwendungsszenario einzurichten, können Sie einen entsprechenden Assistenten starten, der Sie bei der Inbetriebnahme des Public Spots unterstützt.

- Der zweite Abschnitt beschreibt die Konfiguration der Standardwerte für die Benutzer-Assistenten, mit denen auch Mitarbeiter ohne allgemeine Administrator-Rechte neue Public Spot-Benutzer sehr komfortabel anlegen und verwalten können. Hierzu gehört auch das Anlegen eines beschränkten Zugangs, welcher Ihren Mitarbeitern lediglich den Zugriff auf diese Assistenten gewäht.
- Der dritte Abschnitt beschreibt die Benutzerverwaltung im lokalen RADIUS-Server, wahlweise über die Benutzer-Assistenten oder manuell über LANconfig.

Die Abschnitte bauen teilweise aufeinander auf, Sie sollten also idealerweise diese Informationen in der entsprechenden Reihenfolge bearbeiten.

Basis-Installation eines Public Spots für einfache Szenarien

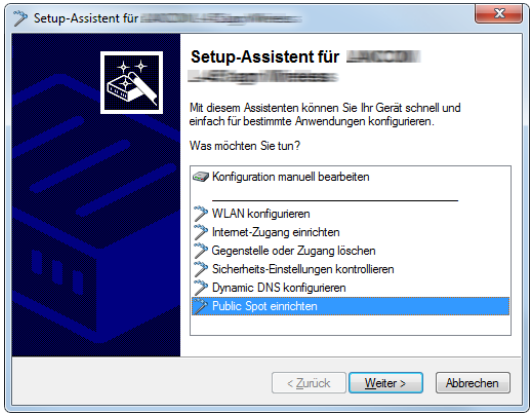
Installation über den Setup-Assistenten

Der folgende Abschnitt beschreibt, wie Sie mit dem Einrichtungs-Assistenten die Basis-Installation eines Public Spots über LANconfig vornehmen.

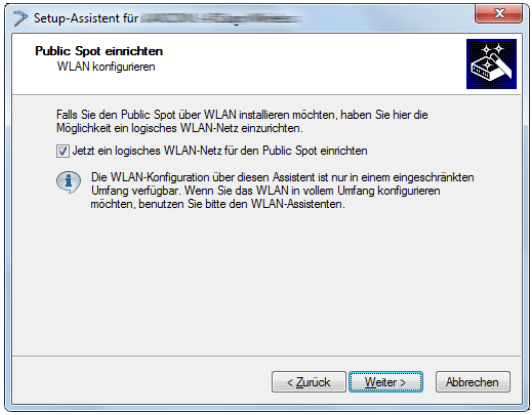
Hinweis: Der Assistent für die Basis-Konfiguration des Public Spots zeigt je nach Gerätetyp und Verlauf verschiedene Dialoge. Dieses Tutorial stellt nur ein mögliches Beispiel dar.

1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point.

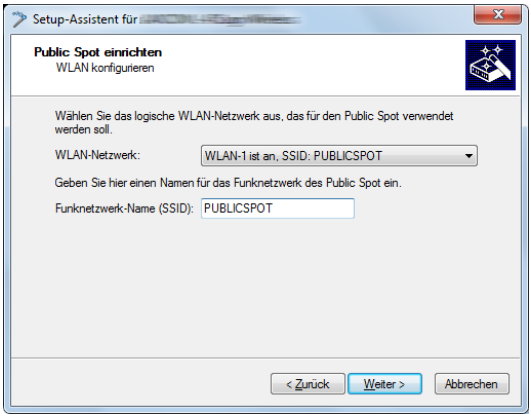
2. Starten Sie den Setup-Assistenten über **Gerät** > **Setup Assistent**, wählen Sie die Aktion **Public Spot einrichten** und klicken Sie anschließend auf **Weiter**.



3. Falls Sie die Nutzung des Public Spots über WLAN einrichten möchten, aktivieren Sie die entsprechende Option und klicken Sie auf **Weiter**.

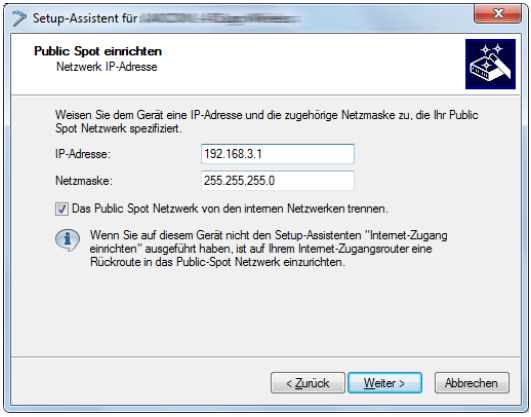


4. Wählen Sie aus dem Auswahlmenü die logische Schnittstelle aus, über die Sie den Public Spot anbieten wollen (z. B. WLAN-1), und geben Sie dem Funknetzwerk einen aussagekräftigen Namen (SSID). Klicken Sie auf **Weiter**.



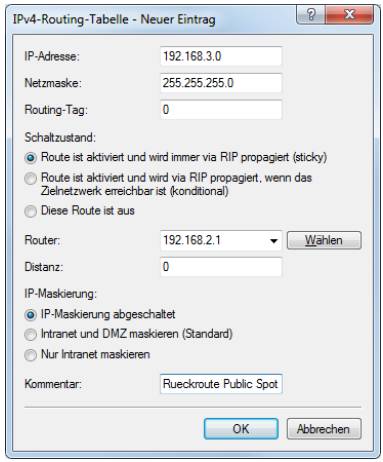
5. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll, und klicken Sie auf **Weiter**.
Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist.

Wenn Sie das Public Spot-Netzwerk aus Sicherheitsgründen von den internen Netzwerken trennen möchten, achten Sie darauf, dass die entsprechende Option aktiviert ist.



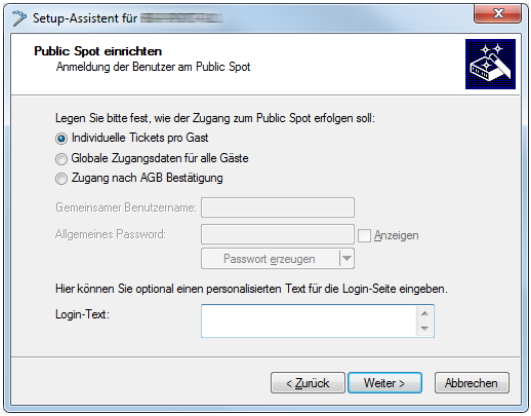
Hinweis: Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.



6. Legen Sie fest, mit welchen Zugangsdaten sich Ihre Benutzer am Public Spot anmelden. Außerdem können Sie die Anmeldeseite optional mit einem Login-Text personalisieren. Klicken Sie anschließend auf **Weiter**. Sie können jedem Benutzer entweder eigene Zugangsdaten aushändigen oder ein allgemeines Konto einrichten, das sämtliche Benutzer für den Zugang zum Public Spot verwenden. Sofern Sie später Voucher ausgeben und feste Benutzerkonten einrichten möchten, wählen Sie die Option **Individuelle Tickets pro Gast**.

Der Login-Text ist ein individueller Text in HTML-Schreibweise in, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Sie können diesen Text auch zu einem späteren Zeitpunkt manuell hinzufügen oder ändern (siehe dazu das Kapitel *Individueller Text auf der Anmeldeseite* auf Seite 1546).

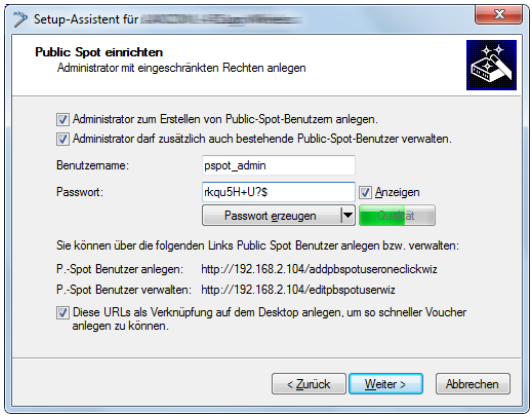


7. Erstellen Sie ggf. einen Administrator mit beschränkten Rechten, der über die Setup-Wizards in WEBconfig Public Spot-Nutzer erstellen und verwalten darf. Klicken Sie anschließend auf **Weiter**.
   Ein solcher Administrator ist z. B. dann sinnvoll, wenn Sie Ihren Mitarbeitern eine Möglichkeit an die Hand geben wollen, selbstständig Benutzerkonten zu administrieren, ohne, dass ein Geräte-Administrator in den Prozess eingebunden werden muss. Die die Erstellungsrechte aktivieren im WEBconfig den Benutzer-Erstellungs-Assistenten; die Verwaltungsrechte den Benutzer-Verwaltungs-Assistenten.

   Über den Benutzer-Erstellungs-Assistenten **Public-Spot-Benutzer einrichten** hat ein Administrator die Möglichkeit, zeitliche befristete Benutzerkonten für Public Spot-Benutzer zu erstellen und die dazugehörigen Zugangsdaten auf einem Voucher auszudrucken.

   Über den Benutzer-Verwaltungs-Assistenten **Public-Spot-Benutzer verwalten** hat ein Administrator die Möglichkeit, diese Nutzer zu admistrieren. Dabei kann er die Gültigkeit des Zugangs verlängern oder verkürzen, oder das betreffende Nutzerkonto komplett löschen. Zusätzlich kann er über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, den Authentifizierungsstatus, die IP-

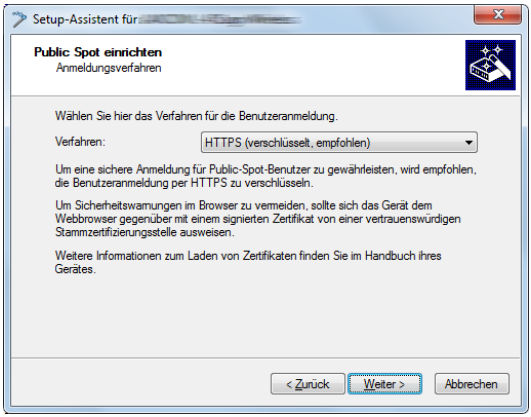
Adresse, die gesendeten/empfangenen Datenmengen oder etwaige Beschränkungen, die für das Konto gelten.



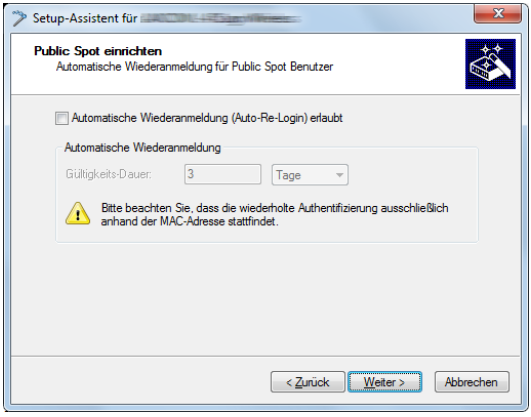
Hinweis: Achten Sie bei der Vergabe eines Passwortes darauf, dass es sicher ist. Der Setup-Assistent prüft während der Eingabe die Qualität des Passwortes. Bei unsicheren Passwörten erscheint das Eingabefeld rot, bei erhöhter Sicherheit wechselt es zu gelb, und bei sehr sicheren Passworten erhält es einen grünen Hintergrund.

8. Wählen Sie das Verfahren für die Benutzer-Anmeldung. Klicken Sie anschließend auf **Weiter**.

   Sie können in der Drop-Down-Liste zwischen **HTTPS** und **HTTP** wählen, wobei Sie mit einer Verbindung über HTTPS die Sicherheit für die Public Spot-Benutzer gewährleisten.

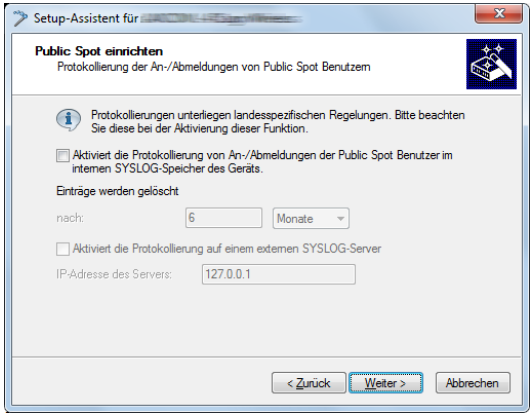


9. Legen Sie fest, ob für sämtliche Public Spot-Nutzer eine automatische Wiederanmeldung erlaubt ist und welche welche maximale Abwesenheit dafür zulässig ist, bevor sich der Nutzer erneut über die Public Spot-Webseite anmelden muss. Klicken Sie anschließend auf **Weiter**.
Die **Automatische Wiederanmeldung** ist eine Komfort-Option, bei welcher der Public Spot ihm bekannte Nutzer bzw. Geräte automatisch authentifiziert. Da die Erkennung bekannter Geräte jedoch ausschließlich über die MAC-Adresse des Netzwerkadapters erfolgt, welche sich fälschen lässt, stellt dieser Anmeldungsweg ein potentielles Sicherheitsrisiko dar und ist deshalb standardmäßig deaktiviert.

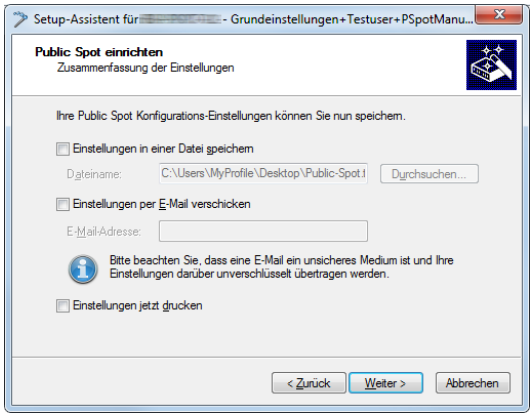


10. Aktivieren Sie bei Bedarf die Protokollierung der An- und Abmeldungen der Pulic-Spot-Benutzer im internen SYSLOG-Speicher des Gerätes. Klicken Sie anschließend auf **Weiter**.

Da die Protokollierung landesspezifischen Regelungen entspricht, ist diese Option standardmäßig deaktiviert. Erkundigen Sie sich vor Aktivieren dieser Funktion nach den gültigen Datenschutzbestimmungen Ihres Landes, um eventuelle rechtliche Probleme zu vermeiden.



11. Speichern Sie bei Bedarf die vorgenommenen Einstellungen.
Bevor Sie die Konfiguration auf Ihr Gerät übertragen, haben Sie die Möglichkeit, die Einstellungen lokal auf Ihrem PC zu sichern, sie per E-Mail zu verschicken oder eine Zusammenfassung auszudrucken.



12. Klicken Sie abschließend auf **Weiter** und **Fertig stellen**, um die Basis-Installation des Public Spots abzuschließen. Der Setup-Assistent sendet die Einstellungen daraufhin an das Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

Manuelle Installation

Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie manuell einen Public Spot für einfache Einsatzszenarien einrichten. Bei dem geschilderten Einsatzszenario aktivieren Sie Public Spot auf einem Interface, über das kein anderer Datenverkehr außer dem des Public Spots läuft; sich z. B. Public Spot- und normale WLAN-Benutzer kein gemeinsames Netzwerk teilen (dedizierte SSID).

Hinweis: Dieses Tutorial stellt nur ein mögliches Beispiel dar. Je nach Geräteart (Access Point, WLAN-Controller, etc.) oder Komplexität der Netzwerkkonfiguration (z. B. Einsatz von VLAN oder ARF) sind abweichende oder zusätzliche Schritte für die Einrichtung eines Public Spots erforderlich! Da derartige Netzwerkkonfigurationen jedoch sehr individuell sind, konzentriert sich das Tutorial bewusst auf ein einfaches Beispiel, damit Sie die notwendigen Schritte bei Bedarf adaptieren können.

1. Starten Sie dazu LANconfig und markieren Sie das Gerät, für das Sie einen Public Spot einrichten wollen, z. B. einen Access Point. Öffnen Sie anschließend den Konfigurationsdialog für das Gerät.
2. Überprüfen Sie die korrekte Uhrzeit.

   Für die Prüfung der Zertifikate und die korrekte Erfassung und Abrechnung der Sitzungsdaten ist die möglichst exakte Uhrzeit im Public Spot wichtig. Bestimmen Sie zunächst Einstellungen wie Zeitzone und Zeitumstellungen (Sommer- und Normalzeit):

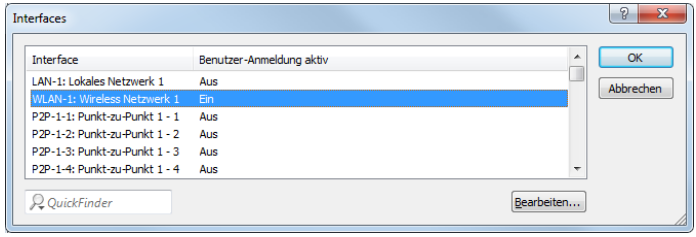
   ▶ LANconfig: **Datum/Zeit** > **Allgemein**

   Hinweis: Damit die Uhrzeit des Public Spots auch später jederzeit korrekt eingestellt bleibt, sollten Sie das Gerät als NTP-Client einrichten. Den dafür notwendigen Zeit-Server tragen Sie unter **Datum/Zeit** > **Synchronisierung** > **Zeit-Server** ein. Öffnen Sie dazu den Hinzufügen-Dialog, um sich eine Liste möglicher Server-Adressen anzeigen zu lassen.

3. Wählen Sie die Schnittstellen für den Public Spot-Betrieb.

Mit der Auswahl einer Schnittstelle legen Sie fest, auf welchen Schnittstellen die Benutzer-Anmeldung aktiviert wird. Zur Auswahl stehen neben den logischen WLAN-Interfaces, über die sich Public Spot-Benutzer direkt anmelden können, auch die logischen LAN-Interfaces (LAN-1 etc.) und die Point-to-Point-Strecken (P2P-1 etc.). Über LAN- und P2P-Interfaces können Sie weitere Access-Points in den Public Spot eines anderen Gerätes einbeziehen. Wählen Sie für einen singulären Access-Point hingegen z. B. das logische WLAN-Interface **WLAN-1**.

▶ LANconfig: **Public-Spot** > **Server** > **Interfaces**

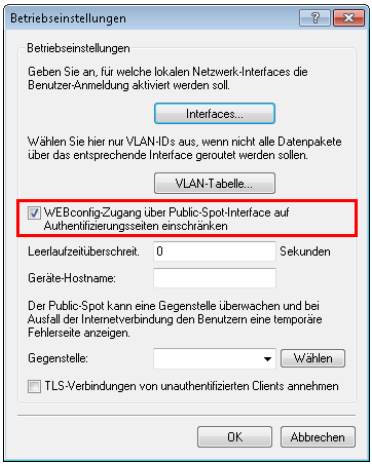


Mit der Aktivierung der Authentifizierung für eine WLAN-Schnittstelle geben Sie automatisch die zugehörige SSID für die Public Spot-Nutzung frei.

Hinweis: Auf einem WLC können Sie bestimmte Ethernet-Interfaces für den Public Spot aktivieren. Dabei können Sie auch eine gezielte Einschränkung auf bestimmte VLANs festlegen.

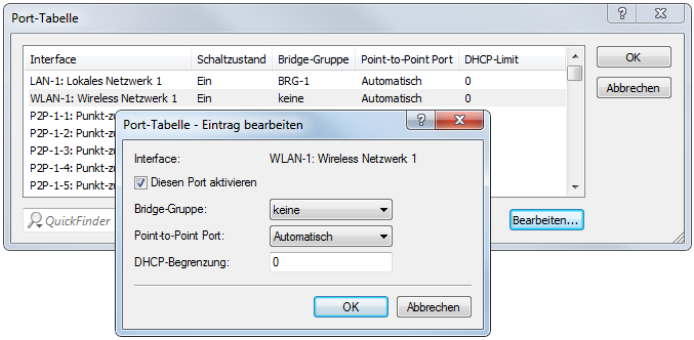
4. Beschränken Sie den Zugriff auf Ihr Gerät aus dem Public Spot-Netzwerk heraus ausschließlich auf die Authentifizierungsseiten.
Wenn Sie den Zugriff nicht einschränken, sind Public Spot-Nutzer dazu in der Lage, auf die Konfigurationsoberfläche Ihres Gerätes (WEBconfig) zuzugreifen. Aus Sicherheitsgründen sollten Sie diese Möglichkeit jedoch ausschließen.

▶ LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



5. Trennen Sie die Schnittstelle, über die Sie den Public Spot-Betrieb anbieten wollen, vom übrigen Netzwerkverkehr.
Damit Endgeräte über unterschiedliche Interfaces bzw. Schnittstellen eines Public Spot-Gerätes (z. B. zwischen LAN-1 und WLAN-1) miteinander kommunizieren können, sind diese Schnittstellen in Ihrem Gerät logisch miteinander verknüpft (gebridged). In einem Public Spot-Szenario ist solch ein Bridging aus Sicherheitsgründen aber oft nicht erwünscht. Um die Kommunikation zwischen der einem Public Spot zugewiesenen Schnittstelle (z. B. WLAN-1) und dem übrigen Netzwerk zu trennen, müssen Sie das Bridging aufheben. Setzen Sie dazu in der **Port-Tabelle** die **Bridge-Gruppe** für das betreffende Interface auf `keine`.

▶ LANconfig: **Schnittstellen** > **LAN** > **Port-Tabelle**

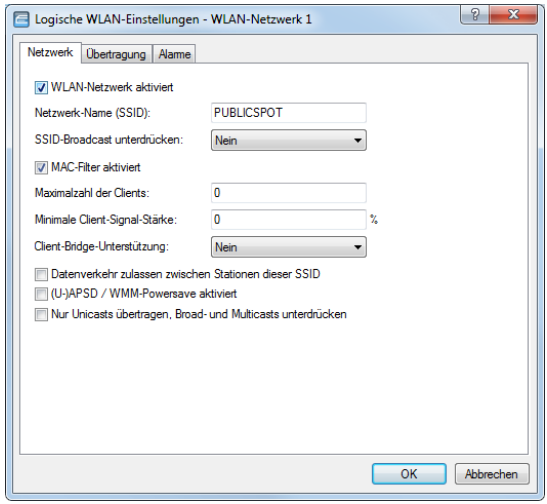


6. Aktivieren Sie WLAN für den Public Spot.

Diese Einstellung betrifft nicht: WLAN Controller.

Aktivieren Sie das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben, und geben Sie diesem Netzwerk einen aussagekräftigen Namen (SSID).

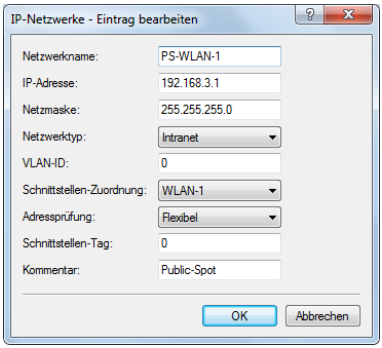
▶ LANconfig: **Wireless-LAN** > **Allgemein** > **Logische WLAN-Einstellungen** > **WLAN-Netzwerk <Nummer>** > **Netzwerk**



Hinweis: Sofern Sie kein privates WLAN einrichten, sollten Sie aus Sicherheitsgründen die Einstellung **Datenverkehr zulassen zwischen Stationen dieser SSID** deaktivieren. Dadurch unterbinden Sie die Kommunikation der einzelnen Public Spot-Benutzer untereinander.

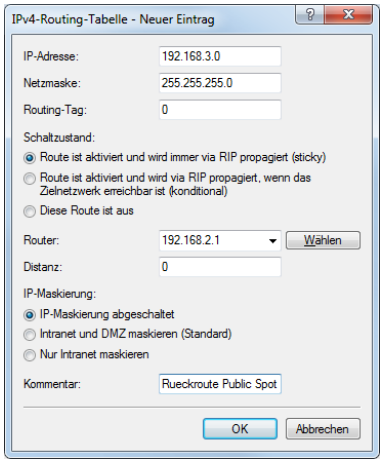
7. Weisen Sie dem Gerät die IP-Adresse und die Netzmaske zu, die Ihr Public Spot-Netzwerk spezifizieren soll.
Das Public Spot-Modul enthält in Ihrem Netzwerk eine eigene IP-Adresse, die unabhängig von der Adresse ist, die Sie dem Gerät zugewiesen haben. Haben Sie z. B. ein 192.168.0.0/24-Netzwerk aufgespannt und Ihr Gerät besitzt darin die IP 192.168.2.1, können Sie dem Public Spot-Modul z. B. die IP `192.168.3.1` und die Subnetzmaske `255.255.255.0` vergeben, sofern diese IP nicht anderweitig belegt ist. Unter **Schnittstellen-Zuordnung** selektieren Sie die gewählte Schnittstelle, z. B. `WLAN-1`.

▶ LANconfig: **IPv4** > **Allgemein** > **IP-Netzwerke**



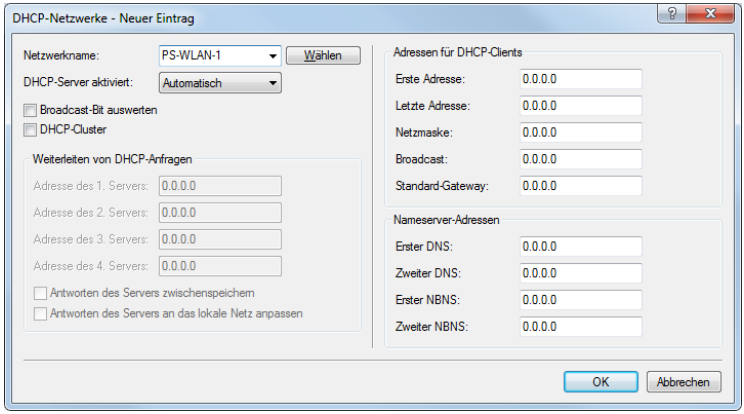
Hinweis: Sofern Ihr Gerät nicht direkt mit dem Internet verbunden ist und Sie für Ihr Public Spot-Netzwerk einen anderen Adresskreis aufgespannt haben, **müssen** Sie in Ihrem Internet-Gateway eine Rückroute in das Public Spot-Netzwerk einrichten. Ohne Rückroute erhalten Public Spot-Nutzer bei der Weiterleitung einen HTTP-Fehler, nachdem sie am Public Spot erfolgreich authentifiziert wurden.

Wie Sie eine Rückroute einrichten, entnehmen Sie bitte der Dokumentation Ihres Internet-Gateways. In LANconfig konfigurieren Sie diese unter **IP-Router** > **Routing** > **IPv4-Routing-Tabelle**. Legen Sie dazu einen neuen Eintrag an und tragen Sie unter **IP-Adresse** die Netzadresse Ihres Public Spot-Netzes ein sowie unter **Router** die Adresse, die der Public Spot in Ihrem lokalen Netz besitzt.



8. Konfigurieren Sie die DHCP-Server-Einstellungen für das Public Spot-Netzwerk.
Da das Gerät ein IP-Netzwerk unabhängig von dem Netzwerk aufspannt, in dem es sich befindet, müssen Sie für dieses Netzwerk einen DHCP-Server konfigurieren. Setzen Sie dazu für das zuvor eingerichtete IP-Netzwerk (z. B. `PS-WLAN-1`) den Wert für **DHCP-Server aktiviert** auf `Automatisch`.

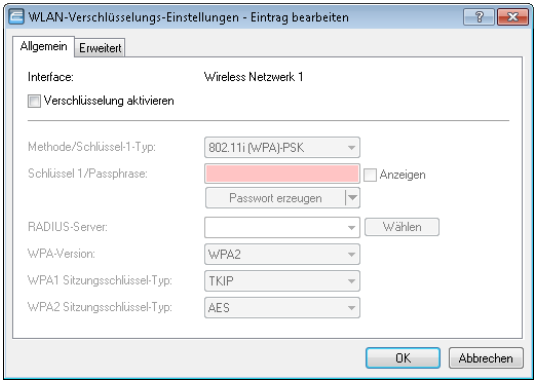
▶ LANconfig: **IPv4** > **DHCPv4** > **DHCP-Netzwerke**



9. Deaktivieren Sie die Verschlüsselung für das Interface, über das Sie den Public Spot anbieten.

   Diese Einstellung betrifft nicht: WLAN Controller.

   Standardmäßig ist für alle logischen WLANs eine Verschlüsselung aktiviert. In Public Spot-Anwendungen werden die Nutzdaten zwischen den WLAN-Clients und dem Access Point üblicherweise unverschlüsselt übertragen. Deaktivieren Sie daher unter **Wireless-LAN** > **Verschlüsselung** > **WLAN-Verschlüsselungs-Einstellungen** die Verschlüsselung für das logische WLAN, welches Sie zuvor für die Public Spot-Anmeldung freigegeben haben.

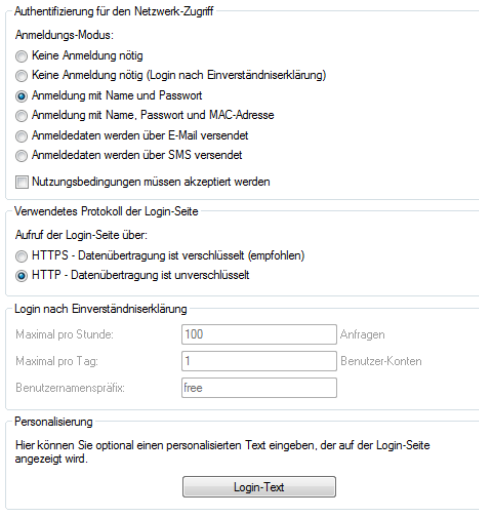


10. Wählen Sie den Anmeldungs-Modus und das verwendete Protokoll für die Benutzeranmeldung aus.

    Über den Anmeldungs-Modus legen Sie fest, mit welchen Informationen sich die Benutzer des Public Spot-WLANs anmelden können. Wählen Sie **Anmeldung mit Name und Passwort**, um Ihren Nutzern z. B. die Anmeldung mit einem individuellen Benutzernamen und einem Passwort zu ermöglichen, das Sie diesen vorab zuweisen. Zusätzlich erlaubt Ihnen dieses Einstellung, über sogenannte Voucher (Tickets) kurzfristig Hotspot-Zugänge für Gäste bereitzustellen.

    Verwenden Sie als Protokoll **HTTPS**, damit die Zugangsdaten Ihrer Nutzer bei der Anmeldung verschlüsselt übertragen werden.

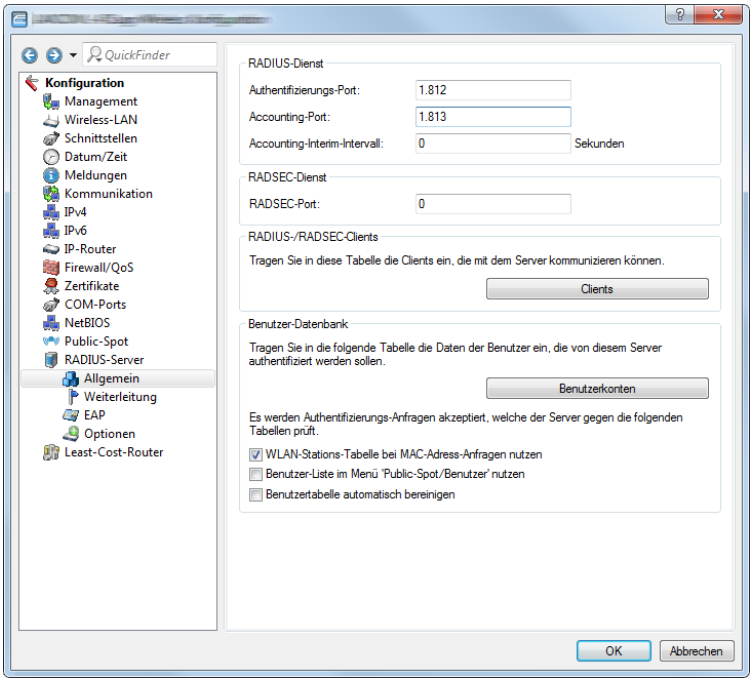
    ▶ LANconfig: **Public-Spot** > **Anmeldung** > **Anmeldungs-Modus**



Hinweis: Beachten Sie, dass – wenn Sie die Einstellungen **Keine Anmeldung nötig** wählen –, auch Unbefugte ungehinderten Zugriff auf Ihren Public Spot haben können!

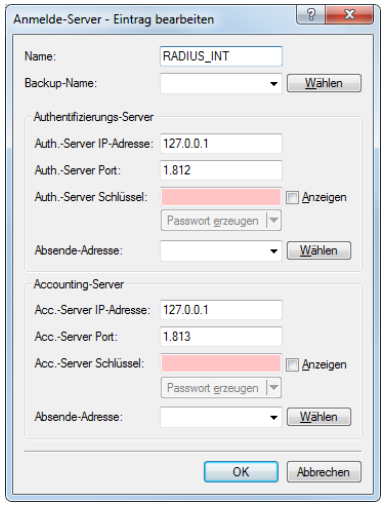
11. Definieren Sie den internen RADIUS-Server als den für die Benutzerverwaltung und das Accounting zuständigen Server. Tragen Sie dazu den **Authentifizierungs-Port** `1.812` und den **Accounting-Port** `1.813` ein. Public-Spot-Zugänge speichern Sie in der Benutzer-Datenbank des geräteinternen RADIUS-Servers. Um diese Public Spot-Zugänge zu nutzen, **müssen** Sie den RADIUS-Server konfigurieren und das Public Spot-Modul auf die Nutzung des RADIUS-Servers einstellen.

▶ LANconfig: **RADIUS-Server** > **Allgemein**



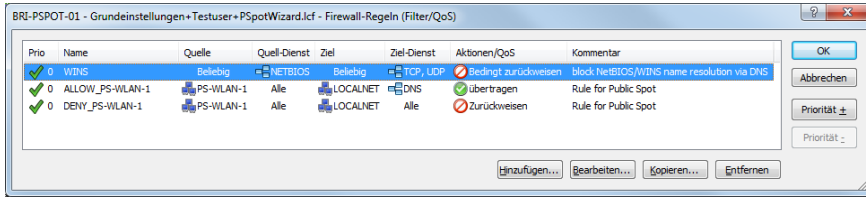
12. Erstellen Sie für den internen RADIUS-Server in der Anmelde-Server-Liste des Public Spots einen Eintrag. Unter **Auth.-Server IP-Adresse** und **Acc.-Server IP-Adresse** tragen Sie die Loopback-Adresse `127.0.0.1` ein; den **Auth.-Server Port** und den **Acc.-Server Port** entnehmen Sie dem Authentifizierungs-Port und Accouting-Port aus dem vorangegangenen Einstellungsdialog.
Der Listeneintrag ist notwendig, damit der Public Spot die Adresse des RADIUS-Servers kennt und er die Public Spot-Zugänge am internen RADIUS-Server authentifizieren kann.

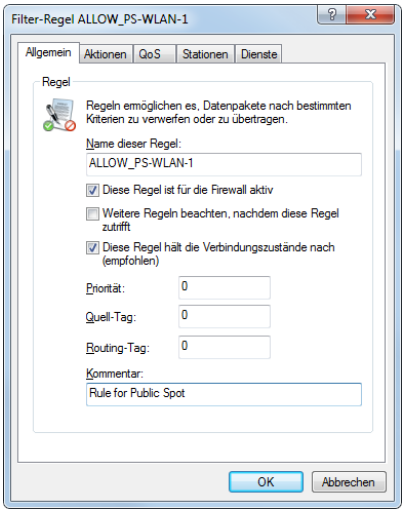
▶ LANconfig: **Public-Spot** > **Benutzer** > **Anmelde-Server**



13. Richten Sie zur Absichererung Ihrer lokalen Netzwerke Filterregeln für den Public Spot in der Firewall ein. Erstellen dazu jeweils eine Erlaubnisregel (z. B. `ALLOW_PS-WLAN-1`) und eine Verbotsregel (z. B. `DENY_PS-WLAN-1`).
Über die Erlaubnisregel gestatten Sie Geräten aus dem Public Spot-Netzwerk explizit, DNS-Anfragen in alle lokalen Netzwerke – z. B. Ihr lokales Intranet – zu senden. Über die Verbotsregel hingegen schließen Sie alle übrigen Zugriffe bzw. Anfragen aus dem Public Spot-Netz in Ihre lokalen Netzwerke generell aus. Die Reihenfolge – Erlaubnis vor Verbot – ist dabei essentiell, da die Firewall Regeln nach Priorität von oben nach unten anwendet.

   ▶ LANconfig: **Firewall/QoS** > **IPv4-Regeln** > **Regeln…**





▶ **Einstellungen für die Erlaubnisregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `ALLOW_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **ACCEPT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Aktivieren Sie unter **Dienste** > **Protokolle/Ziel-Dienste** die Option **folgende Protokolle/Ziel-Dienste** und wählen Sie **Hinzufügen…** > **DNS**.

g) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Erlaubnisregel daraufhin in die Regel-Tabelle ein.

► **Einstellungen für die Verbotsregel:**

a) Tragen Sie unter **Allgemein** den Namen der Regel ein, z. B. `DENY_PS-WLAN-1`.

b) Entfernen Sie alle eventuell voreingestellten Aktions-Objekte aus der Liste und fügen Sie über **Aktionen** > **Hinzufügen…** ein Aktions-Objekt vom Typ **REJECT** hinzu.

c) Aktivieren Sie unter **Stationen** > **Verbindungs-Quelle** die Option **Verbindungen von folgenden Stationen** und wählen Sie **Hinzufügen…** > **Benutzerdefinierte Station hinzufügen**.

d) Wählen Sie im sich öffnenden Stations-Dialog die Option **Alle Stationen im lokalen Netzwerk** und wählen Sie unter **Netzwerk-Name** den Namen Ihres Public Spot-IP-Netzwerks, z. B. `PS-WLAN-1`. Schließen Sie den Stations-Dialog mit **OK**.

e) Aktivieren Sie unter **Stationen** > **Verbindungs-Ziel** die Option **Verbindungen an folgende Stationen** und wählen Sie **Hinzufügen…** den Eintrag **LOCALNET**.

f) Beenden Sie den Filter-Regel-Dialog mit einem abschließenden Klick auf **OK**.
LANconfig trägt die Verbotsregel daraufhin in die Regel-Tabelle ein.

14. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Damit haben Sie Ihr Public Spot-Modul konfiguriert. Wenn Sie sich nun mit einem WLAN-fähigen Gerät in Reichweite des Public Spots begeben, kann das Gerät die eingerichtete SSID als öffentliches Netzwerk finden und sich an diesem anmelden.

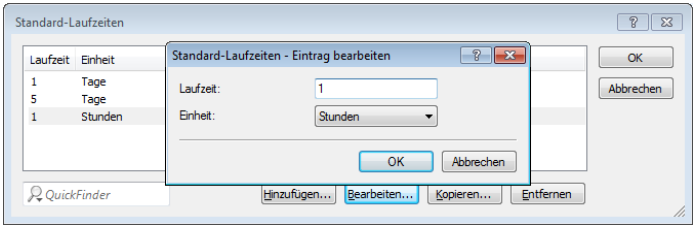
Standardwerte für den Public Spot-Assistenten setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für den **Benutzer-Erstellungs-Assistenten** (Setup-Wizard **Public-Spot-Benutzer einrichten**) an Ihre Bedürfnisse anpassen. Die hier definierten Werte stehen einem Public Spot-Administrator beim Einrichten neuer Benutzer und Voucher-Druck anschließend als Auswahlwerte zur Verfügung (Laufzeiten, Bandbreitenprofile, etc.).

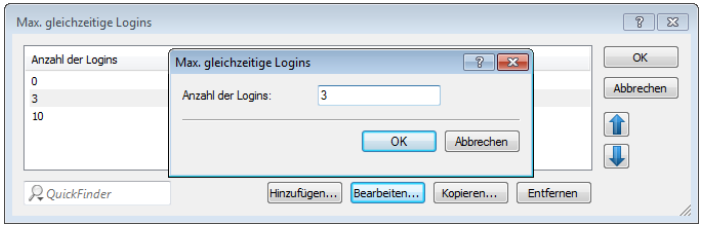
Hinweis: Ausgenommen davon sind die im untenstehenden Dialog abgebildeten Werte für Muster für Benutzernamen und Passwort-Länge, welche ausschließlich dem Gerät als Vorgabewerte dienen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.

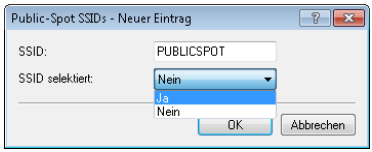
3. Definieren Sie unter **Standard-Laufzeiten**, welche auswählbaren Gültigkeiten von Benutzerkonten und Vouchern der Assistent standardmäßig anbietet.
   Der Benutzer-Erstellungs-Assistent verwendet die kürzeste Laufzeit als Standardwert.



4. Definieren Sie unter **Max. gleichzeitige Logins** die für den jeweiligen Benutzer zutreffende Anzal von Geräten, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen.
   Der Wert `0` steht dabei für 'Unbegrenzt'. Ob die mehrfache Anmeldung mit einem oder mehreren Geräten generell erlaubt ist, gibt der Public Spot-Administrator später beim Anlegen eines neues Benutzers über eine gesonderte Einstellung im Assistenten an.



5. Legen Sie unter **Muster für Benutzernamen** fest, nach welchem Muster der Benutzer-Erstellungs-Assistent den Benutzernamen erzeugt.
   Sie können bis zu 19 Zeichen vergeben, wobei der Assistent für die Variable "%n" für jeden Benutzer eine eindeutige Nummer vergibt. Für die Standardbezeichnung `user%n` erscheint auf dem Voucher später z. B. `user12345`.
6. Bestimmen Sie unter **Passwort-Länge** die Länge des Passwortes, das der Benutzer-Erstellungs-Assistent für den Public Spot-Zugang generiert. Standardmäßig beträgt die Länge 6 Zeichen. Wenn Sie längere Passwörter vergeben möchten, sollten Sie bedenken, dass dem Gast bei deren Eingabe Fehler passieren können, was zu unnötigen Problemen und Rückfragen führt.
7. Optional: Legen Sie unter **Bandbreitenprofile** Grenzen für den Up- und Downlink eines jeden Public Spot-Benutzers fest.
   Mehr zu dieser Einstellung erfahren Sie unter *Bandbreitenprofile verwalten* auf Seite 1474.
8. Nur Public Spot über WLAN: Bestimmen Sie unter **Public-Spot SSIDs** die Namen der Public Spot-Netzwerke, für die Sie mit dem Benutzer-Erstellungs-Assistent Benutzerkonten standardmäßig anlegen.



Der Benutzer-Erstellungs-Assistent markiert die als **SSID selektiert** festgelegten Netzwerknamen bei der Einrichtung neuer Public Spot-Benutzer automatisch vor. Sofern Sie beispielsweise einen Access Point oder WLAN Controller einsetzen, können Sie mehrere Netzwerknamen als Vorgabewert auswählen, um den Benutzern standardmäßig den Zugang zu mehreren WLANs zu bereitzustellen. Beim Erstellen eines neuen Benutzers und dem anschließenden Voucher-Druck erscheinen diese SSIDs ebenfalls auf dem ausgedruckten Ticket.

Über die Pfeil-Schaltflächen ändern Sie die Reihenfolge der angezeigten SSIDs. Oft genutzte SSIDs können Sie damit z. B. an die oberen Positionen verschieben.

Fertig! Damit ist die Konfiguration der Standardwerte für den Public Spot-Assistenten abgeschlossen.

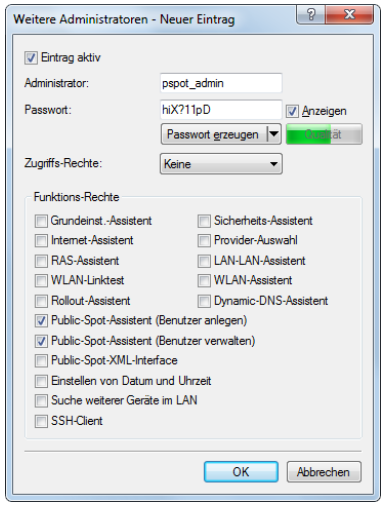
Beschränkten Administrator zur Public Spot-Verwaltung einrichten

Um Mitarbeitern auch ohne Zugriff auf die Gerätekonfiguration die Einrichtung und Verwaltung von Benutzern zu erlauben, haben Sie die Möglichkeit, einen beschränkten Administrator einzurichten, welcher ausschließlich über die Rechte zur Verwendung der *Public Spot-Assistenten* verfügt. Dieses Tutorial beschreibt die dafür erforderlichen Schritte sowie die notwendigen Zugriffs- und Funktionsrechte in LANconfig.

Da die Rechte zur Verwendung der Public Spot-Assistenten getrennt von einander konfigurierbar sind, lässt sich ein beschränkter Administrator auch auf einen einzelnen Assistenten einschränken. Im Falle des Benutzer-Erstellungs-Assistenten leitet das Gerät den beschränkten Administrator nach dem WEBconfig-Login dann automatisch an die entsprechende Eingabemaske weiter.

1. Öffnen Sie in LANconfig den Konfigurationsdialog des Gerätes, für das Sie einen Public Spot-Administrator hinzufügen wollen.
   In diesem Gerät muss das Public Spot-Modul aktiviert sein.
2. Wechseln Sie in die Ansicht **Management** > **Admin**. Klicken Sie im Abschnitt **Geräte-Konfiguration** auf **Weitere Administratoren** und klicken Sie anschließend **Hinzufügen**.

Wenn Sie einem vorhandenen Administrator die Public Spot-Verwaltung zuweisen möchten, markieren Sie dessen Tabelleneintrag und klicken stattdessen **Bearbeiten**.

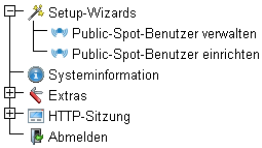


3. Aktivieren Sie das Profil, indem Sie die Option **Eintrag aktiv** markieren.
4. Vergeben Sie einen aussagekräftigen Namen im Feld **Administrator**.
5. Bestimmen Sie ein **Passwort** und wiederholen Sie es zur Kontrolle.
6. Setzen Sie die **Zugriffs-Rechte** auf **Keine**.
7. Aktivieren Sie im Abschnitt **Funktions-Rechte** die Optionen **Public-Spot-Assistent (Benutzer anlegen)** für den Benutzer-Erstellungs-Assistenten und **Public-Spot-Assistent (Benutzer verwalten)** für den Benutzer-Verwaltungs-Assistenten.

   Hinweis: Das Funktionsrecht **Public-Spot-XML-Interface** wird von einem Public Spot-Administrator nicht benötigt. Das Recht ist nur relevant, wenn Sie das XML-Interface verwenden und sollte auch dann aus Sicherheitsgründen nicht mit den oben beschriebenen Funktionsrechten kombiniert werden.

8. Speichern Sie das erstellte oder geänderte Administratorprofil mit einem Klick auf **OK**.

Sofern Sie die Funktions-Rechte für mehrere Assistenten gesetzt haben, kann der beschränkte Administrator in WEBconfig über die Navigationsleiste zwischen den Assistenten navigieren.



Sofern Sie ausschließlich das Funktionsrecht **Public-Spot-Assistent (Benutzer anlegen)** gesetzt haben, kann ein beschränkter Administrator lediglich innerhalb des Benutzer-Erstellungs-Assistenten navigieren; die Navigationsleiste bleibt verborgen. Ein manuelles Abmelden über WEBconfig ist in diesem Fall nicht mehr möglich. Aus Sicherheitsgründen ist die Lebensdauer der WEBconfig-Sitzung daher sehr kurz gehalten. Bei entsprechender Inaktivität loggt das Gerät den beschränkten Administrator automatisch aus.

Hinweis: Aus technischen Gründen kann sich der Benutzer-Erstellungs-Assistent nach Verwenden der Schaltfläche **User anlegen und CSV-Export** nicht automatisch aktualisieren. Möchte ein beschränkter Administrator weitere Benutzer einrichten und Voucher ausdrucken, muss er den Assistenten neu aufrufen (z. B. via URL oder Aktualisieren der Webseite, wenn die Navigationsleiste verborgen ist).

Public-Spot-Benutzer für einfache Szenarien einrichten und verwalten

Sie haben die Möglichkeit, Public Spot-Benutzer sowohl von Hand als auch mit Hilfe der Setup-Wizards einzurichten und zu verwalten. Die Einrichtung und Verwaltung von Hand bietet Ihnen umfassendere Konfigurationsmöglichkeiten und erlaubt Ihnen z. B. das Anlegen selbstdefinierter Benutzer von unbegrenzter Lebensdauer.

Über die Setup-Wizards hingegen erstellen Sie generische Public Spot-Benutzer mit automatisch generierten Zugangsdaten von beschränkter Lebensdauer. Der betreffende Setup-Wizard ist ausschließlich über WEBconfig zugänglich, was Ihnen das schnelle Anlegen von Nutzern erlaubt, ohne dass

dafür allgemeine Administrationsrechte für das komplette Gerät erforderlich sind. Es wird lediglich ein Administrator mit beschränkten Rechten benötigt.

Es steht Ihnen natürlich auch frei, mit Hilfe des Setup-Wizards zunächst einen generischen Nutzer zu erzeugen und diesen dann manuell Ihren Bedürfnissen (z. B. Änderung des Benutzernamens) entsprechend anzupassen.

Einrichtung und Verwaltung über die Setup-Wizards (WEBconfig)

Die Setup-Wizards unterstützen Sie bei der einfachen Verwaltung von Public Spot-Benutzern.

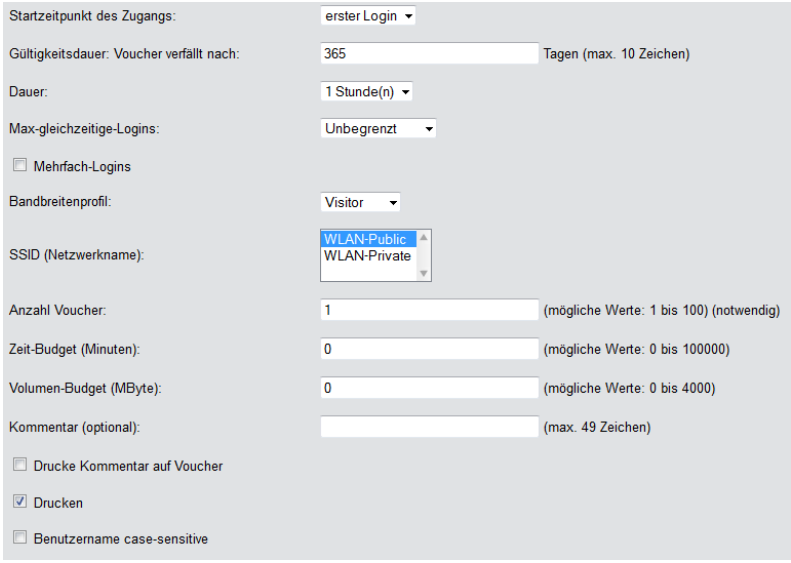
Public-Spot-Benutzer mit einem Klick hinzufügen und Voucher-Druck

Der folgende Abschnitt beschreibt die Einrichtung eines Public Spot-Benutzers über WEBconfig und den anschließenden Ausdruck des Vouchers. Sie können Voucher dabei auch auf Vorrat anlegen.

Hinweis: Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer anlegen)**, um einen neuen Public Spot-Benutzer anzulegen.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer einrichten**.

3. Der Benutzer-Erstellungs-Assistent startet mit der Eingabemaske. Die Felder sind mit Standardwerten vorbelegt.



Der Assistent vergibt daraufhin automatisch einen Nutzernamen und ein Zugangs-Passwort. Im anschließenden Druck-Dialog können Sie den Voucher-Drucker auswählen und den Voucher ausdrucken.

4. Ändern Sie ggf. vor dem Druck die Standardwerte den Anforderungen entsprechend.

   Die folgenden Einträge beeinflussen sowohl Aussehen als auch Gültigkeit des Vouchers:

   - **Startzeitpunkt des Zugangs**: Legt fest, ab wann der Voucher gültig ist. In der Einstellung **erster Login** gilt der Zugang ab Erstanmeldung; in der Einstellung **sofort** ab Anlegen des Benutzers.

     Um mehrere Vouchers auf Vorrat anzulegen, wählen Sie hier als Gültigkeit des Vouchers `erster Login`. Somit stellen Sie sicher, dass die Vouchers auch nach längerer Vorhaltezeit ihre Gültigkeit behalten.

   - **Gültigkeitsdauer: Voucher verfällt nach**: Geben Sie die Dauer an, nach der der Voucher ungültig wird. Es ist nicht möglich, eine Gültigkeitsdauer einzutragen, wenn der Zugang ab sofort gültig ist.

- **Dauer**: Wählen Sie die Dauer aus, für die dieser Zugang ab Erstanmeldung oder Anlegen des Benutzers gültig ist. Die hier aufgelisteten Einträge verwalten Sie in der **Default-Laufzeit**-Tabelle.
- **Max-gleichzeitige-Logins**: Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Die hier aufgelisteten Einträge verwalten Sie in der **Max-gleichzeitige-Logins-Tabelle**.
- **Mehrfach-Logins**: Aktivieren Sie diese Option, um dem Benutzer die Anmeldung mehrerer Geräte mit den selben Zugangsdaten generell zu erlauben. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über die Auswahlliste **Max-gleichzeitige-Logins** fest.
- **Bandbreitenprofil**: Wählen Sie aus der Liste ein Bandbreitenprofil, um die dem Nutzer zur Verfügung gestellte Bandbreite (Uplink und Downlink) selektiv zu beschränken. Banbreitenprofile legen Sie in der **Bandbreitenprofile**-Tabelle an.
- **SSID (Netzwerkname)**: Geben Sie an, für welches WLAN-Netz der Zugang gilt. Die hier aufgelisteten SSIDs verwalten Sie in der **SSID-Tabelle**. Durch drücken der "Strg"-Taste haben Sie die Möglichkeit, mehrere Einträge auszuwählen. Standardeinträge sind bereits vormarkiert.

  Hinweis: Sofern Sie in der Tabelle keinen Eintrag definiert haben, blendet der Assistent diese Einstellungsmöglichkeit aus.

- **Anzahl Voucher**: Geben Sie an, wie viele Vouchers Sie gleichzeitig erstellen möchten. Wenn Sie den ersten Login als Startzeitpunkt des Zugangs festgelegt haben, können Sie hierüber mehrere Vouchers "auf Vorrat" ausdrucken.
- **Zeit-Budget (Minuten)**: Geben Sie an, nach welcher Online-Zeit der Public Spot-Zugang schließt. Je nach gewählter Ablauf-Methode bestimmt entweder dieses Zeit-Budget (inkrementell) oder die eingestellte Voucher-Zugangsdauer (absolut) die Frist für den Zugang.
- **Volumen-Budget (MByte)**: Geben Sie an, nach welcher übertragenen Datenmenge der Zugang schließt.
- **Kommentar (optional)**: Fügen Sie einen Kommentar ein. Dieser Kommentar kann zum Beispiel weitere Hinweise zur Zugangsdauer oder die Telefonnummer der Rezeption bei Zugangsproblemen beinhalten.

- **Drucke Kommentar auf Voucher**: Aktivieren Sie diese Option, damit der Kommentar auf dem Voucher erscheint.
- **Drucken:** Aktivieren Sie diese Option, damit Sie beim Speichern gleichzeitig die registrierten Vouchers ausdrucken.
- **Benutzername case-sensitive**: Aktivieren Sie diese Option, wenn der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten muss.

5. Wenn Sie die Default-Werte unverändert oder die neuen Werte übernehmen möchten, klicken Sie abschließend auf **Speichern und Drucken**.

   Wenn Sie die Option **Drucken** deaktiviert haben, zeigt Ihnen der Assistent nach der Registrierung eine Übersicht der neuen Public Spot-Benutzer. Sie erhalten dann noch einmal die Gelegenheit, die Vouchers auszudrucken.

   Über die Schaltfläche **Benutzerverwaltung aufrufen** gelangen Sie zum Setup-Wizard **Public-Spot-Benutzer verwalten**.

   Hinweis: Diese Schaltfläche können Sie wahlweise anzeigen lassen oder ausblenden. Als Default ist sie eingeblendet.

Assistent zum Verwalten von Public Spot-Benutzern

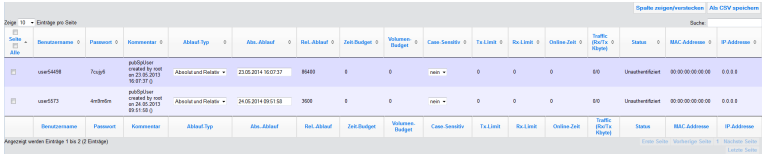
Der folgende Abschnitt beschreibt die Verwaltung von registrierten Public Spot-Benutzern über WEBconfig.

Hinweis: Sie benötigen das Zugriffsrecht **Public-Spot-Assistent (Benutzer verwalten)**, um Public Spot-Benutzer verwalten zu können.

Hinweis: Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten beenden.

1. Melden Sie sich auf der Startseite von WEBconfig als Public Spot-Administrator an.
2. Starten Sie den Setup-Assistenten mit einem Klick auf **Setup-Wizards** > **Public-Spot-Benutzer verwalten**.

3. Der Public Spot-Assistent startet mit einer Liste der registrierten Public Spot-Benutzer.



In der Auswahlliste **Zeige ... Einträge pro Seite** stellen Sie die Anzahl angezeigter Einträge pro Seite ein. Die entsprechenden Seiten rufen Sie über die Seitennavigation rechts unten auf:

- **Erste Seite**: Zeigt die Seite mit den ersten Einträgen an.
- **Vorherige Seite**: Wechselt eine Seite zurück.
- **Seitennummern (1, 2, 3,...)**: Wechselt direkt zur gewählten Seite.
- **Nächste Seite**: Wechselt eine Seite weiter.
- **Letzte Seite**: Zeigt die Seite mit den letzten Einträgen an.

Über **Suche** filtern Sie die angezeigten Einträge. Der Filter führt eingegebene Zeichenfolgen sofort aus.

Markierte Einträge exportieren Sie über **Als CSV speichern**.

Die Tabellenspalten haben folgende Bedeutungen:

- **Seite/Alle**: In dieser Spalte markieren Sie den Benutzer für die gewünschte Aktion (Drucken, Löschen, Speichern). Um alle Einträge der aktuellen Seite auszuwählen, markieren Sie **Seite**. Um alle Einträge komplett auszuwählen, markieren Sie **Alle**.

- **Benutzername**: Zeigt den manuell oder automatisch vom System vergebenen Benutzernamen an.
- **Passwort**: Zeigt das manuell oder vom System vergebene Passwort an.
- **Kommentar**: Beinhaltet sowohl den bei der Registrierung angegebenen Kommentar (in Klammern) sowie Änderungen an den Benutzer-Daten (automatisch vom System dokumentiert).
- **Ablauf-Typ**: Zeigt an, ob die Gültigkeitsdauer dieses Benutzer-Accounts absolut (fester Zeitpunkt) oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) festgelegt ist.
- **Abs.-Ablauf**: Wenn der Ablauf-Typ "Absolut" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts zu dem in diesem Feld angegebenen Zeitpunkt.
- **Rel.-Ablauf**: Wenn der Ablauf-Typ "Relativ" aktiviert ist, endet die Gültigkeit dieses Benutzer-Accounts nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.
- **Zeit-Budget**: Gibt die maximale Nutzungsdauer für diesen Benutzer-Account an. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Volumen-Budget**: Gibt das maximale Datenvolumen für diesen Benutzer-Account an. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.
- **Case-Sensitiv**: Gibt an, ob die Anmeldeseite die Groß- und Kleinschreibung des jeweiligen Benutzernamen berücksichtigt.
- **Tx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Sende-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Rx-Limit**: Sofern beim Erstellen des Benutzers ein Bandbreitenprofil vergeben wurde, zeigt dieser Eintrag die maximale Empfangs-Bandbreite an, die dem Benutzer zur Verfügung steht.
- **Traffic (Rx/Tx Kbyte)**: Zeigt die Datenmenge in Kilobyte an, die der betreffende Benutzer bisher empfangen (Rx) bzw. gesendet (Tx) hat.
- **Status**: Zeigt den Authentifizierungsstatus der einzelnen Benutzer an, also ob der Benutzer derzeit am Public Spot angemeldet ist (**Authentifiziert**) oder nicht (**Unauthentifiziert**).
- **MAC-Addresse**: Zeigt die physikalische Adresse der Netzwerkkarte des Benutzers, mit der Nutzer derzeit verbunden ist.

- **IP-Address**: Zeigt die IPv4-Adresse, die das System dem Benutzer derzeit zugewiesen hat.

Die Schaltflächen am unteren Fensterrand besitzen folgende Funktionen:

- **Drucken**: Drucken Sie die Vouchers der markierten Benutzer aus.
- **Löschen**: Löschen Sie die markierten Benutzer.
- **Speichern**: Speichern Sie die Änderungen.
- **Zurück zur Hauptseite**: Wechseln Sie zur Hauptseite zurück, wobei alle ungespeicherten Änderungen verloren gehen.

Folgenden Angaben eines Benutzers passen Sie an, indem Sie die Inhalte der entsprechenden Felder ändern:

- **Ablauf-Typ**
- **Abs.-Ablauf**
- **Case-Sensitiv**

4. Markieren Sie den zu ändernden Benutzer in der ersten Spalte.
5. Ändern Sie die entsprechenden Feldinhalte, und klicken Sie auf **Speichern**, um diese Änderungen zu übernehmen. Ungespeicherte Änderungen gehen verloren, sobald Sie diesen Assistenten verlassen.
6. Wenn Sie einen Benutzer löschen möchten, markieren Sie den entsprechenden Eintrag in der ersten Spalte, und klicken Sie auf **Löschen**

   Hinweis: Die Löschung eines Eintrags erfolgt ohne vorherige Rückfrage.

Felder mit WEBconfig ausblenden

Im Setup-Assistenten "Public-Spot-Benutzer verwalten" haben Sie über die Schaltfläche **Spalte zeigen/verstecken** die Möglichkeit, Tabellenspalten ein- oder auszublenden. Diese Änderungen sind jedoch nur temporär. Nach einem Seiten-Refresh oder bei einer neuen Sitzung werden die ausgeblendeten Spalten wieder angezeigt.

Um bestimmte Felder dauerhaft zu verbergen, wechseln Sie im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**. Standardmäßig werden alle Felder angezeigt. Blenden Sie bestimmte Felder aus, um z. B. das Zeit-Budget zu verbergen, bleiben diese Spalten sowohl im Assistenten selbst als auch im Dropdown-Menü unter der

Schaltfläche **Spalte zeigen/verstecken** nach einem erneuten Aufrufen der Seite verborgen.

Hinweis: Um einen authentisierten Public Spot-Benutzer zu löschen, müssen die Spalten "Rufende-Station-Id-Maske" und "Gerufene-Station-Id-Maske" im Assistenten sichtbar sein. Nicht authentisierte Benutzer hingegen lassen sich auch löschen, wenn beide Spalten ausgeblendet sind.

Beachten Sie bitte, dass ausgeblendete Felder beim Betätigen der Schaltfläche **Drucken** nicht mit ausgegeben werden. Die Ausgabe als CSV-Datei beinhaltet dagegen alle Daten. Sie haben jedoch die Möglichkeit, die Schaltfläche **Als CSV speichern** zu verbergen. Wechseln Sie dazu im LCOS-Menübaum zur Ansicht **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **CSV-Export-verstecken**. Wählen Sie "Ja" und speichern Sie Ihre Eingabe.

Manuelle Einrichtung und Verwaltung

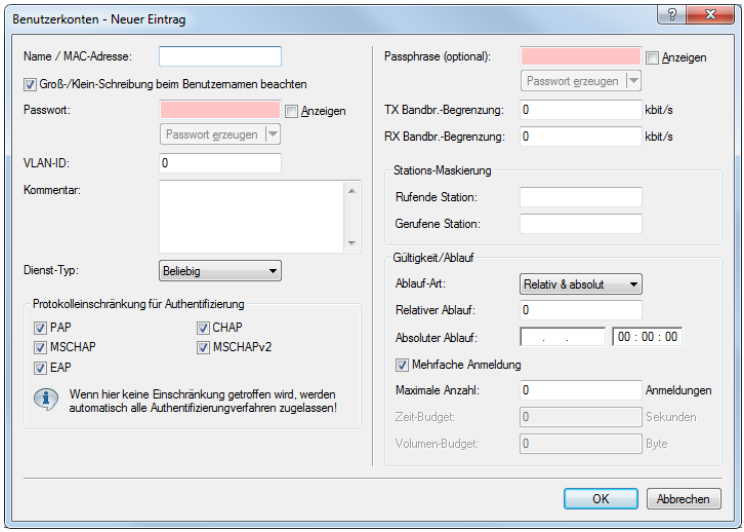
Die nachfolgenden Konfigurationsschritte zeigen Ihnen, wie Sie in LANconfig manuell einen Public Spot-Benutzer für einfache Einsatzszenarien einrichten. Public Spot-Nutzer erstellen und verwalten Sie über die **Benutzer-Datenbank** des geräteinternen RADIUS-Servers, erreichbar unter **RADIUS-Server** > **Allgemein**. Hier tragen Sie – aber auch die Setup-Wizards – alle Benutzer ein, die einen Zugang zum Public Spot erhalten sollen.

Hinweis: Das Public Spot-Modul verfügt für die Benutzerverwaltung noch über eine eigene, interne Liste (erreichbar unter **Public-Spot** > **Benutzer** > **Benutzer-Liste**). Im Zuge der technischen Entwicklung ist diese Liste seit HiLCOS 7.70 durch die Benutzerverwaltung via RADIUS ablöst. Aus Kompatibilitätsgründen wertet das Gerät die interne Benutzer-Liste des Public Spot-Moduls weiterhin aus, sofern Sie dies aktivieren. Für neue Installationen sollten Sie diese Liste jedoch nicht mehr verwenden, da Ihnen sonst zahlreiche Features nicht zur Verfügung stehen (Einrichtung und Verwaltung über die Assistenten, Bandbreiten-Begrenzung, Accounting via RADIUS, VLAN-IDs für Public Spot-Nutzer etc.).

1. Geben Sie unter **Name** den Benutzernamen des zukünftigen Nutzers oder die **MAC-Adresse** seines Endgerätes ein.

Wenn Sie als Authentifizierungs-Modus **Anmeldung mit Name und Passwort** gewählt haben, tragen Sie hier die Kennung ein, mit welcher sich der Nutzer am Public Spot authentisiert. Die Vergabe eines **Passworts** ist optional, ist für den obigen Authentifizierungs-Modus jedoch zu empfehlen.

▶ LANconfig: **RADIUS-Server** > **Allgemein** > **Benutzerkonten**



Hinweis: Sofern die Authentifizierung zusätzlich über die MAC-Adresse erfolgt (Authentifizierungs-Modus **Anmeldung mit Name, Passwort und MAC-Adresse**), definieren Sie die MAC-Adresse über das Feld **Rufende Station** in der Form `12:34:56:78:90:AB`.

2. Setzten Sie den **Dienst-Typ** auf `Anmeldung`.
3. Heben Sie sämtliche Protokolleinschränkungen auf, indem Sie alle Auswahlkästchen deselektieren.
   In einem Public Spot-Szenario findet eine Phase-2-Authentifizierung nicht statt. Diese kann lediglich für direkte WLAN-Verbindungen abseits eines Public Spot-Betriebs und die dazugehörigen RADIUS-Benutzer sinnvoll sein.

Hinweis: Wenn Sie die Protokolleinschränkungen nicht komplett aufheben, kann sich ein Nutzer nicht über die Login-Webseite Ihres Public Spots anmelden!

4. Optional: Auf Wunsch können Sie z. B. noch
   - im Abschnitt **Gültigkeit/Ablauf** ein relatives oder/und absolutes Ablaufdatum für die Gültigkeit des Benutzerkontos angeben (relativ = Gültigkeit in Sekunden nach erstem Login);
   - unter **TX/RX Bandbr.-Begrenzung Bandbreite** den Uplink/Downlink begrenzen;
   - die **Mehrfache Anmeldung** aktivieren und die **Maximale Anzahl** der Endgeräte angeben, die gleichzeitig über das Benutzerkonto angemeldet sein dürfen.
5. Speichern Sie die Konfiguation auf Ihrem Gerät.

Fertig! Ihre Public Spot-Nutzer können sich nun mit den von Ihnen festgelegten Zugangsdaten am Public Spot anmelden.

14.2.2 Sicherheitseinstellungen

Der Public Spot verfügt über zwei zusätzliche Schutzmechanismen, die ihn wirksam gegen Missbrauch absichern.

Traffic-Limit-Option

Um die Anmeldung am Public Spot über den Browser zu ermöglichen, ist es prinzipiell gestattet, dass auch unangemeldete Benutzer Datenpakete (z. B. DNS-Anfragen) an das Public Spot-Gerät senden. In der Standardeinstellung ist diese Datenmenge unbegrenzt. Daraus ergeben sich folgende Risiken:

- **Unberechtigte Nutzung des Public-Spots:** Mit geeigneten Tools könnte ein Benutzer alle Daten in ein DNS-Paket verpacken (also einen DNS-Tunnel aufbauen) und so einen Public Spot ohne Anmeldung nutzen.
- **Denial-of-Service:** Der Angreifer könnte erhebliche Datenmengen an das angegriffene Gerät senden und auf diese Weise versuchen, das Gerät bzw. den Public Spot zu blockieren.

- **Brute-Force:** Der Angreifer könnte versuchen, Zugang zur Basis-Station zu erhalten, indem er einfach so lange alle denkbaren Anmeldedaten durchprobiert, bis ihm der Zugang schließlich gelingt.

Die Traffic-Limit-Option ermöglicht, diese Risiken wirksam auszuschließen.

Sie aktivieren die Traffic-Limit-Option durch einen Wert ungleich "0". Der Wert bestimmt die maximale Datenmenge in Byte, die eine unangemeldetes Endgerät an den Public Spot senden und von ihm empfangen darf.

- LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung ermöglichen** > **Maximales Datenvolumen**

Sobald ein Endgerät dieses Transfervolumen überschreitet, sperrt der Public Sport dieses Gerät und verwirft fortan die von ihm empfangenen Daten ungeprüft. Diese Sperre erlischt erst wieder, wenn der zum Gerät gehörige Eintrag in der Stationstabelle verschwindet.

Hinweis: Bei WLAN-Geräten kann diese Löschung z. B. durch den Ablauf des allgemeinen Idle-Timeouts geschehen:

- WEBconfig: **HiLCOS-Menübaum** > **Setup** > **WLAN** > **Idle-Timeout**

Bitte beachten Sie, dass bei eingeschalteter Stationsüberwachung die Sperre möglicherweise auch schon früher entfernt wird. Ist eine Mobilstation 60 Sekunden lang unerreichbar, entfernt das Gerät dessen Eintrag aus der Stationstabelle und damit auch die Sperre.

Hinweis: Die Leerlaufzeitüberschreitung für das Public Spot-Modul erfüllt den gleichen Zweck wie der Idle-Timeout für WLAN, beschränkt sich allein auf Verbindungen über Public Spot. Ist die Leerlaufzeitüberschreitung gesetzt und kommen von einem Benutzer keine Datenpakete mehr, loggt das Gerät diesen nach Ablauf der eingetragenen Zeit automatisch aus.

- LANconfig: **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung**

Der optimale Wert des Traffic-Limits hängt zum einen von der Datengröße der Anmeldeseite ab. Zum anderen wirkt sich dieser Wert maßgeblich auf die mögliche Anzahl erfolgloser Anmeldeversuche durch einen Benutzer aus. Im Regelfall bewirkt ein Traffic-Limit von 60.000 Bytes den wirksamen Schutz des Public-Spots, lässt aber gleichzeitig eine ausreichende Anzahl von

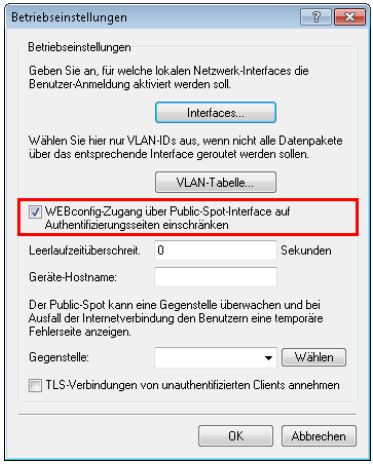
Anmeldeversuchen zu. Bei Bedarf können Sie diesen Wert den individuellen Bedürfnissen anpassen. Der Default-Wert von "0" Bytes steht für ein unbegrenztes Datenvolumen.

Hinweis: Die Traffic-Limit-Option überwacht ausschließlich den Datenverkehr vor der Anmeldung. Sie berücksichtigt nicht den Datenverkehr von und zu einem ggf. eingerichteten, freien Web-Server. Dieser bleibt zu jeder Zeit unlimitiert.

Konfigurationszugriff einschränken

Der Zugriff aus einem Public Spot-Netzwerk auf die Konfiguration eines Public Spots (WEBconfig) sollte aus Sicherheitsgründen immer ausgeschlossen sein. Mit einem speziellen Schalter besteht die Möglichkeit, den Zugang über Public Spot-Interfaces auf die Public Spot-Authentisierungsseiten zu reduzieren und automatisch alle anderen Konfigurationsprotokolle zu sperren.

- LANconfig: **Public-Spot** > **Server** > **Betriebseinstellungen** > **WEBconfig-Zugang über Public Spot-Interface auf Authentifizierungsseiten einschränken**



Hinweis: Bitte beachten Sie, dass Sie über die Zugriffsrechte unter **Management** > **Admin** > **Konfigurations-Zugriffs-Wege** > **Zugriffs-Rechte** nicht generell den Zugriff über HTTP(S) auf das Gerät einschränken.

14.2.3 Erweiterte Funktionen und Einstellungen

Der Public Spot beinhaltet zahlreiche erweiterte Funktionen, Optionen und Parameter, mit denen Sie ihn individuell an die spezifischen Eigenarten seines Einsatzgebietes anpassen können.

In den folgenden Abschnitten finden Sie Informationen über:

- Multiple Anmeldungen

  Standardmäßig ist die Nutzung von Zugangsdaten auf die Anmeldung mit einem Gerät beschränkt. Erfahren Sie, wie Sie diese Limit heraufsetzen oder die Beschränkung für ein Benutzerkonto komplett aufheben.

- Anmeldungsfreie Netze

  Richten Sie zusätzliche Netze ein, die ein Public Spot-Benutzer auch ohne Anmeldung am Public Spot erreichen kann, um um ihn online mit zusätzlichen Informationen (z. B. Kundenwebseite in einem Unternehmen, Veranstaltungskalender in einem Hotel) zu versorgen.

- Benutzerverwaltung über das Web-API

  Nutzen Sie URLs, um Public Spot-Benutzer über Datei-Verknüpfungen oder Skripte zu anzulegen und zu verwalten.

- Individuelle Begrenzung der Bandbreite

  Begrenzen Sie für jeden Public Spot-Nutzer individuell den ihm zugewiesenen Up- und Downlink.

- Automatische Bereinigung von Benutzerkonten und Mobilstationen

  Nutzen Sie die geräteeigenen Funktionen, um abgelaufene Public Spot-Benutzerkonten und nicht ordnungsgemäß abgemeldetete Mobilstationen (nur WLAN) automatisch aus den geräteinternen Datenbanken zu entfernen.

- Übergabe von WLAN-Sitzungen zwischen Geräten

Erfahren Sie mehr über die Roaming-Möglichkeiten von Mobilstationen zwischen einzelnen Access Points, und welche besonderen Konfigurationen notwendig sind, um Ihren Benutzern die unterbrechungsfreie Übergabe von WLAN-Sitzungen zu ermöglichen.

- Authentifizierung über RADIUS

  Erfahren Sie, wie Sie ein mehrere RADIUS-Server für Authentifizierung und Accounting bereitstellen, und wie Sie Server sinnvoll miteinander verketten, um im Falle der Unerreichbarkeit einzelner Systeme die Nutzerdaten an entsprechende Backup-Systeme weiterzuleiten.

- Abrechnung von Public Spot-Verbindungen im kommerziellen Betrieb

  Erfahren Sie mehr über die Abrechnungsfunktionen, die Ihnen der Public Spot für den kommerziellen Betrieb bereitstellt. Diese Abrechnungsfunktionen lassen sich grob in zwei Modelle unterteilen:

  - Bezahlung tatsächlich genutzter Ressourcen im Nachhinein (Kredit-Abrechnung)
  - Benutzung des Services auf Guthabenbasis (Debit-Abrechnung, Pre-Paid)

- Verwenden mehrstufiger Zertifikate

  Erfahren Sie, wie Sie SSL-Zertifikatsketten in Ihr Gerät laden.

- Individuelle Zuweisung von VLAN-IDs

  Erfahren Sie, wie Sie einzelnen Public Spot-Nutzern individuelle VLAN-IDs zuweisen.

Mehrfach-Logins

Sie haben die Möglichkeit, Public Spot-Benutzern zu gestatten, sich mit mehreren Geräten gleichzeitig auf ein Benutzerkonto einzuloggen. Dies kann dann erforderlich sein, wenn eine Gruppe von zusammengehörigen Personen (z. B. eine Familie) mehrere Geräte besitzt und diese zur gleichen Zeit für den Zugang ins Netz nutzen möchte.

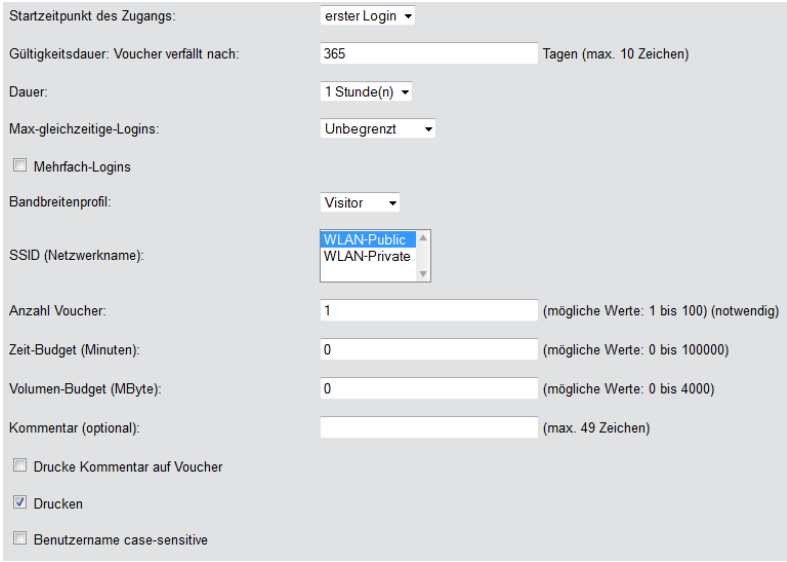
Standardwerte festlegen

Um diese Funktion zu verwenden, definieren Sie im ersten Schritt die mögliche Anzahl der gleichzeitig nutzbaren Geräte im Setup-Menü unter **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Max-gleichzeitige-Logins-Tabelle**. Hier tragen Sie jene Werte ein, die Sie im zweiten Schritt mit Hilfe des Assistenten **Public-Spot-Benutzer einrichten** zuweisen. Der Wert `0` steht dabei für "Unbegrenzt".

Auswahl der Mehrfach-Logins im Benutzer-Erstellungs-Assistenten

Wenn Sie den Assistenten **Public-Spot-Benutzer einrichten** aufrufen, finden Sie das Auswahlmenü **Max-gleichzeitige-Logins** vor. Die hier angezeigten Werte entsprechen den Zahlen, die Sie zuvor in der analog benannten Tabelle festgelegt haben. Die Zahlen werden innerhalb der Phrase "Nur...Gerät(e)" wiedergegeben.

Wählen Sie hier die für den jeweiligen Benutzer zutreffende Anzal von Geräten aus, die maximal gleichzeitig auf das Benutzerkonto zugreifen dürfen. Beachten Sie, dass für die Aktivierung der Funktion zusätzlich noch die Option **Mehrfach-Logins** ausgewählt sein muss.



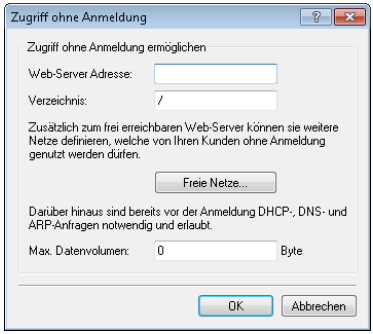
Anmeldungsfreie Netze

Um den Benutzern den Zugang zu wichtigen Informationen auch ohne Anmeldung zu ermöglichen (z. B. wichtige Kontaktinformationen), können Sie einen frei erreichbaren Web-Server definieren.

▶ LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung**

Falls Sie den hier definierten Server nicht vollständig freigegeben wollen, können Sie optional einen abweichenden Pfad auf dem Web-Server angeben:

▶ LANconfig: **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Verzeichnis**



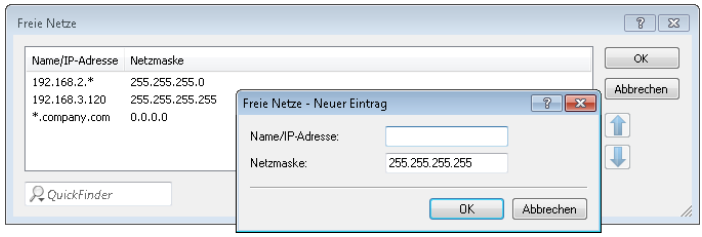
Zusätzlich zum frei erreichbaren Web-Server können Sie weitere Netze und Spezial-Seiten definieren, welche von Ihren Kunden ohne Anmeldung genutzt werden dürfen.

▶ **Public-Spot** > **Server** > **Zugriff ohne Anmeldung** > **Freie Netze**

Tragen Sie die IP-Adresse des zusätzlichen Servers oder Netzwerks inklusive Netzmaske ein, auf welche die Public Spot-Benutzer zugreifen dürfen. Alternativ haben Sie auch die Möglichkeit, Domain-Namen (mit oder ohne Wildcard "*") einzutragen. Durch Wildcards können Sie z. B. auch den freien Zugriff auf alle Subdomains einer Domäne erlauben. Der Eintrag `*.company.com` gibt somit auch die Adressen `mail.company.com`, `service.company.com` etc. frei.

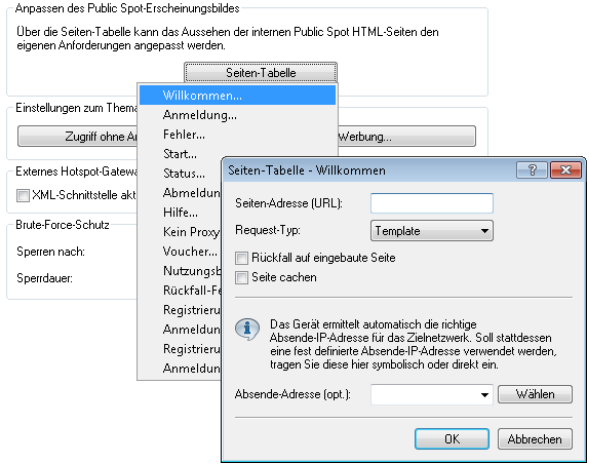
Wenn Sie nur eine einzelne Station mit der zuvor benannten Adresse oder eine Domain freischalten wollen, geben Sie als Netzmaske `255.255.255.255` ein. Wenn Sie ein ganzes IP-Netz freigeben wollen,

geben Sie dafür die zugehörige Netzmaske an. Sofern Sie keine Netzmaske setzen (Wert `0.0.0.0`), ignoriert das Gerät den betreffenden Tabelleneintrag.



▶ **Public-Spot** > **Server** > **Seiten-Tabelle**

Tragen Sie die Adressen (URL) der Webseiten ein, die der Public Spot dem Benutzer für die Anmeldung, Fehlermeldungen, Status usw. anzeigen soll. Lesen Sie dazu auch das Kapitel über *geräteeigene und individuelle Authentifizierungsseiten*.



DNS-Snooping

Webdienste mit hohen Nutzerzahlen verteilen die Datenanfragen zur besseren Auslastung auf mehrere Server. So kommt es, dass zwei DNS-Anfragen für denselben Hostnamen (z. B. "www.google.de") zu zwei unterschiedlichen IP-Adressen führen können. Erhält der Public Spot für einen eingegebenen Hostnamen vom zuständigen DNS-Server nun mehrere gültige IP-Adressen,

wählt er davon eine aus und speichert sie für zukünftige Anfragen von Public Spot-Benutzern. Bekommt der Benutzer jedoch bei einer weiteren Anfrage für denselben Hostnamen die IP-Adresse eines anderen Servers zugeteilt, sperrt der Public Spot diese Verbindung, weil er diese IP-Adresse nicht als zugangsberechtigt gespeichert hat.

Damit Public Spot-Benutzer sich trotz wechselnder IP-Adressen mit dem angefragten Host verbinden können, analysiert der Public Spot die DNS-Anfragen der Benutzer und speichert die jeweils zurückgegebene IP-Adresse zusammen mit dem Hostnamen, der Gültigkeitsdauer (TTL: "Time to Live"), dem Alter und der Datenquelle fortan als freie Zieladresse in der Tabelle **Status** > **Public-Spot** > **Freie-Hosts**.

Die Einträge in dieser Tabelle verfallen nach der in der DNS-Antwort übertragenen Gültigkeitsdauer (TTL). Um bei sehr niedrigen Werten (z. B. 5 Sekunden) den Public Spot-Benutzer nicht sofort nach einer Anfrage wieder auszusperren, können Sie unter **Setup** > **Public-Spot-Modul** > **Freie-Hosts-Minimal-TTL** eine Mindest-Gültigkeitsdauer festlegen.

Verwaltung von Public Spot-Nutzern über das Web-API

Über die Eingabe einer speziellen URL in der Adresszeile haben Sie die Möglichkeit, Public Spot-Benutzer direkt statt über den Setup-Assistenten anzuzeigen, neu anzulegen oder zu löschen.

URL-Aufbau

Die URL hat folgenden Aufbau:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=actiontodo&parameter1=value1&parameter2=value2
```

Die folgenden Aktionen stehen Ihnen zur Verfügung:

- **action=addpbspotuser**: legt einen oder mehrere neue Public Spot-Benutzer an und druckt anschließend Vouchers in der benötigten Anzahl.
- **action=delpbspotuser**: löscht den Public Spot-Benutzer mit der angegebenen Benutzer-ID.

- **action=editpbspotuser**: zeigt einen Public Spot-Benutzer an, dessen Benutzer-ID Sie mit übergeben haben. Anschließend können Sie den Voucher des Benutzers neu ausdrucken.

Die notwendigen Parameter und deren Werte sind abhängig von der angegebenen Aktion.

Hinweis: Der Assistent ignoriert falsche Parameter-Angaben und übernimmt ausschließlich die korrekten Parameter. Falls Sie einen erforderlichen Parameter falsch angegeben oder ausgelassen haben, zeigt der Assistent eine Eingabemaske. Tragen Sie in diese den korrekten Parameter-Wert ein.

Hinzufügen eines Public Spot-Benutzers

Über die folgende URL registrieren Sie einen neuen Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`comment`

Kommentar zum registrierten Benutzer

Sind für einen Public Spot-Benutzer mehrere Kommentare möglich, geben Sie die Kommentare und die entsprechenden Kommentarfeld-Namen wie folgt an:

```
&comment=<Inhalt1>:<Feldname1>,<Inhalt2>:<Feldname2>,…,<Inhalt5>:<Feldname5>,
```

Existiert ausschließlich ein Kommentarfeld pro Benutzer, genügt die Angabe des Kommentars:

```
&comment=<Kommentar>
```

Hinweis: Deutsche Umlaute werden nicht unterstützt.

Hinweis: Die maximale Zeichenanzahl des Kommentar-Parameters beträgt 191 Zeichen.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche, über die Sie den Voucher ausdrucken können.

`printcomment`

Kommentar auf den Voucher drucken.

Fehlt dieser Parameter, erscheint der Kommentar nicht auf dem Voucher (Default-Einstellung).

`nbGuests`

Anzahl der anzulegenden Public Spot-Benutzer.

Fehlt dieser Parameter, legt der Assistent ausschließlich einen Benutzer an (Default-Einstellung).

`defaults`

Default-Werte verwenden

Der Assistent ersetzt fehlende oder falsche Parameter durch Default-Werte.

`expirytype`

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both`und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die

maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`ssid`

Netzwerk-Name

Fehlt dieser Parameter, verwendet der Assistent den Standard-Netzwerk-Namen (Default-Einstellung).

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Die folgenden Angaben sind möglich:

- k oder K: Angabe in Kilobytes (kB), z. B. `volumebudget=1000k`.

- `m` oder `M`: Angabe in Megabytes (MB), z. B. `volumebudget=100m`.
- `g` oder `G`: Angabe in Gigabytes (GB), z. B. `volumebudget=1g`.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Fehlt dieser Parameter komplett, verwendet der Assistent den Default-Wert.

`multilogin`

Mehrfach-Logins

Wenn Sie diesen Parameter angeben, kann sich der Benutzer mehrfach mit seinem Benutzer-Account anmelden. Fehlt dieser Parameter, sind Mehrfach-Logins standardmäßig deaktiviert.

`maxconclogin`

Anzahl der maximal gleichzeitigen Logins

Mit diesem Parameter legen Sie fest, mit wie vielen Endgeräten parallel sich ein Nutzer am Public Spot anmelden kann. Gültige Werte sind Ganzzahlen wie z. B. `0, 1, 2, ….`

Fehlt dieser Parameter oder der Parameter hat den Wert `0`, ist dies gleichbedeutend mit einer unbegrenzten Anzahl von Endgeräten.

Hinweis: Dieser Parameter erfordert, dass Mehrfach-Logins erlaubt sind. Das Setzen dieses Parameters allein hat keine Auswirkungen.

`casesensitive`

Benutzername case-sensitive

Wenn Sie diesen Parameter angeben, muss der Public Spot-Nutzer bei der Anmeldung auf die Groß- und Kleinschreibung seines Benutzernamens achten. Gültige Werte sind:

- `0`: Benutzername case-sensitive ist deaktiviert
- `1`: Benutzername case-sensitive ist aktiviert

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`bandwidthprof`

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Hinweis: Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesen die fehlenden Werte ein.

Bearbeiten eines Public Spot-Benutzers

Über die folgende URL bearbeiten Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

Ihnen stehen folgende Parameter zur Verfügung:

`pbspotuser`

Name des Public Spot-Benutzers

Mehrere Benutzer geben Sie in der Form `&pbspotuser=<Benutzer1>+<Benutzer2>+...` an.

Findet der Assistent den angegebenen Benutzer nicht, haben Sie die Möglichkeit nach einem Benutzer suchen.

Nach der Änderung übernehmen Sie diese und drucken Sie diese ggf. zusätzlich aus.

`expirytype`

Kombinierte Angabe von Ablauf-Typ und ggf. Verfallsdauer des Vouchers.

Geben Sie diesen Parameter wie folgt an:

```
&expirytype=<Wert1>+validper=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Ablauf-Typ. Mögliche Werte sind `absolute`, `relative`, `both` und `none`.
- `Wert2`: Verfallsdauer des Vouchers, wenn `expirytype` den Wert `both` besitzt. In diesem Fall definieren Sie mittels `validper` die maximale Gültigkeit des Vouchers in Tagen für den absoluten Ablauf. Für alle anderen Ablauf-Typen wird der Parameter `validper` nicht gesetzt.

Fehlt ein Parameter oder geben Sie falsche Werte ein, setzt der Assistent die Default-Werte ein.

`unit`

Zugangsdauer

Geben Sie diesen Parameter wie folgt an:

```
&unit=<Wert1>+runtime=<Wert2>
```

Die Parameter-Werte haben folgende Bedeutung:

- `Wert1`: Einheit der Laufzeit. Mögliche Werte sind: Minute, Stunde, Tag
- `Wert2`: Laufzeit

`timebudget`

Zeit-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`volumebudget`

Volumen-Budget

Fehlt dieser Parameter, verwendet der Assistent den Default-Wert.

`print`

Automatischer Ausdruck des Vouchers.

Fehlt dieser Parameter, zeigt der Assistent anschließend eine entsprechende Schaltfläche. Über diese haben Sie die Möglichkeit den Voucher auszudrucken.

`bandwidthprof`

Bandbreitenprofil

Mit diesem Parameter weisen Sie einem Public Spot-Nutzer ein existierendes Bandbreitenprofil zu. Als gültigen Wert für diesen Parameter geben Sie die Zeilennummer eines unter **Setup** > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent** > **Bandbreitenprofile** angelegten Profilnamens an; z. B.

```
&bandwidthprof=1
```

für den ersten Eintrag in der Tabelle.

Fehlt dieser Parameter oder die Zeilennummer ist ungültig (die Tabelle ist z. B. leer), nimmt der Assistent kein Begrenzung der Bandbreite vor.

Hinweis: Sind für fehlende Parameter in der Public Spot-Verwaltung keine Default-Werte angegeben, öffnet Ihnen der Assistent einen entsprechenden Dialog. Tragen Sie in diesem die fehlenden Werte ein.

Löschen eines Public Spot-Benutzers

Über die folgende URL löschen Sie einen oder mehrere Public Spot-Benutzer:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=delpbspotuser&pbSpotuser=<Benutzer1>+<Benutzer2>+...
```

Findet der Assistent den angegebenen Benutzer in der Benutzer-Liste, löscht er ihn und gibt eine entsprechende Meldung aus.

Findet der Assistent den angegebenen Benutzer nicht, zeigt er Ihnen eine Tabelle der registrierten Public Spot-Benutzer. Markieren Sie in dieser die zu löschenden Einträge.

Public Spot-Benutzer auf einem entfernten Public Spot-Gateway anlegen

Bei der Verwendung von Smart Ticket erhält der Benutzer im RADIUS-Server des lokalen Public Spot-Gateways einen entsprechenden Public Spot-Account.

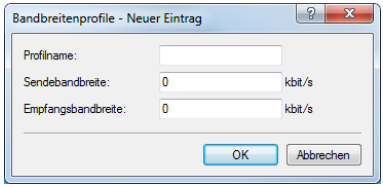
Sind jedoch mehrere Public Spot-Gateways im Einsatz und soll nur ein Gateway die Benutzerkonten in seinem RADIUS-Server vorhalten, wird der Public Spot-Account bei der Verwendung von Smart Ticket auf dem zentralen RADIUS-Server angelegt. Dazu ist es notwendig, das entfernte Public Spot-Gateway im LCOS-Menübaum unter **Setup** > **Public-Spot-Modul** > **Authentifizierungs-Module** festzulegen.

Hinweis: Sofern kein entferntes Public Spot-Gateway definiert wird, werden Public Spot-Benutzerkonten auf dem lokalen Public Spot-Gateway angelegt.

Bandbreitenprofile

Bandbreitenprofile verwalten

Über den Dialog **Public-Spot** > **Assistent** > **Bandbreitenprofile** haben Sie die Möglichkeit, Profile zur Beschränkung der Bandbreite (Uplink und Downlink) für Public Spot-Benutzer einzurichten. Diese Profile lassen sich neuen Benutzern beim Erstellen eines Zugangs für den Public Spot zuweisen, indem Sie im WEBconfig den Setup-Assistenten **Public-Spot-Benutzer einrichten** aufrufen.



Um die Einträge in der Tabelle **Bandbreitenprofile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

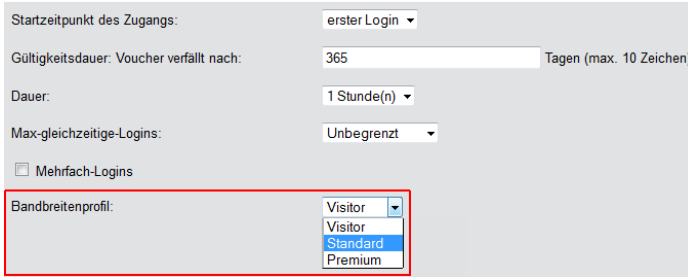
- **Profilname**: Geben Sie hier den Namen für das Bandbreitenprofil ein.

- **Sendebandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Uplink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.
- **Empfangsbandbreite**: Geben Sie hier die maximale Bandbreite (in KBit/s) ein, die einem Public Spot-Benutzer im Downlink zur Verfügung stehen soll. Um die Bandbreite auf z. B. 1 MBit/s zu beschränken, tragen Sie den Wert `1024` ein.

Bandbreitenprofile zuweisen

Die nachfolgenen Schritte erläutern, wie sie einem Public Spot-Nutzer eingerichtete Bandbreitenprofile zuweisen.

1. Öffnen Sie WEBconfig.
2. Starten Sie über **Setup-Wizards** > **Public Spot-Benutzer einrichten** den Benutzer-Erstellungs-Assistenten.
3. Weisen Sie dem neuen Benutzer aus der Auswahlliste **Bandbreitenprofil** ein entsprechendes Profl zu.



Beim Anlegen eines neuen Benutzers weist das RADIUS-Server dem dazugehörigen Konto automatisch die Ober- und Untergrenzen des betreffenden Bandbreitenprofils zu (nicht das Bandbreitenprofil an sich).

Benutzertabelle automatisch bereinigen

Das Gerät bietet Ihnen die Möglichkeit, abgelaufene Konten von Public Spot-Benutzern automatisch zu löschen.

Die Anwender des Public Spot-Assistenten haben als Administratoren in der Regel stark eingeschränkte Rechte und können Einträge in der Benutzertabelle

daher nicht selbst löschen. Da die Benutzertabelle nur eine bestimmte Anzahl von Einträgen umfasst, können veraltete Einträge die Kapazität des Public Spot ggf. einschränken. Die Aktivierung dieser Option ist somit dringend zu empfehlen.

Sofern Sie den internen RADIUS-Server für die Verwaltung der Benutzerkonten verwenden, aktivieren Sie die automatische Bereinigung unter **RADIUS-Server** > **Allgemein** > **Benutzertabelle automatisch bereinigen**.

Hinweis: Diese Einstellung hat keine Auswirkungen auf die Benutzertabelle eines externen RADIUS-Servers!

Stationsüberwachung

Bei eingeschalteter Stationsüberwachung überprüft der Public Spot regelmäßig alle angemeldeten Endgeräte daraufhin, ob sie auch tatsächlich erreichbar sind. Verschollene Endgeräte löscht er automatisch aus seiner lokalen Benutzertabelle. Bei ausgeschalteter Stationsüberwachung wird ein Benutzer erst dann abgemeldet, wenn die Gültigkeit seiner Authentifizierung abläuft.

Hinweis: Für kommerziell auf Zeitbasis betriebene Public-Spots ist die Stationsüberwachung außerordentlich wichtig. Bei solchen Installationen muss jederzeit gewährleistet sein, dass Benutzer nur für diejenigen Zeiten bezahlen, in denen sie die Dienste des Public-Spots auch tatsächlich in Anspruch genommen haben.

Konfiguration

Die Stationsüberwachung des Public Spot-Moduls ist standardmäßig deaktiviert. Sie aktivieren sie, indem Sie unter **Public-Spot** > **Server** > **Interface-Auswahl** > **Leerlaufzeitüberschreitung** einen Wert größer `0` – dieser Wert deaktiviert die Funktion – eintragen. Fortan werden alle Endgeräte nach einer bestimmten Zeit der Inaktivität automatisch vom Public Spot getrennt.

Hinweis: Sofern Ihr Gerät über Wireless LAN verfügt, haben Sie zusätzlich die Möglichkeit, eine Stationsüberwachung global für alle WLAN-Schnittstellen zu aktivieren. Die dazugehörige Einstellung finden Sie unter **Wireless LAN** >

Security > **Stationen überwachen, um inaktive Stationen zu erkennen**. Hierbei meldet das Gerät Mobilstationen nach spätestens 60 Sekunden ab (Vorgabewert); bei deaktivierter WLAN-Stationsüberwachtung kann dies hingegen bis zu einer Stunde dauern.

Sofern Sie Public-Spot über WLAN anbieten, beachten Sie bitte, dass die Stationsüberwachung für WLAN der für Public Spot übergeordnet ist, und eine Trennung früher erfolgen kann, wenn die Leerlaufzeitüberschreitung für WLAN (im Setup-Menü einstellbar unter **WLAN** > **Idle-Timeout**) geringer ist als die für Public Spot.

Überwachung

Im laufenden Betrieb können Sie den Public Spot via WEBconfig überwachen. Die Stations-Tabelle im Benutzer-Authentifizierungs-Menü gibt eine Aufstellung der

- aktuell am Public Spot angemeldeten Benutzer und der
- nicht angemeldeten Endgeräte im Netzwerk.

Sie erreichen die Stations-Tabelle im Status-Menü unter **Public-Spot** > **Stations-Tabelle**. Mit der Schaltfläche **Diese Tabelle beobachten** erneuern Sie die Ansicht der Tabelle automatisch und regelmäßig.

Übergabe von WLAN-Sitzungen zwischen Geräten

Wann immer der mit Hotspots zu versorgende Bereich größer wird, kann es erforderlich sein, mehr als nur einen Access Point einzusetzen. Eine mögliche Variante ist dann, ein zentrales Gerät für die Authentifizierung einzurichten, allein auf diesem Gerät das Public Spot-Modul zu aktivieren, und alle anderen Access Points dazu aufzufordern, die entsprechenden Anfragen an das zentrale Gerät weiterzuleiten. Damit fungieren alle übrigen Access Points als einfache, transparente Bridges, welche sich über das Ethernet-Backbone mit diesem zentralen Gateway verbinden. Das versetzt Benutzer in die Lage, sich mit Ihren Clients frei zwischen den Access Points zu bewegen, da alle Session-Informationen in dem zentralen Gateway gespeichert werden.

Diese Variante hat allerdings auch zwei Nachteile:

- Das zentrale Gateway ist ein "single point of failure" und skaliert zudem nicht mit den Anforderungen. Durch den Einsatz von VRRP zum Aufbau einer Redundanz-Lösung lässt sich das Ausfallrisiko minimieren.

  Hinweis: Da über VRRP keine Konfigurationen – wie z. B. die Benutzerdatenbank – abgeglichen werden, bedarf diese Lösung eines externen RADIUS-Servers. Dadurch stehen Ihnen jedoch auch bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht mehr zur Verfügung.

- Roaming ist nur dann notwendig, wenn das Public Spot-Modul in den Access Points selbst eingerichtet ist. Wenn Sie einen WLAN-Controller verwenden, kann die Authentifizierung zum zentralen Gateway weitergeleitet werden. In diesem Fall ist das Roaming zwischen den Access Points für den WLAN-Controller transparent.

Eine Alternative zu diesem zentralisierten Aufbau ist das Aktivieren des Public Spot-Moduls in allen Access Points. Die Authentifizierung und Seiten-Ablaufsteuerung ist dadurch auf alle Geräte verteilt, und es existiert kein "single point of failure".

Inter Access Point Protocol (IAPP)

Da das Public Spot-Modul als eine "schaltbare" transparente Brigde implementiert ist, benötigen Clients keine neue IP-Adresse, wenn sie zu einem neuem Access Point roamen; offene Verbindungen werden daher auch nicht getrennt. Daraus ergibt sich allerdings die Anforderung, dass sich ein einmal authentifizierter Client nach dem Roamen zu einem anderen Access Point nicht erneut authentifizieren braucht. Die Authentifizierungsinformationen sollten also vom alten zum neuen Access Point mitgenommen werden.

Um Informationen über die roamenden Clients auszutauschen, verwenden Access Points deshalb das sogenannte Inter Access Point Protocol (IAPP): Wann immer ein WLAN-Client zu einem anderen Access Point wechselt, hat er die Möglichkeit, dem neuen Access Point mitzuteilen, mit welchem Access Point er vorher verbunden war. Diese Information erlauben – zusammen mit den regulären Hello-Paketen aus dem Ethernet-Backbone – dem neuen Access Point, den alten Access Point über den Wechsel zu informieren. Der alte Access Point kann daraufhin den Client aus seiner Stationstabelle austragen und die Übergabe bestätigen.

Sollte ein Client für die Verbindung zum neuen Access Point das entsprechende Reassociate-Paket nicht verwenden, sendet der neue Access Point eine Multicast-Übergabeanfrage über den Backbone, statt die Anfrage direkt an den alten Access Point zu richten. Daher funktioniert eine Übergabe auch für Clients, die das IAPP nicht unterstützen.

Die Hauptaufgabe des IAPPs in einem WLAN ist, den alten Access Point anzuweisen, keine Pakete mehr an den entsprechenden Client in seinem Funkbereich zu senden, weil dieser sie nicht mehr empfängt. Ein solches Verhalten könnte andernfalls (aufgrund der Beschaffenheit des 802.11-Frame-Austausch-Protokolls) zu Beeinträchtigungen der anderen mit ihm verbundenen Clients führen.

Wenn das Public Spot-Modul verwendet wird, dient der Kommunikationskanal, den das IAPP liefert, als Übertragungsmedium für Sitzungsinformationen über die WLAN-Clients. Immer dann, wenn ein Access Point eine Übergabeanfrage für einen seiner Clients erhält und für diesen Client über Sitzungsinformationen in seiner Stationstabelle verfügt, leitet er diese Informationen an den anfragenden Access Point weiter. Diese Information beinhalten:

- Den aktuellen Zustand des Clients (authentifiziert oder nicht authentifiziert)

  Für den Fall, dass der Client authentifiziert ist, zusätzlich noch:

  - Den zur Authentifizierung verwendeten Benutzernamen
  - Den bisher vom Client erzeugten Datenverkehr
  - Die bisher verstrichene Sitzungsdauer
  - Die IP-Adresse des Clients
  - Mögliche Limits zu Sitzungsdauer und Datenvolumen
  - Mögliche Angaben zur Leerlauf-Zeitüberschreitung

- Wenn RADIUS-Accounting für die Sitzung verwendet wurde:

  - Den für das RADIUS-Accounting verwendeten Eintrag in der Anmelde-Server-Liste, referenziert durch den Namen
  - Den für die Interim-Updates verwendeten Accounting-Zyklus

Nach erfolgreicher Übergabe beendet der alte Access Point die Sitzung; d. h. er sendet im Falle von RADIUS-Accounting eine Accounting-Stop-Anfrage an den RADIUS-Accounting-Server. Diese ist erforderlich, da ein RADIUS-Server die NAS-Identifizierung nutzen kann, um Anfragen bestimmten Sitzungen zuzuordnen, und er diese Anfragen nicht mehr der richtigen Sitzung

zuordnen kann, sobald er die Datenpakete zu einer Sitzung von mehreren Geräten bekommt. Wenn ein Access Point diese Informationen in einer Übergabeantwort erhält, markiert er den Client sofort als authentifiziert und startet nach Möglichkeit eine neue RADIUS-Accounting-Session.

Hinweis: Beachten Sie, dass der neue Access Point einen entsprechenden Eintrag in seiner **Anmelde-Server**-Liste benötigt, um die hierfür benötigten Informationen zu erhalten. Der für das Public Spot-Modul spezifische Teil einer Übergabeantwort ist durch ein "shared secret" geschützt, welches im Setup-Menü unter **Public-Spot-Modul** > **Roaming-Schluessel**. Diese Sicherheitsmaßnahme soll das Fälschen von Übergabeantworten verhindern. Ohne ein konfiguriertes Passwort hängt ein Access Point die oben angeführten Informationen nicht an eine Übergabeantwort an, was den Client zwingt, sich erneut zu authentifizieren.

Authentifizierung über RADIUS

RADIUS ist ein weitläufig anerkanntes Protokoll, um auch größeren Benutzergruppen den Zugang zu einem Server bereitzustellen. Ursprünglich für den Dial-in-Serverzugang über Telefonleitungen entwickelt, eignet sich das Konzept ebenfalls für den Authentifizierungsprozess eines Hotspots. In einem komplexeren Provider-Netzwerk lässt sich dadurch z. B. dieselbe Benutzerbasis sowohl für Zugänge über Dial-in als auch via Hotspot verwenden. RADIUS-Server und ihre Zugangsparameter konfigurieren Sie im Dialog **Public-Spot** > **Server** unter **Anmelde-Server**.

In bestimmten Szenarien kann es sinnvoll sein, mehr als nur einen RADIUS-Server einzusetzen. Generell wird ein RADIUS-Server durch seine IP-Adresse, den UPD-Port (typischerweise Port 1645 oder 1812) und das sogenannte "shared secret" spezifiziert. Dies ist eine beliebige Zeichenfolge, welche als Passwort für den Zugang zum Server fungiert. Nur Clients, die das shared secret kennen, können mit dem RADIUS-Server interagieren, da das Passwort des Benutzerkontos mit dem shared secret gehashed wird, anstatt es im Klartext zu übermitteln.

Die einfachste Transaktion zwischen einem RADIUS-Server und einem Client besteht aus dem Übermitteln der eingegebenen Benutzerdaten durch das Gerät und der Antwort des Server mit "ja" oder "nein". Das RADIUS-Protokoll erlaubt allerdings auch komplexere Antworten und Anfragen, bei denen die

Kommunikationspartner für Anfragen und Anworten eine variable Liste von Werten – sogenannte "Attribute" – verwendet. Im *Anhang* finden Sie eine Liste, welche Attribute Ihr Gerät an einen RADIUS-Server senden kann und welche Attribute einer RADIUS-Antwort Ihr Gerät versteht.

Multiple Anmelde-Server

Wie erwähnt, kann die Liste der Anmelde-Server mehr als nur einen Eintrag beinhalten. Es sind Szenarios denkbar, in denen ein Hotspot den Internetzugang für Kunden verschiedener Service-Provider (Anbieter) bereitstellt. Diese Anbieter haben möglichweise getrennte Benutzerdatenbanken und eigene RADIUS-Server. Das Gerät muss dann anhand des Benutzernamens entscheiden, welcher Anbieter zum betreffenden Benutzer gehört.

Immer, wenn das Gerät für einen zu authentifizierenden Benutzer keinen Eintrag in eigenen, internen Benutzerliste vorfindet, geht es die Liste der Anmelde-Server durch und versucht den Anbieter zu finden, der zu dem betreffenden Benutzer gehört. Der Eintrag `Max.Mustermann@mydomain.de` enthält beispielsweise den Anmelde-Server-Eintrag `MYDOMAIN`. Scheitert diese erste Zuordnung, versucht das Gerät, dem Benutzer den Eintrag `DEFAULT` zuzuordnen. Sofern auch dieser Eintrag nicht existiert, wählt das Gerät den Anmelde-Server, in der Liste an erster Stelle steht. Findet das Gerät auch hier keinen Eintrag (d. h. die Liste ist leer), schlägt die Benutzerauthentifizierung fehl.

Unabhängig von der Zuordnung eines Benutzers zum Anmeldeserver übermittelt Ihr Gerät stets den vollen Benutzername an den ausgewählten RADIUS-Server. Der ausgewählte RADIUS-Server wird als Anbieter für die anschließende Sitzung gespeichert und für das optionale RADIUS-Accounting verwendet.

Verkettung von Backup-Servern

Internetanbieter wünschen sich eine hohe Verfügbarkeit ihres Angebots und eine übliche Methode, dies zu erreichen, ist Redundanz. Diese Redundanz wird über Backup-Servers erreicht, welche immer dann angefragt werden, wenn die Anfrage auf den primären Server eine Zeitüberschreitung erzeugt hat, z. B. weil der Server selbst oder andere Netzwerkkomponenten auf dem Weg dahin unerreichbar sind.

Der Bedarf an Backup-Servern variiert dabei stark zwischen den unterschiedlichen Anbietern, weshalb die Liste der Anmeldeserver keine fixe Anzahl von Eingabefeldern vorgibt. Stattdessen bietet Ihnen das Gerät eine Verkettung von Backup-Servern an (Backup-Chaining). Hierbei werden zwei oder mehr Einträge der Anmelde-Server-Liste miteinander verkettet, um eine Abfolge von RADIUS-Servern zu erstellen. Das Gerät arbeitet diese Liste Glied für Glied ab, bis es das Ende erreicht hat (Scheitern der Authentifizierung wegen Nicht-Erreichbarkeit des Servers) oder eine Antwort erhält (entweder Positiv oder Negativ).

Sie verketten Backup-Server über das Eingabefeld **Backup-Name** im Hinzufügen-/Bearbeiten-Dialog unter **Public-Spot** > **Server** > **Anmelde-Server**. Wann immer eine RADIUS-Anfrage scheitert (also eine Zeitüberschreitung erzeugt), prüft das Gerät das Backup-Feld und versucht, den darin referenzierten Server zu erreichen. Grundsätzlich lässt sich damit eine beliebige Anzahl von Servern miteinander verketten, wodurch auch die Möglichkeit besteht, mehreren Providern denselben Fallback-Server zuzuweisen. Die Kette von Backup-Servern wird dann abgebrochen, wenn eines der folgenden Ereignisse auftritt:

- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein leeres Backup-Feld.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste hat ein ungültiges Backup-Feld, der referenzierte Eintrag lässt sich also nicht in der Anmelde-Server-Liste finden.
- Das Anfragen eines RADIUS-Servers ist fehlgeschlagen und der dazugehörige Eintrag der Anmelde-Server-Liste referenziert einen Eintrag, den das Gerät bereits zu erreichen versucht hat. Dadurch werden endlose RADIUS-Anfragen durch Kreisverkettungen verhindert. Es ist möglich, dass zwei RADIUS-Server einander als Backup angeben, während der primäre Server durch den Benutzernamen gewählt wird.

Hinweis: Während das Gerät eine RADIUS-Anfrage sendet, bleibt die TCP/HTTP-Verbindung zum Client weiterhin bestehen. Überschreitet die Laufzeit der Verkettung irgendwann die Laufzeit der TCP/HTTP-Verbindung, bricht der Client den Anmeldeversuch ab. Es kann daher empfehlenswert sein, die Zahl der Anfrage-Wiederholungen an die einzelnen Backup-Server sowie die Zeitspanne zwischen Anfragen zu verringern. Sie tätigen diese Einstellungen im Dialog **RADIUS-Server** > **Optionen**.

Abrechnung ohne RADIUS-Accounting-Server

Sofern die Benutzerverwaltung über die interne Benutzer-Liste des Public Spot-Moduls stattfindet und Sie keinen RADIUS-Accounting-Server einsetzen wollen, können Sie lediglich das Ablaufdatum der Benutzerkonten für Abrechnungszwecke verwenden.

Die Verwendung der internen Benutzer-Liste wird nicht mehr empfohlen. Verwenden Sie für neue Installationen stattdessen den internen RADIUS-Server zur Benutzerverwaltung und zum Accouting, um vom vollen Funktionsumfang des Public Spots zu profitieren.

Hinweis: Für Abrechnungsmodelle auf Kredit-Basis kann der Public Spot per SYSLOG detaillierte Verbindungsinformationen an beliebige Rechner im Netzwerk ausgeben. Bei Einsatz entsprechender Software auf dem Zielrechner können Sie die tatsächlich verwendeten Ressourcen (Verbindungszeiten oder Transfervolumen) exakt abrechnen.

Abrechnung über RADIUS-Accounting-Server

Bei Abrechnung über einen RADIUS-Server können Sie den Public Spot so einstellen, dass er regelmäßig aktuelle Verbindungsinformationen über jeden aktiven Benutzer an den angegebenen Accounting-Server ausgibt. Ein Accounting wird immer dann gestartet, wenn ein Client über RADIUS authentifiziert wurde und in der **Anmelde-Server**-Liste für den betreffenden **Authentifizierungs-Server** auch ein gültiger **Accounting-Server** konfiguriert ist. Es ist daher auch möglich, verschiedene RADIUS-Server für Accounting und Authentifizierung zu verwenden.

Jedes der regelmäßigen Meldepakete an den Accounting-Server enthält Angaben darüber, welche Ressourcen (Zeit, übertragene Datenmenge, etc.) der Benutzer seit der letzten Meldung verbraucht hat. So gehen bei einem Ausfall eines Public Spots (etwa durch Stromausfall o. ä.) auch im schlimmsten Fall nur wenige Abrechnungsinformationen verloren.

Die regelmäßige Meldung der Abrechnungsinformationen an den Accounting-Server (Interim-Updates) ist in der Voreinstellung ausgeschaltet. Die Aktivierung erfolgt, wenn Sie den Meldezyklus größer 0 festlegen.

- LANconfig: **Public-Spot** > **Benutzer** > **Update-Zyklus**

Hinweis: Der Meldezyklus wird in Sekunden angegeben. Er bestimmt den Zeitabstand, in dem Ihr Gerät regelmäßig Verbindungsinformationen an den Accounting-Server sendet. Ein Meldezyklus von `0` Sekunden deaktiviert die Funktion. In diesem Fall sendet Ihr Gerät nur zu Beginn und am Ende einer Sitzung Abrechnungsinformationen.

Bei Einsatz von Abrechnungsmodellen auf Guthabenbasis (PrePaid) übernimmt der RADIUS-Server die Überwachung der festgelegten Nutzungsbeschränkungen (Kontingente für Verbindungszeit oder Transfervolumen, Ablaufdatum). Sobald ein Benutzer sein Guthaben aufgebraucht hat, sperrt der RADIUS-Server das Benutzerkonto. Ihr Gerät weist künftige Anmeldeversuche des Benutzers daraufhin ab.

Hinweis: Zeitkontingente für PrePaid-Modelle kann der Public Spot auch während der aktiven Sitzungen überwachen. Wird ein Zeitguthaben vollständig aufgebraucht, so beendet der Public Spot automatisch die betreffende Sitzung. Die Guthabenüberwachung wird eingeschaltet, indem der RADIUS-Server zum Sitzungsbeginn eines Benutzers dessen Zeitguthaben als Attribut "Session Timeout" an den Public Spot übermittelt.

Anfragetypen

Ihr Gerät ist in der Lage, verschiedene Typen von RADIUS-Anfragen an einen Accounting-Server zu senden. Diese Anfragen unterscheiden sich nach je nach Sitzungsstatus eines Benutzers:

- Ein Accounting-Start wird nach einer erfolgreichen Authentifizierung gesendet.
- Ein Accounting-Stop wird nach Beenden einer Public Spot-Sitzung gesendet.
- Optional: Zwischenzeitliche Aktualisierungen (Interim-Updates) werden während der Sitzung gesendet.

Es gibt zwei Arten von Interim-Updates: Ein initiales Update wird im direkten Anschluss an die Start-Anfrage gesendet, da einige RADIUS-Server dieses benötigen, um eine Sitzung in ihrer Accounting-Datenbank anzulegen. Alle weiteren Updates sind davon abhängig, ob ein Accounting-Zyklus für die

jeweilige Sitzung definiert wurde (unter **Public-Spot** > **Benutzer** > **Update-Zyklus**).

Alternativ kann dieser Wert auch Bestandteil einer RADIUS-Authentifizierungs-Antwort sein: Dabei bietet der RADIUS-Server einem RADIUS-Client (also z. B. Ihrem Public Spot) ein Accounting-Interim-Intervall an, welches der Client bei entsprechender Unterstützung übernimmt, sofern für ihn lokal kein eigenes Intervall definiert wurde.

Hinweis: Sofern ein lokaler Wert gesetzt wurde, wird dieser immer höher priorisiert als der von einem RADIUS-Server gelieferte Wert, welchen die RADIUS RFCs standardmäßig fordern!

Im *Anhang* finden Sie eine Liste, welche Attribute Ihr Gerät an einen RADIUS-Server senden kann und welche Attribute einer RADIUS-Antwort Ihr Gerät versteht.

Accounting-Backup

Die Backup-Lösung für das RADIUS-Accounting entspricht der für die RADIUS-Authentifizierung, d. h. Ihr Gerät arbeitet die in der Anmelde-Server-Liste angelegten Einträge nach und nach ab (siehe Kapitel *Verkettung von Backup-Servern*). Die Backup-Einträge für die Accouting-Server sollten dabei mit derselben Umsicht gewählt werden wie die für die Authentifizierungs-Server: Sofern Sie mehrere Backup-Server verwenden, müssen sie ggf. Werte für Wiederholung und Zeitüberschreitung der Anfragen anpassen, um eine gute Erreichbarkeit des Gesamtsystems zu erreichen.

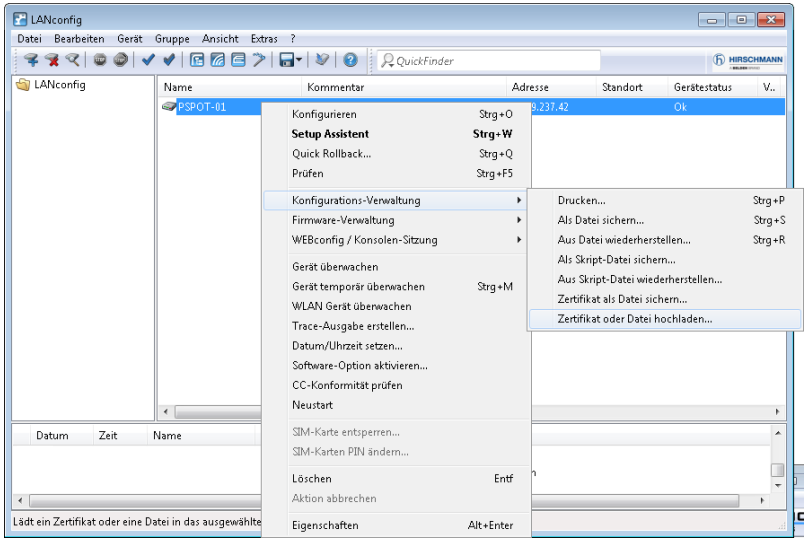
Hinweis: Während das Gerät Accounting-Anfragen sendet, werden laufende Benutzersitzungen nicht angehalten, was – im Gegensatz zur Authentifizierung – zusätzliche Ressourcen im Gerät verbraucht. Bitte achten Sie darauf, dass der Zeitbedarf für die Auswahl eines Accounting-Servers* geringer ausfällt als die Länge eines Accounting-Zyklusses bei Interim-Update-Anfragen. Somit vermeiden Sie einen Anfragestau und daraus resultierenden Stapelüberlauf.

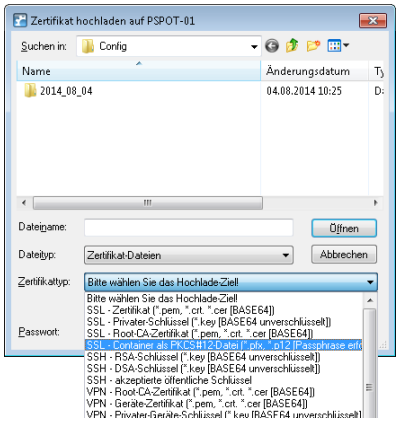
**Anzahl Backups x (Leerlaufzeit-Überschreitung + Anzahl Wiederholungen)*

Mehrstufige Zertifikate für Public Spots

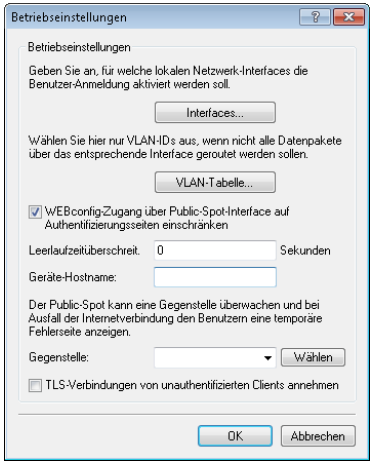
SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das Gerät geladen werden. Diese Zertifikatsketten können für die Public Spot-Authentifizierungsseiten über den im Gerät implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im Public Spot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei Public Spot-Authentifizierungen zu vermeiden.

Das Zertifikat laden Sie über LANconfig im Dateimanagement mit den einzelnen Dateien des Root-CA-Zertifikats oder als PKCS#12-Container in das Gerät:





Da Zertifikate üblicherweise auf DNS-Namen ausgestellt werden, muss der Public Spot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (einzugeben unter **Public-Spot** > **Server** > **Betriebseinstellungen** bei **Geräte-Hostname**). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des Public Spots aufgelöst werden.

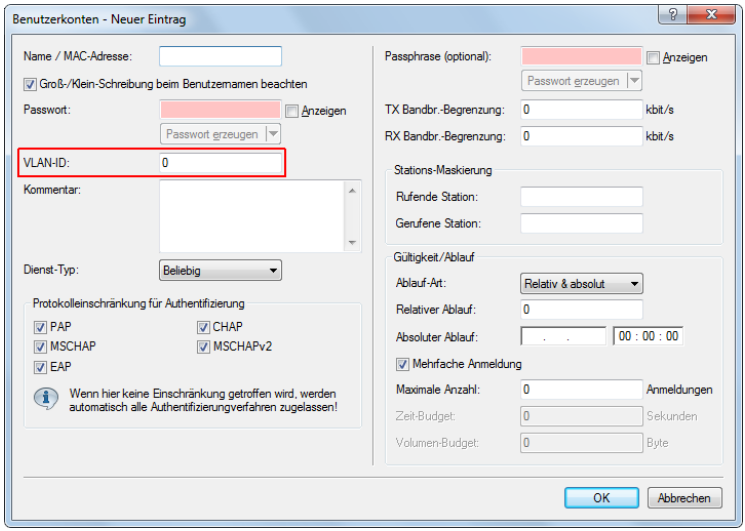


Benutzern individuelle VLANs zuweisen

Unabhängig von der Zuweisung einer VLAN-ID für das gesamte Public Spot-Modul bietet Ihnen das Gerät die Möglichkeit, individuelle VLAN-IDs für ein-

zelne Public Spot-Benutzer zu vergeben. Diese ID wird Ihren Benutzern im Anschluss an eine erfolgreiche Authentifizierung automatisch vom RADIUS-Server zugewiesen. Auf diese Weise ist es z. B. möglich, unterschiedliche Public Spot-Nutzer in getrennte Netze mit verschiedenen Rechten und Zugriffsmöglichkeiten einzuordnen, ohne dass sich diese an getrennten SSIDs anmelden oder Sie die Verfügbarkeit verschiedener Netze öffentlich aussenden müssen (z. B. Netze für unterschiedliche Kunden-Typen). Die entsprechenden Regeln lassen sich über die Firewall realisieren, indem Sie als Quell-Tag die VLAN-ID des betreffenden Nutzers / der betreffenden Nutzergruppe angeben.

Hinweis: Vorraussetzung für die oben beschrieben Funktionen ist ein aktiviertes VLAN-Modul.



- Öffnen Sie die Tabelle **Benutzerkonten** im Dialog **RADIUS-ServerAllgemein** und klicken Sie auf **Hinzufügen...**, um einen neuen Benutzer zu erstellen.
- Weisen Sie dem neuen Benutzer eine individuelle VLAN-ID über das Eingabefeld **VLAN-ID** zu. Die individuelle VLAN-ID überschreibt nach der Authentifizierung durch den RADIUS-Server eine globale VLAN-ID, die ein Nutzer ansonsten über das Interface erhalten würde. Der Wert `0` deaktiviert die Zuweisung einer individuellen VLAN-ID.

Hinweis: Die Vergabe einer VLAN-ID erfordert technisch bedingt die erneute Adresszuweisung durch den DHCP-Server. Solange ein Client nach der erfolgreichen Authentifizierung noch keine neue Adresse zugewiesen bekommen hat, befindet sich er sich nachwievor in seinem bisherigen (z. B. ungetaggten) Netz. Damit der Client möglichst rasch in das neue Netz überführt wird, ist es notwendig, die Lease-Time des DHCP-Servers unter **IPv4** > **DHCPv4** möglichst gering einzustellen. Mögliche Werte (in Minuten) sind z. B.:

- **Maximale Gültigkeit:** 2
- **Standard-Gültigkeit:** 1

Berücksichtigen Sie dabei, dass eine derart starke Verkürzung der globalen Lease-Time Ihr Netz bedingt mit DHCP-Nachrichten flutet und bei größeren Nutzerzahlen zu einer gesteigerten Netzlast führt! Alternativ haben Sie die Möglichkeit, einen externen DHCP-Server einzusetzen oder Ihre Nutzer manuell – über ihren Client – eine neue Adresse anfordern zu lassen. In der Windows-Kommandozeile erfolgt dies z. B. über die Befehle `ipconfig /release` und `ipconfig /renew`.

Hinweis: Durch die Zuweisung einer VLAN-ID verliert ein Nutzer nach Ablauf des initialen DHCP-Leases seine Verbindung! Erst ab dem zweiten Lease – also nach erfolgter Zuweisung der VLAN-ID – bleibt die Verbindung konstant.

Fehlerseite bei Wegfall der WAN-Verbindung einrichten

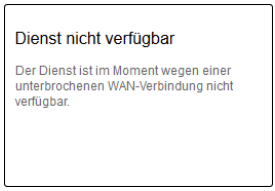
Sie haben die Möglichkeit, das Public Spot-Modul gegenüber noch nicht authentifizierten Benutzern – zusätzlich zu den allgemeinen Anmeldefehlern – auch WAN-Verbindungsfehler ausgeben zu lassen. Dadurch werden mögliche Benutzer bereits vorab über die fehlende Verfügbarkeit des Netzwerks informiert. Die entsprechende Variante der **Fehler**-Seite erscheint immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert.

Damit die Anzeige der Fehlerseite für diesen Fall korrekt funktioniert, **muss** eine entsprechende Gegenstelle benannt sein, deren Verbindungsstatus das

Public Spot-Modul überwacht. Tragen Sie dazu im Dialog **Public-Spot** > **Server** eine entsprechende **Gegenstelle** ein. Über die Schaltfläche **Wählen** können Sie dem Auswahl-Eingabefeld bequem eine bereits eingerichtete oder neue Gegenstelle zuweisen.

Hinweis: Ohne Benennung einer zu überwachenden Gegenstelle deaktiviert das Public Spot-Modul die Ausgabe von Verbindungsfehlern auf der Fehlerseite. Ein Wegfall der WAN-Verbindung führt dann bei unauthentifizierten Benutzern stattdessen zu einem Verbindungs-Timeout in ihrem Browser.

Innerhalb einer individuellen Fehlerseite verwenden Sie den Bezeichner `LOGINERRORMSG`, um die Fehlermeldung des HiLCOS bei Wegfall der WAN-Verbindung einzufügen. Im Falle eines WAN-Verbindungsfehlers wird dann die folgende Fehlermeldung ausgegeben:



Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.

AP-spezifische Anmeldung an einem zentralen Public Spot

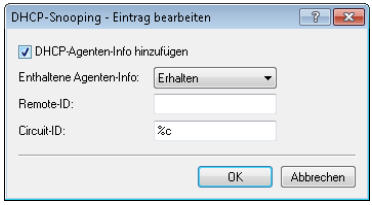
Ein zentraler WLC verwaltet in einer verteilten Infrastruktur einen Public Spot, dessen Konfiguration (Public Spot-SSID, Sicherheitsstandards) auf allen beteiligten APs entsprechend identisch ist. Auf diesem Weg kann ein Public Spot-Anbieter z. B. in allen seinen räumlich getrennten Filialen einen identischen Public Spot zur Verfügung stellen.

Die Kunden hätten also nach dem Erhalt eines Vouchers in jeder Filiale Zugriff auf diesen Public Spot. Um dennoch die Nutzung auf die Filiale zu beschränken, in der der Kunde den Voucher erhalten hat, überträgt der AP zusätzlich zu Username und Passwort auch seine Kennung. Diese Kennung ermöglicht die Zuordnung des Vouchers zu diesem AP. Der AP nutzt für die Übertragung der Kennung die Circuit-ID (DHCP-Option 82), die er den DHCP-

Requests anhängt. Diese DHCP-Pakete durchlaufen den zentralen Public Spot, der die Kennung anhand der Einträge in der RADIUS-User-Tabelle überprüft.

Der Public Spot lässt diese Anfrage nur zu, wenn diesem Voucher in der RADIUS-User-Tabelle auch dieser AP zugeordnet ist. Kunden, die einen Voucher in Filiale A erhalten haben, können sich also nicht in der Filiale B am gleichen Public Spot anmelden, da beide Filial-APs unterschiedliche Kennungen übertragen.

Die AP-Kennung konfigurieren Sie als Circuit-ID unter **Schnittstellen** > **Snooping** > **DHCP-Snooping** bei der entsprechenden Schnittstelle ein.

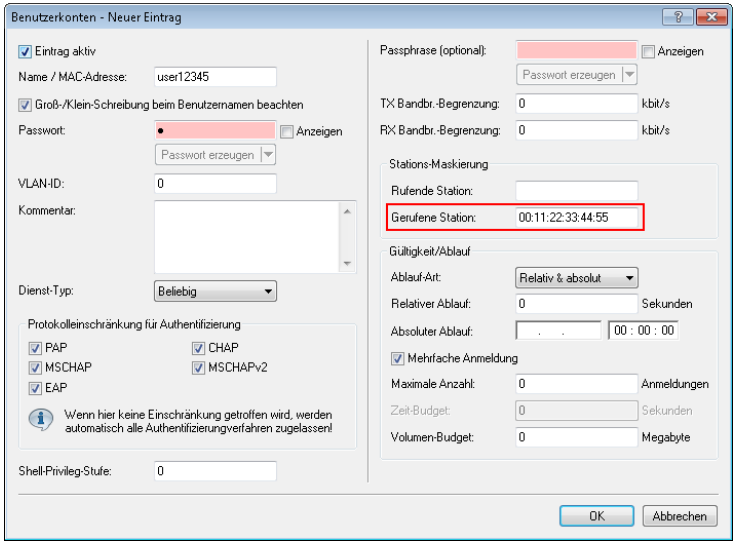


Sie können die folgenden Variablen verwenden:

- **%%**: fügt ein Prozent-Zeichen ein.
- **%c**: fügt die MAC-Adresse der Schnittstelle ein, auf der sich der Public Spot-User anmeldet. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- **%i**: fügt den Namen der Schnittstelle ein, auf der sich der Public Spot-User anmeldet.
- **%n**: fügt den Namen des APs ein, wie er z. B. unter **Management** > **Allgemein** festgelegt ist.
- **%v**: fügt die VLAN-ID des DHCP-Request-Paketes ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- **%p**: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind **%p** und **%i** identisch.
- **%s**: fügt die WLAN-SSID ein, wenn die Anmeldung über einen WLAN-Client erfolgt. Bei anderen Clients enthält diese Variable einen leeren String.

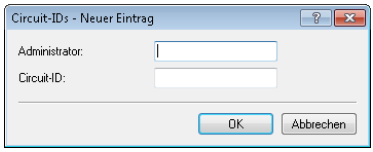
- **%e**: fügt die Seriennummer des APs ein, wie sie z. B. unter **Management** > **Allgemein** zu finden ist.

Im WLC konfigurieren Sie diese Kennung in der RADIUS-User-Tabelle unter **RADIUS-Server** > **Allgemein** > **Benutzerkonten**.



Als “Gerufene Station” fügen Sie die Kennung des APs ein, der den entsprechenden Voucher-Zugriff ermöglichen soll.

Der Public Spot-Setup-Assistent kann bei der Einrichtung neuer Public Spot-Nutzer automatisch die Kennung des Gerätes übernehmen, wenn diese unter **Public-Spot** > **Assistent** > **Circuit-IDs** konfiguriert ist.



Der Setup-Assistent prüft beim Anlegen eines neuen Public Spot-Nutzers, ob für den angemeldeten **Administrator** ein Eintrag in dieser Tabelle hinterlegt ist. Ist das der Fall, übernimmt der Setup-Assistent die entsprechende **Circuit-ID** als “gerufene Station” in die RADIUS-User-Tabelle.

Redirect für HTTPS-Verbindungen

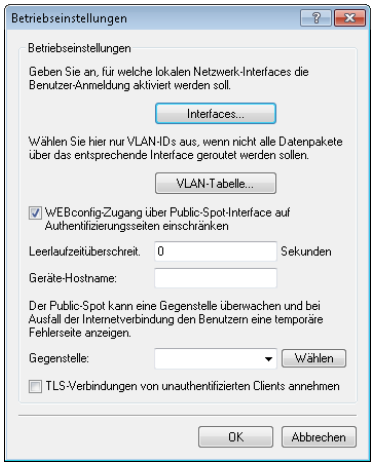
Versucht ein nicht angemeldeter Client über eine Schnittstelle, für die der Public Spot aktiv ist, via HTTPS auf eine Webseite zuzugreifen, wird diese Verbindungsanfrage an das Public Spot-Gateway selber umgeleitet, um dem Nutzer die Anmeldeseite zu präsentieren (ist bei HTTP auch der Fall). In diesem Fall wird dem Benutzer normalerweise eine Zertifikatswarnung seines Browsers präsentiert, da Name oder IP der ursprünglich angesurften Seite nicht dem Namen oder der IP des Public Spot entspricht. Um dies und die Erzeugung von erhöhter Last durch die aufgebauten HTTPS-/TLS-Verbindungen auf dem Public Spot Gateway zu verhindern, können Sie mit dieser Einstellung der Verbindungsaufbau über HTTPS für unangemeldete Clients verhindern.

Hinweis: Ist der Client einmal angemeldet, findet keinerlei Umleitung mehr statt und es können beliebig HTTP- und HTTPS-Verbindungen durch den Client aufgebaut werden.

Heutzutage übliche Clients führen eine "Captive Portal Detection" via HTTP durch. Dabei wird versucht, auf eine bestimmte URL via HTTP zuzugreifen, um das Vorhandensein einer Anmeldeseite (durch Public Spot oder andere Lösungen) zu überprüfen. Dieser Mechanismus wird durch das Ausschalten der HTTPS-Umleitung nicht beeinflusst, da die Erkennung normalerweise über HTTP stattfindet.

Ist es in einem Public Spot-Szenario jedoch nicht vorgesehen, dass unbekannte WLAN-Clients eine Verbindungsanfrage auch über HTTP ausführen sollen, würde dieser wirkungslose HTTPS-Redirect das Public Spot-Gateway unnötig belasten. Entsprechend ist es möglich, diesen HTTPS-Redirect prinzipiell zu deaktivieren. In diesem Fall würde der Benutzer vom Browser eine leere Seite erhalten.

Das Redirect für HTTPS-Verbindungen konfigurieren Sie im LANconfig unter **Public-Spot** > **Server** > **Betriebseinstellungen**.



Um das HTTPS-Redirect einzuschalten, aktivieren Sie die Option **TLS-Verbindungen von unauthentifizierten Clients annehmen**. In der Standardeinstellung ist diese Option deaktiviert.

Schutz vor Brute Force-Angriffen

Brute-Force-Angriffe sind die bekanntesten Angriffe auf ein Netzwerk. Diese Art von Angriff besteht darin, eine Menge an möglichen Passwörtern innerhalb kurzer Zeit auszuprobieren, bis das richtige Passwort gefunden wird. Ein möglicher Schutz vor Brute-Force-Angriffen besteht darin, nach einem oder mehreren aufeinander folgenden fehlgeschlagenen Eingabeversuchen die Zeit bis zur nächsten möglichen Eingabe zu verzögern.

Den Schutz vor Brute-Force-Angriffen konfigurieren Sie mit LANconfig unter **Public-Spot** > **Server** im Abschnitt **Brute-Force-Schutz**.

Sperren nach

Bestimmen Sie, nach wie vielen Fehlversuchen die Eingabesperre für weitere Versuche eingreifen soll.

Sperrdauer

Bestimmen Sie, für wie lange die Eingabesperre gelten soll.

Über die Konsole zeigt der Befehl `show pbbruteprotector` den aktuellen Status des Brute-Force-Schutzes:

`show pbbruteprotector`

Zeigt eine Übersicht über alle am Public Spot angemeldeten MAC-Adressen.

`show pbbruteprotector [MAC-Adresse[ MAC-Adresse[ ...]]]`

Die Angabe einer oder mehrerer durch Leerzeichen getrennter MAC-Adressen zeigt den Status der jeweiligen MAC-Adressen an.

Hinweis: Die Angabe von MAC-Adressen erfolgt in den Formaten `11:22:33:44:55:66`, `11-22-33-44-55-66` oder `112233445566`.

14.2.4 Alternative Anmeldeformen

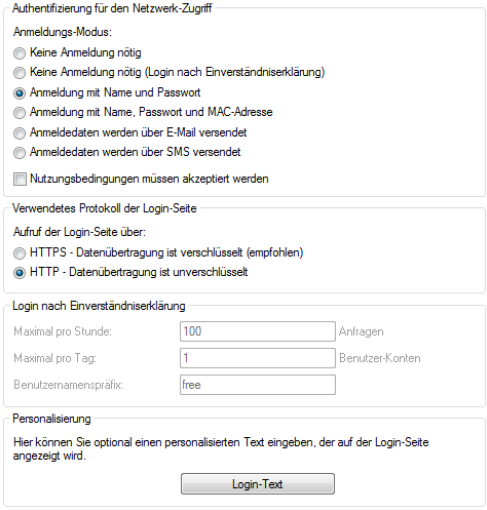
Neben der Anmeldung über vorab mitgeteilte Zugangsdaten können Ihre Nutzer die Zugangsdaten auch selbstständig per E-Mail oder SMS anfordern, oder den schnellen Public Spot-Zugang durch Akzeptieren einer Einverständniserklärung erlangen. Alternativ können Sie über die XML- oder die PMS-Schnitstelle (Modul als Option erhältlich) Ihren Public Spot auch mit anderen Software-Systemen verknüpfen, um so umfassendere oder mehrstufige Anmeldeszenarien zu realisieren.

Ebenso können Sie Ihren Nutzern einen zusätzlichen Komfort bieten, indem Sie z. B. automatisierte Anmeldeverfahren erlauben (Automatische Anmeldung sowie Re-Login über die MAC-Adresse, Anmeldung über WISPr, Hotspot 2.0) und Ihren Nutzern – darauf aufbauend – entsprechende Roaming-Dienste anbieten.

Hinweis: Die Hotspot-2.0- und Roaming-Funktionalitäten sind nur im Zusammenhang mit WLAN verfügbar.

Übersicht der Anmeldemodi

Die Anmeldung am Public Spot kann auf verschiedenen Wegen erfolgen. Diese Einstellungen für die Authentifizierung am Netzwerk legen Sie im Dialog **Public-Spot** > **Anmeldung** fest.



Folgende Anmeldungsmodi stehen Ihnen zur Auswahl:

- **Keine Anmeldung nötig**

  Nutzer erhalten freien Zugang zum Public Spot, eine Anmeldung ist nicht erforderlich.

  Hinweis: Verwenden Sie diese Einstellung nicht, wenn Ihr Gerät uneingeschränkten Zugriff auf das Internet bietet!

- **Keine Anmeldung nötig (Login nach Einverständniserklärung)**

  Nutzer erhalten freien Zugang zum Public Spot, nachdem sie die Einverständniserklärung des Betreibers akzeptiert haben. Die Anmeldung erfolgt dabei für die Nutzer völlig transparent über einen RADIUS-Server. Voraussetzung dafür ist, dass Sie eine individuelle Seitenvorlage (Willkommensseite mit Einverständniserklärung) eingerichtet haben: In diesem Fall leitet

der Public Spot einen neuen Nutzer zunächst auf die Willkommensseite weiter. Nach Zustimmung der Einverständniserklärung legt das Gerät entsprechend der unter **Public-Spot** > **Assistent** gesetzten Standardwerte automatisch ein Benutzerkonto an und gibt den Zugriff auf das angeschlossene Netzwerk frei.

Darüber hinaus ist bei Anwählen dieses Anmeldungsmodus der Dialog-Abschnitt **Login nach Einverständniserklärung** verfügbar, in dem Sie zusätzliche Rahmenbedingungen für das Erstellen von freien Benutzerkonten durch den RADIUS-Server festlegen:

- **Maximal pro Stunde**: Geben Sie an, wie viele Benutzer sich pro Stunde am Gerät automatisch ein Konto erstellen können. Verringern Sie diesen Wert, um Leistungseinbußen durch übermäßig viele Nutzer zu reduzieren.
- **Maximal pro Tag**: Geben Sie an, wie viele Konten ein Nutzer pro Tag anlegen darf. Ist dieser Wert erreicht und die Nutzer-Sitzung abgelaufen, kann sich ein Benutzer für den Rest des Tages nicht mehr automatisch am Public Spot anmelden und authentifizieren lassen.
- **Benutzernamenspräfix**: Geben Sie hier einen Präfix an, anhand dessen Sie Benutzer in der RADIUS-Benutzertabelle erkennen, die das Gerät automatisch nach Bestätigen der Nutzungsbedinungen angelegt hat. Dieser Präfix wird dem unter **Public-Spot** > **Assistent** spezifizierten **Muster für den Benutzernamen** unmittelbar vorangestellt.

Hinweis: Die in der Willkommensseite hinterlegten Einverständniserklärung ist nicht mit der Nutzungsbedingungsseite zu verwechseln. Die Seite **Nutzungsbedingungen** ist eine Sonderseite, die nach gesonderter Aktivierung bei anderen Anmeldungsmodi zur Verfügung steht (siehe *Mögliche Authentifizierungsseiten* auf Seite 1540). Sofern Sie keine Willkommensseite einrichten (siehe *Konfiguration benutzerdefinierter Seiten* auf Seite 1550), zeigt das Gerät beim Zugriff auf den Public Spot eine Fehlermeldung an.

▶ **Anmeldung mit Name und Passwort**

Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher.

▶ **Anmeldung mit Name, Passwort und MAC-Adresse**

Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten erhalten Nutzer von einem Netzwerk-Administrator über einen Voucher. Zusätzlich muss bei diesem Anmeldungs-Modus die MAC-Adresse des Client mit der in der Benutzer-Liste vom Administrator hinterlegten Adresse übereinstimmen.

- **Anmeldedaten werden über E-Mail versendet**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per E-Mail. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 1498.

- **Anmeldedaten werden über SMS versendet**

  Nutzer melden sich am Public Spot mit ihrem Namen und ihrem Passwort an. Die Login-Daten generieren sich die Nutzer selbst; zugestellt werden die Daten per SMS. Die Aktivität eines Administrators ist nicht erforderlich. Mehr zu diesem Anmeldungsmodus erfahren Sie unter *Selbständige Benutzeranmeldung (Smart Ticket)* auf Seite 1498.

Durch aktivieren der Option **Nutzungsbedingungen müssen akzeptiert werden** haben Sie in bestimmten Anmeldungsmodi außerdem die Möglichkeit, die Anmeldung an die Anerkennung von Nutzungsbedingungen zu koppeln. In diesem Fall zeigt der Public Spot auf der Anmeldeseite ein zusätzliches Optionsfeld an, welches die Benutzer vor Registrierung bzw. Anmeldung zum Akzeptieren der Nutzungsbedingungen auffordert. Stimmt ein Nutzer diesen Nutzungsbedingungen nicht explizit zu, bleibt ihm eine Anmeldung am Public Spot verwehrt.

Hinweis: Denken Sie daran, vorab eine Seite mit Nutzungsbedingungen in das Gerät zu laden, bevor Sie diese Option aktivieren. Andernfalls zeigt das Gerät dem Benutzer lediglich einen Platzhalter an Stelle der Nutzungsbedingungen an.

Selbständige Benutzeranmeldung (Smart Ticket)

Geräte mit Public Spot bieten Anwendern einen zeitlich begrenzten Zugang zu bestimmten Netzwerken, klassischerweise dem Internet. In vielen Szena-

rien wird für das Anlegen eines Zugangs ein beschränkter Administrations-Account eingesetzt: Ein Mitarbeiter an einer Hotel-Rezeption z. B. erhält hierbei einen Account, der ausschließlich über die Funktionsrechte zum Anlegen und ggf. Verwalten von Public Spot-Benutzern verfügt. Mit wenigen Mausklicks kann der Mitarbeiter dann den Hotelgästen einen Voucher für den Netzzugang ausdrucken.

Da allerdings auch die komfortable Lösung mit Vouchern immer die Aktivität eines Administrators erfordert, können Sie Ihren Nutzern alternativ die Möglichkeit einräumen, die Zugangsdaten zum drahtlosen Netzwerk eigenständig zu generieren und sich die Zugangsdaten per E-Mail oder SMS zusenden zu lassen (Anmeldung über "Smart Ticket").

Login nach Einverständniserklärung

Alternativ bietet das Gerät Ihnen die Möglichkeit, die Anmeldung für Public Spot-Nutzer völlig transparent über einen RADIUS-Server abzuwickeln. Der Benutzeranmeldung ist in diesem Fall eine Abfrage vorangestellt, bei der ein Nutzer zunächst der im Gerät hinterlegten Einverständniserklärung zustimmen muss, bevor er automatisch Zugang zum Public Spot erhalten. Ein nutzerseitiges Erstellen eigener Zugangsdaten via E-Mail oder SMS entfällt bei dieser Authentifizierungsmethode. Mehr hierzu erfahren Sie im betreffenden Abschnitt unter *Übersicht der Anmeldemodi* auf Seite 1496, da der "Login nach Einverständniserklärung" kein Bestandteil der Smart-Ticket-Funktion ist.

E-Mail-Anmeldung konfigurieren

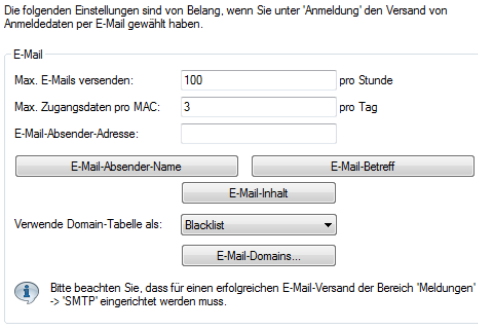
Die Einstellungen für den Versand der Anmeldedaten an das vom Benutzer angegebene E-Mail-Konto nehmen Sie im Dialog **Public-Spot** > **E-Mail** vor. Die nachfolgenden Schritte zeigen Ihnen, wie Sie die E-Mail-Anmeldung korrekt konfigurieren.

Wichtig: Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 1504. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte

finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1506.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über E-Mail versendet**.
4. Wechseln Sie in die Ansicht **Public-Spot** > **E-Mail**.



5. Tragen Sie im Eingabefeld **Max. E-Mails versenden** die maximale Anzahl an E-Mails ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die E-Mail-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
6. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
7. Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der E-Mail als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.
8. Geben Sie über das Auswahlmenü **Verwende Domain-Tabelle als** an, ob das Gerät die Tabelle **E-Mail-Domains** als Blacklist oder Whitelist verwendet.

   Diese Definition bestimmt, welche E-Mail-Adressen bzw. Domains Ihre Public Spot-Benutzer zur Registrierung angeben dürfen.

   - **Blacklist**: Die Registrierung ist über alle E-Mail-Domains erlaubt bis auf diejenigen, die in dieser Tabelle stehen.

- **Whitelist**: Die Registrierung ist ausschließlich über die E-Mail-Domains möglich, die in dieser Tabelle stehen.

Wichtig: Bitte beachten Sie, dass der Public Spot bei einer leeren Domain-List als Whitelist alle Domains ablehnt.

9. Definieren Sie über die Tabelle **E-Mail-Domains** alle E-Mail-Domains, die Sie im Falle einer Anmeldung Ihrer Public Spot-Benutzer via E-Mail erlauben bzw. verbieten wollen. Geben Sie die Domains im Format `@web-domain.de` an.
10. Schreiben Sie die Konfiguration zurück auf das Gerät.

SMS-Anmeldung konfigurieren

Die Einstellungen für den Versand der Anmeldedaten als Kurznachricht (SMS) an die vom Benutzer angegebene Rufnummer nehmen Sie im Dialog **Public-Spot** > **SMS** vor. Dabei können Sie – je nach Gerätetyp – zwischen mehreren Varianten wählen:

- Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes;
- Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, welches die Umwandlung der E-Mail in eine SMS übernimmt.

Hinweis: HiLCOS überprüft die eingegebene Rufnummer auf ungültige Zeichen. Erlaubt sind ausschließlich Zahlen zwischen 0 und 9. Der Nutzer muss 5 bis 15 Zahlen (exklusive Landesvorwahl) eingeben.

Die nachfolgenden Schritte zeigen Ihnen, wie Sie die einzelnen Varianten der SMS-Anmeldung korrekt konfigurieren.

Wichtig: Der SMS-Versand eignet sich für Installationen mit einem maximalen Durchsatz von 10 SMS pro Minute.

Wichtig: Für den erfolgreichen Versand der Anmeldedaten als E-Mail muss unter **Meldungen** > **SMTP-Konto** sowie **Meldungen** > **SMTP-Optionen** ein gültiges SMTP-Konto eingerichtet sein.

Darüber hinaus haben Sie in dem Dialog auch die Möglichkeit, individuelle Texte festzulegen, die das Gerät für den Versand der Anmeldedaten nutzt; siehe *Nachrichtentexte anpassen* auf Seite 1504. Standardmäßig setzt das Gerät vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1506.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Anmeldung**.
3. Ändern Sie den Anmeldungsmodus auf **Anmeldedaten werden über SMS versendet**.
4. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.

5. Legen Sie fest, auf welche Art und Weise der SMS-Versand erfolgt:

   - Für den Versand der Anmeldedaten als SMS über das 3G/4G WWAN-Modul eines anderen Gerätes, führen Sie zunächst die Schritte im Abschnitt *Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen* auf Seite 1503 aus und fahren anschließend mit dem nächsten Konfigurations-Hauptschritt fort.
   - Für Versand der Anmeldedaten als E-Mail an ein externes E-Mail2SMS-Gateway, wählen Sie die Einstellung **SMS über externes E-Mail-zu-SMS-Gateway versenden** und fahren im Anschluss an die nachstehenden Unterschritte mit dem nächsten Konfigurations-Hauptschritt fort.

a) Tragen Sie im Eingabefeld **Gateway E-Mail-Adresse** die IP-Adresse oder den Host-Namen des Gateway-Servers ein, der die E-Mail in eine SMS umwandelt. Erwartet der Provider die Mobilfunknummer im lokalen Teil der E-Mail, können Sie dafür die Variable `$PSpotUserMobileNr` verwenden.

b) Geben Sie im Eingabefeld **E-Mail-Absender-Adresse** die E-Mail-Adresse an, die dem zukünftigen Public Spot-Benutzer bei der Zustellung der SMS als Absenderadresse angezeigt wird, z. B. `support@providerX.org`.

6. Tragen Sie im Eingabefeld **Max. Nachrichten versenden** die maximale Anzahl an Kurznachrichten ein, die das Public Spot-Modul innerhalb einer Stunde an Benutzer für die SMS-Anmeldung verschicken darf. Reduzieren Sie den Wert, um die Anzahl der neuen Benutzer pro Stunde zu verringen.
7. Geben Sie im Eingabefeld **Max. Zugangsdaten pro MAC** an, wie viele verschiedene Zugangsdaten das Gerät für eine MAC-Adresse innerhalb eines Tages bereitstellen darf.
8. Tragen Sie in die Tabelle **Zielländer-Codes** sämtliche Rufnummern ein, die der Public Spot für den Versand der Anmeldedaten über SMS akzeptiert.
   Die Eingabe eines Länder-Codes kann direkt oder mit vorangestellter Doppel-Null erfolgen, zum Beispiel für Deutschland `49` oder `0049`.

   Wichtig: Diese Tabelle agiert als Whitelist. Sie müssen Länder-Codes definieren, damit ein Versand der Login-Daten erfolgt.

9. Schreiben Sie die Konfiguration zurück auf das Gerät.

Geräte mit 3G/4G WWAN-Modul als SMS-Gateway einsetzen

Sie haben bei der Public Spot-Anmeldung via SMS (Smart Ticket) die Möglichkeit, den Versand der Zugangsdaten über das 3G/4G WWAN-Modul eines anderen Gerätes anstelle eines externen E-Mail2SMS-Gateways abzuwickeln. Dazu hinterlegen Sie im Gerät, das den Public Spot bereitstellt, die Adresse und die Zugangsdaten des betreffenden 3G/4G-Gerätes. Für den Versand der SMS schickt das Public Spot-Modul dann via URL-Aufruf die Anmeldedaten und die Kurznachricht an das fremde 3G/4G-Gerät.

1. Starten Sie LANconfig und richten Sie auf dem 3G/4G-Gerät, das als SMS-Gateway fungieren soll, dass SMS-Modul ein (siehe *Basiskonfiguration des SMS-Moduls*). Darüber hinaus empfiehlt es sich, für den Zugang einen separaten Administrator ohne Zugriffsrechte (Auswahl **Keine**) mit dem alleinigen Funktionsrecht **Senden von SMS** anzulegen.
2. Öffnen Sie den Konfigurationsdialog für das Gerät, das den Public Spot bereitstellt.
3. Wechseln Sie in die Ansicht **Public-Spot** > **SMS**.

4. Wählen Sie die Einstellung **SMS über ein GSM-fähiges Gerät (z. B. mit 3G/4G-Modem) versenden**.
5. Geben Sie in den Eingabefeldern **Administrator** und **Passwort** den Namen und das Passwort für den Administrator auf dem anderen 3G/4G-Gerät ein.
6. Geben Sie im Eingabefeld **Adresse des GSM-Gerätes** die IP-Adresse ein, unter der das andere 3G/4G-Gerät für den Public Spot erreichbar ist.

Nachrichtentexte anpassen

Standardmäßig setzt das Gerät für den Inhalt der versendeten E-Mails oder Kurznachrichten vordefinierte Textbausteine ein; eine Übersicht dieser Standardtexte finden Sie unter *Standardtexte für E-Mail-Absender, -Betreff und -Inhalt* auf Seite 1506. Sie haben aber auch die Möglichkeit, eigene Texte zu definieren.

Hinweis: Sofern Sie für eine Sprache keinen individuellen Text spezifizieren, trägt das Gerät automatisch den geräteinternen Standardtext ein.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie – je nach gewähltem Anmeldungsmodus – in die Ansicht **Public-Spot** > **E-Mail** bzw. **SMS**.
3. Geben über die Schaltfläche **E-Mail-Absender-Name** zu den verfügbaren Sprachen einen individuellen Absendernamen an, den die vom Public Spot zugestellten E-Mails bzw. Kurznachrichten tragen, z. B. `Provider X`.
4. Geben über die Schaltfläche **E-Mail-Betreff** zu den verfügbaren Sprachen eine individuelle Betreffzeile an, die das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 1505.
5. Geben über die Schaltfläche **E-Mail-Inhalt** bzw. **Nachrichteninhalt** zu den verfügbaren Sprachen einen individuellen Text an, den das Public Spot-Modul für seine E-Mails bzw. Kurznachrichten verwendet. Die dabei zur Verfügungen stehenden Variablen und Steuerzeichen entnehmen Sie dem Abschnitt *Verfügbare Variablen und Steuerzeichen* auf Seite 1505.
6. Schreiben Sie die Konfiguration zurück in das Gerät.

Verfügbare Variablen und Steuerzeichen

Für die Individualisierung der Standardtexte von Smart Ticket stehen Ihnen verschiedene Variablen und Steuerzeichen zur Verfügung. Die Variablen werden vom Public Spot-Modul beim Versand der E-Mail an den Benutzer bzw. das SMS-Gateway automatisch mit Werten gefüllt.

Variablen

Folgende Variablen stehen Ihnen im Eingabefeld **E-Mail-Inhalt** zur Verfügung:

`$PSpotPasswd`

Platzhalter für das nutzerspezifische Passwort des Public Spot-Zugangs.

`$PSpotLogoutLink`

Platzhalter für die Abmelde-URL des Public Spots in der Form `http://<IP-Adresse des Public Spots>/authen/logout`. Über diese URL hat ein Public Spot-Benutzer die Möglichkeit, sich vom Public Spot abzumelden, falls nach einem erfolgreichen Login das Sitzungsfenster – welches diesen Link ebenfalls enthält – z. B. vom Browser geblockt oder vom Benutzer geschlossen wird.

Steuerzeichen

Der Text in den Eingabefeldern **E-Mail-Betreff** und **E-Mail-Inhalt** darf auch folgende Steuerzeichen enthalten:

`\n`

CRLF (Carriage Return, Line Feed)

`\t`

Tabulator

`\<ASCII>`

ASCII-Code des entsprechenden Zeichens

Hinweis: Verlangt der E-Mail2SMS-Provider eine Variable, in der ein Backslash ("\") vorkommt, müssen Sie diesem ein weiteres "\" voranstellen. Dies unterbindet die Umwandung des "\" durch HiLCOS.

Standardtexte für E-Mail-Absender, -Betreff und -Inhalt

Wenn Sie im Dialog **Public-Spot** > **E-Mail** oder. **SMS** zu einer Sprache für das jeweilige Eingabefeld keinen individuellen Text angeben, greift das Gerät beim Generieren der E-Mail automatisch auf die im HiLCOS hinterlegten Standardtexte zurück. Die verwendete Sprache ist dabei abhängig von der Spracheinstellung des Browsers, den der Benutzer für die Registrierung verwendet hat. Sofern zu einer Sprache keine geräteinternen Standardtexte vorliegen, setzt das Gerät die englischen Texte ein.

	E-Mail-Absender-Name	*E-Mail-Betreff*	*E-Mail-Inhalt*
Deutsch	Public Spot	Ihre Anmeldedaten für den Public Spot	Ihr Passwort für den Public Spot: $PSpotPasswd $PSpotLogoutLink

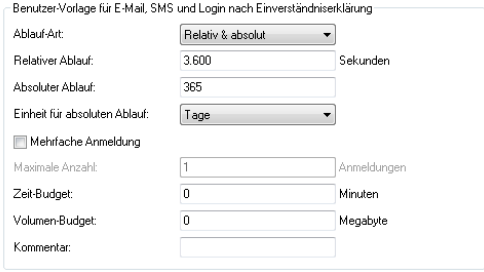
	E-Mail-Absender-Name	*E-Mail-Betreff*	*E-Mail-Inhalt*
Englisch	Public Spot	Your Public Spot account	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

Tabelle 28: Übersicht der geräteinternen Standardtexte für die Anmeldung über E-Mail/SMS

Standardwerte für die Benutzer-Vorlage setzen

Der nachfolgende Abschnitt beschreibt, wie Sie die Standardwerte für die **Benutzer-Vorlage** an Ihre Bedürfnisse anpassen. Das Gerät verwendet die hier definierten Werte als Vorgabewerte beim Anlegen neuer Benutzer über Smart-Ticket und dem Login nach Einverständniserklärung. Sofern Sie also den Versand der Anmeldedaten über E-Mail/SMS oder den Login nach Einverständniserklärung als Anmeldungsmodus gewählt haben, enthält jeder neue Benutzer-Account die von der Benutzer-Vorlage vorgegebenen Befugnisse und Einschränkungen.

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog für das Gerät.
2. Wechseln Sie in die Ansicht **Public-Spot** > **Assistent**.



3. Füllen Sie die Eingabefelder im Abschnitt **Benutzer-Vorlage** entsprechend Ihren Vorstellungen aus:

   ### Ablauf-Art

   Über diesen Eintrag definieren Sie, auf welche Art ein automatisch angelegtes Public Spot-Benutzerkonto abläuft. Sie können festlegen, ob die Gültigkeitsdauer eines Benutzer-Accounts absolut (fester Zeitpunkt) und/oder relativ (Zeitspanne ab dem ersten erfolgreichen Login) ist. Wenn Sie beide Werte auswählen, hängt der Ablaufzeitpunkt davon ab, welcher Fall als Erstes eintritt.

Relativer Ablauf

Über diesen Eintrag definieren Sie die relative Ablaufzeit eines automatisch angelegten Benutzerkontos (in Sekunden). Der von Ihnen gewählte **Ablauf-Typ** muss ein `relativ` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet nach der in diesem Feld angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Absoluter Ablauf

Über diesen Eintrag definieren Sie die absolute Ablaufzeit eines automatisch angelegten Benutzerkontos (in Tagen). Die von Ihnen gewählte **Ablauf-Art** muss ein `absolut` beinhalten, damit diese Einstellung greift. Die Gültigkeit des Kontos endet zu dem in diesem Feld angegebenen Zeitpunkt, hochgerechnet vom Tag der Kontoerstellung.

Einheit für absoluten Ablauf

Um kürzere Ablaufzeiten zu konfigurieren, wählen Sie im Dropdown-Menü die Einheit für den absoluten Ablauf aus. Passen Sie ggf. den Wert des absoluten Ablaufes an.

Mehrfache Anmeldung

Über diesen Eintrag erlauben bzw. verbieten Sie ganz allgemein, ob Nutzer eines automatisch erstellten Accounts mehrere Geräte gleichzeitig mit den selben Zugangsdaten am Public Spot anmelden dürfen. Die erlaubte Menge der gleichzeitig angemeldeten Geräte legen Sie über das Eingabefeld **Maximale Anzahl** fest.

Maximale Anzahl

Über diesen Eintrag legen Sie die maximale Anzahl der Geräte fest, die gleichzeitig unter einem automatisch erstellten Account angemeldet sein dürfen. Der Wert `0` steht dabei für 'unbegrenzt'. Damit diese Einstellung greift, muss gleichzeitig der Parameter **Mehrfache Anmeldung** aktiviert sein.

Zeit-Budget

Über diesen Eintrag definieren Sie das Zeit-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Volumen-Budget

Über diesen Eintrag definieren Sie das Volumen-Budget, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

Kommentar

Über diesen Eintrag vergeben Sie einen Kommentar oder Infotext, mit dem der RADIUS-Server ein automatisch erstelltes Benutzerkonto versieht.

4. Optional: Verändern Sie bei Bedarf das **Muster für Benutzernamen** sowie die **Passwort-Länge**. Das Gerät benutzt in den o. g. Anmeldungsmodi die betreffenden *Vorgabewerte des Benutzer-Erstellungs-Assistenten*, um automatisch einen Benutzernamen und ein Passwort zu generieren.
5. Schreiben Sie die Konfiguration zurück auf das Gerät.

Automatisches Re-Login

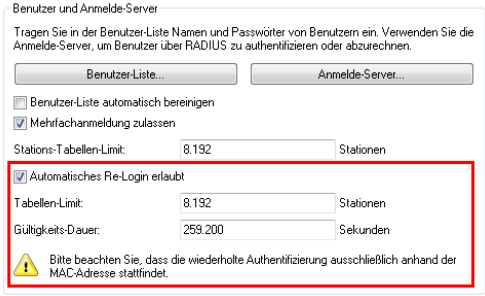
Mobile WLAN-Clients (z. B. Smartphones und Tablett-PCs) buchen sich automatisch in bekannte WLAN-Netze (SSID) ein, wenn sie erneut deren Funkzelle erreichen. Viele Apps greifen in diesem Fall automatisch ohne Umweg über den Webbrowser auf Webinhalte zu, um aktuelle Daten abzufragen (z. B. E-Mails, Soziale Netzwerke, Wetterbericht, etc.). Ähnliches gilt für mobile LAN-Clients (z. B. Notebooks), welche für einen Ortswechsel (z. B. in einer Hochschule dem Wechsel zwischen Hörsaal und Bibliothek) kurzzeitig vom Netz getrennt werden müssen. In allen Fällen ist es unpraktisch, wenn der Benutzer sich zunächst erneut im Browser manuell an einem Public Spot autorisieren muss.

Mit dem automatischen Re-Login genügt es, wenn der Benutzer sich einmalig am Public Spot identifiziert. Nach einer temporären Abwesenheit kann der Benutzer anschließend nahtlos weiter den Public Spot nutzen.

Der Public Spot protokolliert sowohl die manuelle An- und Abmeldung sowie einen Re-Login im SYSLOG. Dabei speichert er für einen Re-Login dieselben Anmeldedaten, die der Benutzer für die erstmalige Authentifizierung verwendet hat.

Hinweis: Die Authentifizierung erfolgt ausschließlich über die MAC-Adresse des Clients, wenn Re-Login aktiviert ist. Da das zu Sicherheitsproblemen führen kann, ist Re-Login standardmäßig deaktiviert.

Die Einstellungen für das automatische Re-Login finden sich bei LANconfig in der Geräte-Konfiguration unter **Public-Spot** > **Benutzer** im Abschnitt **Benutzer und Anmelde-Server**.



Das Auswahlkästchen **Automatische Wiederanmeldung (Auto-Re-Login) erlaubt** aktiviert diese Funktion.

Im Feld **Auto-Re-Login-Tabellen-Limit** bestimmen Sie die Anzahl der Clients (maximal 65536), die die Funktion Re-Login nutzen dürfen.

Im Feld **Auto-Re-Login-Gültigkeitsdauer** bestimmen Sie, wie lange der Public Spot die Anmeldedaten eines Clients für ein Re-Login in der Tabelle speichert. Nach Ablauf dieser Frist muss sich der Public Spot-Benutzer erneut über den Browser auf der Anmeldeseite des Public Spots anmelden.

Automatische Authentifizierung mit der MAC-Adresse

Ein Public Spot gewährt einem Benutzer nach erfolgreicher Authentifizierung den Zugang zu bestimmten Diensten. Zur Authentifizierung zeigt der Public Spot dem Benutzer nach dem Öffnen des Browsers üblicherweise eine Webseite. Der Benutzer gibt in dieser Anmeldeseite seine Benutzerdaten ein, der Public Spot leitet den Benutzer dann auf die erlaubten Webseiten weiter.

In manchen Anwendungsfällen ist die Authentifizierung über eine Webseite nicht erwünscht oder nicht möglich, wie die folgenden Beispiele zeigen:

- Das Endgerät verfügt nicht über einen Browser und kann daher die Anmeldeseite nicht öffnen.
- Der manuelle Aufruf der Anmeldeseite ist z. B. für einen Performance-Test zu langwierig.

Die automatische Authentifizierung am Public Spot mit der MAC-Adresse erlaubt die Nutzung des Public Spot ohne den vorherigen Aufruf der Anmeldeseite. Dazu trägt der Administrator alle MAC-Adressen der entsprechenden Endgeräte in die Tabelle der erlaubten MAC-Adressen unter **Public-Spot** > **Benutzer** > **MAC-authentifizierte Benutzer** ein.

Ablauf der MAC-Adress-Prüfung

Wenn das Gerät die Anfrage eines Clients empfängt, vollzieht der Public Spot bei der automatischen Authentifizierung mit der MAC-Adresse folgende Schritte:

- Wenn der Public Spot die MAC-Adresse der empfangenen Datenpakete bereits authentifiziert hat, leitet das Gerät die zugehörigen Datenpakete weiter.
- Wenn die MAC-Adresse in der Liste der erlaubten Clients enthalten ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert und eine positive, noch gültige Authentifizierung für die MAC-Adresse im Public Spot-Cache gespeichert ist, startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Datenpakete weiter.
- Wenn ein Provider für die Prüfung der MAC-Adressen über RADIUS definiert, jedoch keine gültige Authentifizierung für die MAC-Adresse im Cache des Public Spot gespeichert ist, leitet der Public Spot die Authentifizierung der MAC-Adresse bei dem entsprechenden RADIUS-Server ein. Nach einer positiven Antwort startet der Public Spot eine neue Sitzung für diesen Benutzer und leitet die zugehörigen Pakete weiter.
- Sind alle zuvor beschriebenen Prüfungen erfolglos, leitet der Public Spot den Benutzer an die Anmeldeseite weiter.

Authentifizierung der MAC-Adresse über RADIUS

Wenn die MAC-Adresse eines anfragenden WLAN-Clients nicht in der Liste der erlaubten Adressen enthalten ist, kann der Public Spot die Adresse alternativ über einen RADIUS-Server authentifizieren.

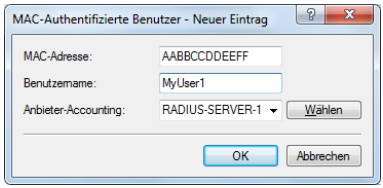
Zur Aktivierung dieser RADIUS-Authentifizierung wählt der Administrator einen der im Gerät definierten RADIUS-Server aus der Anbieter-Liste aus.

Zusätzlich definiert der Administrator eine Lebensdauer für die abgelehnten MAC-Adressen. Mit dieser Lebensdauer verhindert der Public Spot das Fluten des RADIUS-Servers mit wiederholten Anfragen nach MAC-Adressen, die weder über die MAC-Adress-Tabelle noch über den RADIUS-Server ohne Anmeldung authentifiziert werden können.

Wenn eine MAC-Adresse bei einer Anfrage zur Authentifizierung über den RADIUS-Server abgelehnt wird, speichert der Public Spot diese Ablehnung für die definierte Lebensdauer. Weitere Anfragen für die gleiche MAC-Adresse beantwortet der Public Spot innerhalb der Lebensdauer direkt ohne Weiterleitung an den RADIUS-Server.

Konfiguration in LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Parameter für die Authentifizierung der Clients über die MAC-Adresse im Dialog **Public-Spot** > **Benutzer** > **MAC-Authentifizierte Benutzer**.



Automatische Anmeldung über WISPr

Ihr Gerät stellt eine Schnittstelle für die Anmeldung über WISPr bereit. Der **WISPr**-Standard ist der technologische Vorläufer der 802.11u- und Hotspot-2.0-Spezifikation. Die Abkürzung steht für **Wireless Internet Service Provider Roaming** und bezeichnet sowohl ein Verfahren als auch Protokoll, welches Nutzern von WLAN-fähigen Endgeräten dazu ermöglicht, zwischen den WLANs unterschiedlicher Betreiber – respektive deren Internet-Service-Provider – unterbrechungsfrei zu roamen. Die Idee dahinter ähnelt somit der von 802.11u und Hotspot 2.0, erfordert allerdings eine umfassendere Betreuung durch den jeweiligen Nutzer.

Über das WISPr-Protokoll können Sie Endgeräten, für die herstellerseitig keine Unterstützung für Hotspot 2.0 mehr angeboten wird, eine Hotspot-2.0-ähnliche Anmeldung und Netzwerknutzung über Ihren Hotspot ermöglichen. Voraussetzung ist, dass Ihr Service-Provider die dazugehörige Infrastruktur

bereitstellt. Nutzerseitig erfolgt die Unterstützung entweder über das verwendete Betriebssystem oder eine geeignete App (Smart-Client). Dieser Client übernimmt für den Nutzer die Authentifizierung am Hotspot; liegen für das betreffende Netzwerk keine Authentifizierungsdaten vor, fragt der Client den Nutzer auf Systemebene nach gültigen Zugangsdaten. Für den Nutzer entfällt somit in jedem Fall die Anmeldung über eine Login-Seite in seinem Browser.

Aufgrund seines Alters unterstützen fast alle aktuelle Endgeräte mit iOS, Android und Windows 8 das WISPr-Protokoll. Darüber hinaus bieten größere WLAN-Internet-Service-Provider häufig auch eigene Apps an, um Ihren Kunden die Anmeldung zu erleichtern: Diese Apps beeinhalten eine vorkonfigurierte Datenbank der Provider-eigenen Hotspots und – optional – der Hotspots seiner Roaming-Partner. Der Ablauf der Authenifizierung entspricht dann dem folgenden Schema:

1. Ein Kunde installiert als Client die Hotspot-App seines Providers, welche in einer Datenbank vorkonfigurierte Hotspot-SSIDs bereitstellt.
2. Der Client verbindet sich automatisch mit einem dieser Hotspots und sendet einen HTTP-GET-Request an eine beliebige URL, um zu testen, ob ein direkter Internetzugriff besteht oder der Public Spot eine Authentifizierung anfordert.
3. Der Hotspot sendet im HTTP-Redirect ein WISPr-XML-Tag mit der Login-URL.
4. Der Client sendet in einem HTTP-Post seine Anmeldedaten an die Login-URL.

Beispiel für XML-Tag im Redirect:

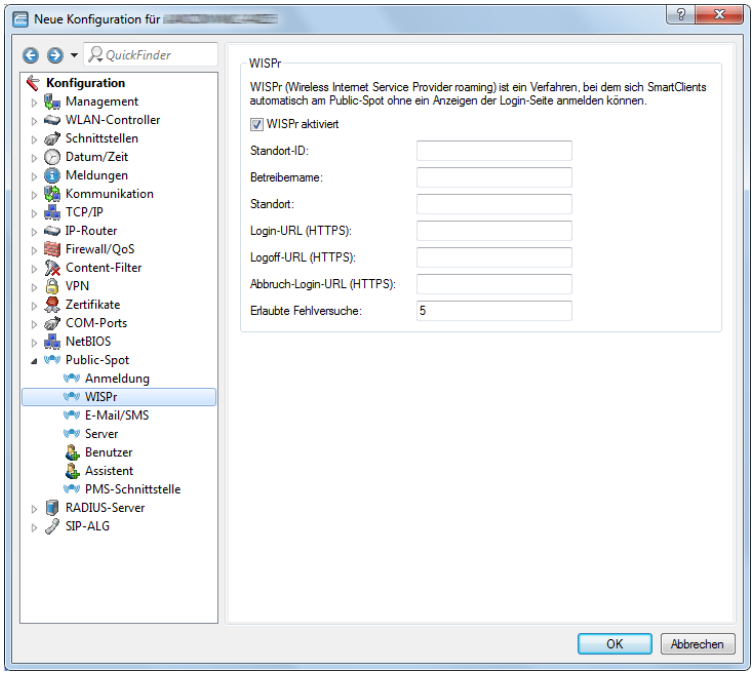
```
<HTML>
<?xml version=”1.0” encoding=”UTF-8”?>
  <WISPAccessGatewayParam
xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
   xsi:noNamespaceSchemaLocation=”http://www.acmewisp.com/WISPAccess
GatewayParam.xsd”>
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
```

```
   </WISPAccessGatewayParam>
</HTML>
```

Hinweis: Für die Nutzung von WISPr sind zwingend ein SSL-Zertifikat und ein Private-Key im Gerät erforderlich. Das Zertifikat muss entweder von einer vertrauenswürdigen Stelle signiert oder – sofern Sie ein selbst-signiertes Zertifikat verwenden – im Client als vertrauenswürdig importiert sein. Ansonsten verweigert ein Client das Login via WISPr.

WISPr konfigurieren

Die WISPr-Funktion Ihres Gerätes konfigurieren Sie über den Dialog **Public-Spot** > **WISPr**.



In diesem Dialog haben Sie folgende Einstellungsmöglichkeiten:

- **WISPr aktiviert**: Aktivieren oder deaktivieren Sie die WISPr-Funktion für das Gerät.
- **Standort-ID**: Vergeben Sie hierüber eine eindeutige Standort-Nummer oder -Kennung für Ihr Gerät, z. B. in der Form `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`.
- **Betreibername**: Geben Sie hier den Namen des Hotspot-Betreibers ein, z. B. `providerX`. Diese Angabe hilft dem Nutzer bei der manuellen Auswahl eines Internet-Service-Providers.
- **Standort**: Beschreiben Sie den Standort Ihres Gerätes, z. B. `CafeX_Markt3`. Diese Angabe dient einem Nutzer zur besseren Identifizierung Ihres Hotspots.
- **Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die die WISPr-Client die Zugangsdaten für Ihren Internet-Service-Provider übermittelt. Es kann hier eine beliebige externe URL angegeben werden oder der Public Spot selbst. Falls der Public Spot selbst Benutzer über WISPr authentifizieren soll geben Sie die URL an in der Form `https://<Device-FQDN>/wisprlogin`. Für "wisprlogin" im Beispiel kann eine beliebige, frei definierbare Sub-URL verwendet werden.
- **Logoff-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, über die sich ein WISPr-Client von Ihrem Internet-Service-Provider abmeldet. Es gelten die gleichen Regeln wie bei der Login-URL.
- **Abbruch-Login-URL (HTTPS)**: Geben Sie die HTTPS-Adresse ein, an die das Gerät einen WISPr-Client weiterleitet, wenn die Authentifizierung fehlschlägt. Es gelten die gleichen Regeln wie bei der Login-URL.

  Hinweis: Die drei URLs müssen unterschiedlich sein, falls der Public Spot im Gerät verwendet wird, z. B.:

  - Login-URL: https://<Device-FQDN>/wisprlogin
  - Logoff-URL: https://<Device-FQDN>/wisprlogoff
  - Abbruch-Login-URL: https://<Device-FQDN>/wisprabort

  Ausschließlich zu Testzwecken können Sie auch eine URL mit IP-Adressen konfigurieren. In einem Produktiv-System wird ein Client den FQDN des Zertifikates prüfen!

- **Erlaubte Fehlversuche**: Geben Sie hier die Anzahl der Fehlversuche ein, welche die Login-Seite Ihres Internet-Service-Providers maximal erlaubt. Wenn der Public Spot verwendet wird, verweigert der Public Spot nach dieser Anzahl der Fehlversuche weitere Logins vom betreffenden Client.

IEEE 802.11u und Hotspot 2.0

Ab HiLCOS 8.90 unterstützt Ihr Gerät WLAN-Verbindungen nach dem IEEE-Standard 802.11u und – darauf aufbauend – die Hotspot-2.0-Spezifikation. Über 802.11u haben Sie die Möglichkeit, in einem lokalen WLAN-Netzwerk (z. B. innerhalb Ihrer Firma) oder einem Public Spot-Netzwerk die automatische Authentisierung und Authentifizierung Ihrer Nutzer zu realisieren. Voraussetzung dafür ist, dass die betreffenden Stationen (Smartphones, Tablet-PCs, Notebooks, usw.) Verbindungen nach 802.11u und Hotspot 2.0 auch unterstützen. Folgende Funktionen bieten sich Ihnen im Detail:

- **Automatische Netzwerkwahl**

  In einer 802.11u-fähigen Umgebung entfällt für einen Benutzer die manuelle Suche und Auswahl einer SSID. Stattdessen übernehmen die Stationen eigenständig die Suche und Auswahl eines geeigneten Wi-Fi-Netzwerks, indem sie selbstständig die Betreiber- und Netzwerkdaten aller 802.11u-fähigen Access Points in Reichweite erfragen und auswerten. Eine vorangehende Anmeldung am Access Point ist dabei nicht erforderlich.

  Mit Hotspot 2.0 erhalten Stationen überdies die Möglichkeit, Informationen über die in einem Wi-Fi-Netzwerk verfügbaren Dienste abzurufen. Sind spezifische, für einen Benutzer aber relevante Dienste (z. B. Verbindungen via HTTP, VPN oder VoIP) für ein Wi-Fi-Netzwerk nicht verfügbar, werden alle Netzwerke, die die Kriterien nicht erfüllen, von der weiteren Suche ausgeschlossen. Somit ist sichergestellt, dass Nutzer immer das für sie optimale Netzwerk erhalten.

- **Automatische Authentisierung und Authentifizierung**

  In einer 802.11u-fähigen Umgebung übernimmt die Station automatisch die Anmeldung des Benutzers, sofern die notwendigen Zugangsdaten vorliegen. Die Authentifizierung kann z. B. anhand einer SIM-Karte, eines Benutzernamens und Passworts, oder eines digitalen Zertifikats erfolgen. Ein manuelles und wiederholtes Eingeben der Zugangsdaten in eine Anmeldemaske durch den Benutzer entfällt. Nach erfolgreicher Authentifizierung kann der Nutzer die benötigten Dienste unmittelbar nutzen.

- **Unterbrechnungsfreie Verbindungsübergabe (Seamless Handover)**

  Verbindungen nach 802.11u ermöglichen im Zusammenspiel mit 802.21 die unterbrechungsfreie Übergabe von Datenverbindungen über verschiedene Netzwerktypen hinweg. Dies erlaubt es Nutzern, mit ihren Stationen aus dem Mobilfunknetz unterbrechungsfrei in ein WLAN-Netz zu wechseln, sobald sie in den Empfangsbereich einer entsprechenden Hotspot-2.0-Zone kommen – und umgekehrt. Gleiches gilt für den Wechsel zwischen verschiedenen Betreibern, wenn Nutzer z. B. während einer Busfahrt von einem homogenen Netzwerk in ein anderes wechseln.

- **Automatisches Roaming**

  Verbindungen nach 802.11u ermöglichen das Roaming über unterschiedliche Betreibernetzwerke hinweg. Gelangt ein Benutzer in die Hotspot-2.0-Zone eines Betreibers, für den er keine Authentifizierungsdaten besitzt, besteht für seine Station dennoch die Option, in das Heimnetzwerk zu roamen. Die Authentifizierung an der fremden Hotspot-2.0-Zone erfolgt dann durch den Roaming-Partner des Betreibers, was den Nutzer schließlich zur Nutzung des fremden Wi-Fi-Netzwerks berechtigt. Neben Gebieten, in denen nur einzelne Netzwerkbetreiber mit Acess Points präsent sind, gewinnt diese Möglichkeit vor allem auch für Auslandsreisende an Attraktivität.

Beispiel: Angenommen, ein Nutzer ist mit seinem 802.11u-fähigen Smartphone (seiner Station) in der Stadt unterwegs und aktiviert die WLAN-Funktion, um im Internet zu surfen. Die Station beginnt daraufhin damit, alle verfügbaren Wi-Fi-Netzwerke in der Umgebung zu suchen. Bietet ein Teil der dazugehörigen Access Points 802.11u an, wählt die Station anhand der vorab erhaltenen Betreiber- und Netzinformationen dasjenige Netzwerk aus, welches am besten zum benötigten Dienst passt – z. B. einen Hotspot des der eigenen Mobilfunkgesellschaft mit Internetfreigabe. Die anschließende Authentifizierung kann in diesem Fall automatisch über die SIM-Karte erfolgen, sodass der Benutzer während des gesamten Vorgangs nicht mehr einzugreifen braucht. Die für die Verbindung gewählte Verschlüsselungsmethode – z. B. WPA2 – bleibt davon unberührt.

Zusammengefasst verknüpfen Datenverbindungen nach 802.11u und mit aktiviertem Hotspot 2.0 die Sicherheitsmerkmale und Leistungsfähigkeit klassischer Wi-Fi-Hot-Spots mit der Flexibilität und Einfachheit von Datenverbindungen über Mobilfunk. Zeitgleich entlasten sie die Mobilfunknetzwerke,

indem sie den Datenverkehr (und ggf. auch die Telefonie) auf die Netzstrecken und Frequenzbänder der Access Points umverteilen.

Hotspot-Betreiber und -Service-Provider

Die Hotspot-2.0-Spezifikation der Wi-Fi Alliance unterscheidet zwischen Hotspot-Betreibern und Hotspot-Service-Providern: Ein **Hotspot-Betreiber** unterhält lediglich ein Wi-Fi-Netzwerk, während ein **Hotspot-Service-Provider** (SP) die Verbindung der Nutzer ins Internet oder Mobilfunknetz realisiert. Natürlich ist es möglich, dass ein Betreiber gleichzeitig ein SP ist. In allen anderen Fällen jedoch benötigt ein Hotspot-Betreiber entsprechende Roaming-Vereinbarungen mit einem SP oder einem Zusammenschluss mehrerer SP (Roaming-Konsortium genannt). Erst wenn ein Betreiber diese Vereinbarungen getroffen hat, sind Kunden der entsprechenden Roaming-Partner dazu in der Lage, sich am Hotspot des Betreibers zu authentifizieren. Jeder Service-Provider betreibt dazu seine eigene AAA-Infrastruktur. Die Liste der möglichen Roaming-Partner und der Name des Hotspot-Betreibers teilt ein Hotspot den Stationen über ANQP mit (siehe Funktionsbeschreibung).

Funktionsbeschreibung

Bei **802.11u** handelt es sich um den Basis-Standard der IEEE. Dieser Standard erweitert Access Points bzw. Hotspots im Wesentlichen um die Fähigkeit, sogenannte **ANQP-Datenpakete** (Advanced Message Queuing Protocol) in seinen Funksignalen auszustrahlen. ANQP ist ein Query/Response-Protokoll, mit dem ein Gerät eine Reihe von Informationen über den Hotspot abfragen kann. Hierzu gehören sowohl Meta-Daten, wie z. B. Angaben zum Betreiber und dem Standort, als auch Angaben zum dahinterliegenden Netzwerk, wie z. B. Angaben zu Betreiber-Domänen, Roaming-Partnern, den Authentifizierungsmethoden, Weiterleitungsadressen, usw.. Alle 802.11u-fähigen Geräte in Reichweite haben die Möglichkeit, diese Datenpakete ohne vorangehende Anmeldung am Access Point abzufragen, um anhand ihrer die Netzwerkwahl und den -beitritt zu entscheiden.

Die Wi-Fi Alliance hat dem Standard weitere ANQP-Elemente hinzugefügt und vermarktet diese Spezifikation als **Hotspot 2.0**. Die Hotspot-2.0-Funktion ist somit lediglich eine Erweiterung des Standards um zusätzliche Elemente, die Geräte bei ihrer Netzwerkwahl als Kriterien heranziehen können. Hierzu gehören z. B. Angaben zu den am Hotspot verfügbaren Diensten und WAN-Metriken.

ANQP-Datenpakete stellen also das zentrale Informationselement des 802.11u-Standards dar. Um die Unterstützung für 802.11u zu signalisieren und die Datenpakete zu übertragen, bedarf es allerdings noch weiterer Elemente, die für den Betrieb von 802.11u essentiell sind:

- Die Signalisierung der 802.11u-Unterstützung in den Beacons und Probes eines Hotspots erfolgt durch das sogenannte **Interworking-Element**. In ihm sind bereits erste grundlegende Netzwerkinformationen – wie z. B. die Netzklassifikation, die Internetverfügbarkeit (Internet-Bit) und die OI des Roaming-Konsortiums und/oder des Betreibers – enthalten. Zugleich dient es 802.11u-fähigen Geräten als erstes Filterkriterium bei der Netzsuche.
- Die Übertragung der ANQP-Datenpakete erfolgt innerhalb der sogenannten GAS-Container. **GAS** steht für Generic Advertisement Service und bezeichnet generische Container, welche einem Gerät erlauben, vom Hotspot – ergänzend zu den Informationen in den Beacons – erweiterte interne und externe Informationen für die Netzwahl abzufragen. Die GAS-Container werden ihrerseits durch sogenannte Public Action Frames auf Layer 2 übermittelt.

Anmeldung eines 802.11u-fähigen Clients an einem Hotspot 2.0

Diese Funktionsbeschreibung erläutert schematisch Auswahl und Anmeldevorgang eines 802.11u-fähigen Geräts an einem Hotspot 2.0.

Anmeldung via Benutzername/Passwort oder digitalem Zertifikat

1. Die Hotspots antworten daraufhin mit einem ANQP-Response, der u. a. jeweils den Namen des Hotspot-Betreibers sowie eine Liste der NAI-Realms enthält, welche alle verfügbaren Roaming-Partner (Service-Provider, kurz SP) auflistet.
2. Das Gerät lädt die auf ihm lokal abgespeicherten Zugangsdaten aus den vom Benutzer eingerichten WLAN-Profilen oder installierten Zertifikaten, und gleicht die dortigen Realms mit den unter (2) erhaltenen NAI-Realm-Listen ab.
   a. Erzielt das Gerät hierbei einen Treffer, weiß es, dass es sich bei betreffenden Wi-Fi-Netzwerk erfolgreich authentisieren kann.
   b. Erzielt das Gerät mehrere Treffer, erfolgt die Auswahl eines Wi-Fi-Netzwerks anhand einer vom Benutzer eingerichteten Präferenzliste.

Diese Liste legt die Reihenfolge der bevorzugten Betreiber im Zusammenhang mit den möglichen Roaming-Partnern fest. Das Gerät vergleicht hierbei die unter (2) erhaltenen Betreiber-Namen mit der Liste und wählt jenen Betreiber aus, der die höchste Priorität besitzt.

3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für den passenden SP. Der Access Point übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Die Authentisierung erfolgt dabei über die vom SP festgelegte Authentifizierungsmethode; bei der Authentisierung via Benutzername/Passwort umfasst dies EAP-TTLS, bei der Authentisierung via digitalem Zertifikat EAP-TLS.

Anmeldung via (U)SIM

1. Im Unterschied zur Anmeldung via Benutzername/Passwort oder digitalem Zertifikat fragt ein Gerät bei vorliegen einer (U)SIM in seinen ANQP-Requests nicht nach der Liste der NAI-Realms, sondern der 3GPP Cellular Network Information. In den ANQP-Responses beinhaltet diese Cellular-Netzwerk-Informations-Liste alle Mobilfunkanbieter, für die der Access Point eine Authentisierung ermöglicht.
2. Das Gerät lädt aus seiner lokalen (U)SIM-Karte die Kennwerte für das Mobilfunknetzwerk und gleicht diese Daten mit den erhaltenen Cellular-Netzwerk-Informations-Listen ab. Der Listenabgleich sowie die Auswahl eines bevorzugten Betreibernetzwerkes erfolgen synonym zur Anmeldung via Benutzername/Passwort oder digitalem Zertifikat.
3. Das Gerät authentisiert sich mit seinen lokalen Zugangsdaten am Hotspot des bevorzugten Betreibers für die passende Mobilfunkgesellschaft. Der Hotspot übermittelt diese Daten seinerseits über die SSPN-Schnittstelle (Subscription Service Provider Network) an ein für die Authentifizierung zuständiges AAA-System. Durch das Vorhandensein einer (U)SIM-Karte ändert sich die mögliche Authentifizierungsmethode für das Gerät zu EAP-SIM oder EAP-AKA.
4. Das AAA-System erkundigt sich für die Authentifizierung über die MAP-Schnittstelle (Mobile Application Part) beim HLR-Server (Home Location Register) der Mobilfunkgesellschaft, um die Zugangsdaten zu verifizieren.

Im Falle einer erfolgreichen Authentisierung erhält das Gerät den Zugriff auf das WLAN-Netzwerk entweder via Hotspot (Zugangsdaten für das Betreiber-

Netzwerk liegen vor) oder automatischem Roaming (Zugangsdaten für das Betreiber-Netzwerk liegen nicht vor).

Stehen dem Gerät mehrere Authentifizierungsmöglichkeiten zur Auswahl (z. B. SIM-Karte und Benutzername/Passwort), hat es die Möglichkeit, anhand der NAI-Realm- bzw. Cellular-Netzwerk-Informations-Liste die bevorzugte EAP-Authentifizierungsmethode und damit die bevorzugten Zugangsdaten auszuwählen.

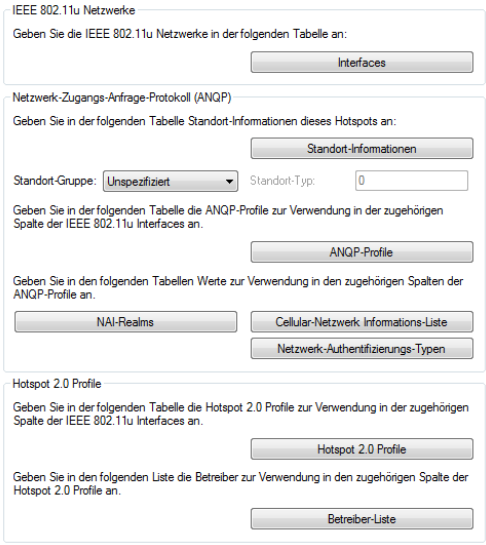
Empfohlene allgemeine Einstellungen

Die Hotspot-2.0-Spezifikation empfiehlt für den 802.11u-Betrieb folgende allgemeine Einstellungen:

- Aktivierte WPA2-Enterprise Sicherheit (802.1x)
- Authentifizierung via EAP mit der entsprechenden Variante:
  - EAP-SIM/EAP-AKA bei Authentifizierung mit SIM/USIM-Karte
  - EAP-TLS bei Authentifizierung mit digitalem Zertifikat
  - EAP-TTLS bei Authentifizierung mit Benutzername und Passwort
- Aktiviertes und eingerichtetes Proxy-ARP
- Deaktivierte Multicast- und Broadcasts in Funkzellen
- Nicht-zugelassener Datenverkehr zwischen den einzelnen mobilen Endgeräten (Layer-2 Traffic-Inspection & Filtering). Die dazugehörigen Schalter finden Sie im LANconfig unter **Wireless-LAN** > **Securtity**.
- Aktivierte und eingerichtete Firewall auf dem Access-Router, welcher den Internetzugang zur Verfügung stellt

Konfigurationsmenü für IEEE 802.11u / Hotspot 2.0

Das Konfigurationsmenü für IEEE 802.11u und Hotspot 2.0 finden Sie unter **Konfiguration** > **Wireless-LAN** > **IEEE 802.11u**.



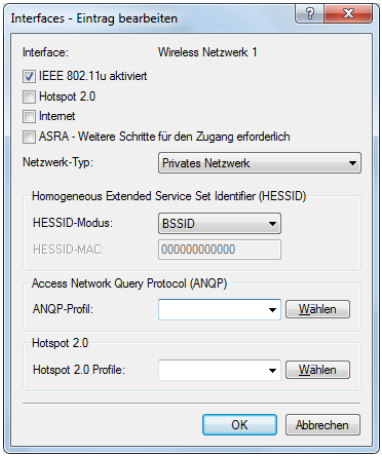
Das Gerät bietet Ihnen über die Schaltfläche **Interfaces** die Möglichkeit, die Unterstützung für den IEEE-802.11u-Standard sowie die Hotspot-2.0-Funktionalität für jede logische WLAN-Schnittstelle separat zu aktivieren bzw. deaktivieren sowie zu konfigurieren.

Ein Teil der zu konfigurierenden Parameter ist in sogenannte "Profile" ausgelagert. Über Profile gruppieren Sie Reihen unterschiedlicher Parameter in Listen, auf die Sie aus den einzelnen Dialogen lediglich referenzieren. Im Wesentlichen handelt es sich dabei um Profile für ANQP-Datenpakete sowie Hotspot 2.0. Die Beziehungen zwischen den Profillisten untereinander stellen sich wie folgt dar:

```
|-- Interfaces
  |-- ANQP-Profile
    |-- NAI-Realms
    |-- Cellular-Netzwerk Informations-Liste
    |-- Netzwerk-Authentifizierungs-Typen
  |-- Hotspot 2.0 Profile
    |-- Betreiber-Liste
```

Aktivierung für Interfaces

Die Tabelle **Interfaces** ist die höchste Verwaltungsebene für 802.11u und Hotspot 2.0. Hier haben Sie die Möglichkeit, die Funktionen für jede Schnittstelle ein- oder auszuschalten, ihnen unterschiedliche Profile zuzuweisen oder allgemeine Einstellungen vorzunehmen.



Um die Einträge in der Tabelle **Interfaces** zu bearbeiten, klicken Sie auf die Schaltfläche **Bearbeiten…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Interface**: Name der logischen WLAN-Schnittstelle, die Sie gerade bearbeiten.
- **IEEE 802.11u aktiviert**: Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Verbindungen nach IEEE 802.11u. Wenn Sie die Unterstüzung aktivieren, sendet das Gerät für die Schnittstelle – respektiv für die dazugehörige SSID – das Interworking-Element in den Beacons/Probes. Dieses Element dient als Erkennungsmerkmal für IEEE 802.11u-fähige Verbindungen: Es enthält z. B. das Internet-Bit, das ASRA-Bit, die HESSID sowie den Standort-Gruppen-Code und den Standort-Typ-Code. Diese Einzelelemente nutzen 802.11u-fähige Geräte als erste Filterkriterien bei der Netzsuche.
- **Hotspot 2.0**: Aktivieren oder deaktivieren Sie an der betreffenden Schnittstelle die Unterstützung für Hotspot 2.0 der Wi-Fi Alliance®. Hotspot 2.0 erweitert den IEEE-802.11u-Standard um zusätzliche Netzwerkinfor-

mationen, welche Stationen über einen ANQP-Request abfragen können. Dazu gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Über diese zusätzlichen Informationen sind Stationen dazu in der Lage, die Wahl eines Wi-Fi-Netzwerkes noch selektiver vorzunehmen.

- **Internet**: Wählen Sie aus, ob das Internet-Bit gesetzt wird. Über das Internet-Bit informieren Sie alle Stationen explizit darüber, dass das Wi-Fi-Netzwerk den Internetzugang erlaubt. Aktivieren Sie diese Einstellung, sofern über Ihr Gerät nicht nur interne Dienste erreichbar sind.

  Hinweis: Über diese Funktion teilen Sie lediglich die Verfügbarkeit einer Internetverbindung mit. Die entsprechenden Regularien konfigurieren Sie unabhängig von dieser Option über die Firewall!

- **ASRA - Weitere Schritte für den Zugang erforderlich**: Wählen Sie aus, ob das ASRA-Bit (Additional Step Required for Access) gesetzt wird. Über das ASRA-Bit informieren Sie alle Stationen explizit darüber, dass für den Zugriff auf das Wi-Fi-Netzwerk noch weitere Authentifizierungsschritte notwendig sind. Aktivieren Sie diese Einstellung, wenn Sie z. B. eine Online-Registrierung, eine zusätzliche Web-Authentifikation oder eine Zustimmungswebseite für Ihre Nutzungsbedingungen eingerichtet haben.

  Hinweis: Denken Sie daran, in der Tabelle **Netzwerk-Authentifizierungs-Typen** eine Weiterleitungsadresse für die zusätzliche Authentifizierung anzugeben und/oder **WISPr** für das Public Spot-Modul zu konfigurieren, wenn Sie das ASRA-Bit setzen.

- **Netzwerk-Typ**: Wählen Sie aus der vorgegebenen Liste einen Netzwerk-Typ aus, der das Wi-Fi-Netzwerk hinter der ausgewählten Schnittstelle am ehesten charakterisiert. Anhand der hier getroffenen Einstellung haben Nutzer die Wahl, die Netzsuche ihrer Geräte auf bestimmte Netzwerk-Typen zu beschränken. Mögliche Werte sind:
  - `Privates Netzwerk`: Beschreibt Netzwerke, in denen unauthorisierte Benutzer nicht erlaubt sind. Wählen Sie diesen Typ z. B. für Heimnetzwerke oder Firmennetzwerke, bei denen der Zugang auf die Mitarbeiter beschränkt ist.
  - `Privat mit Gast-Zugang`: Wie `Privates Netzwerk`, doch mit Gast-Zugang für unauthorisierte Benutzer. Wählen Sie diesen Typ z. B.

für Firmennetzwerke, bei denen neben den Mitarbeitern auch Besucher das Wi-Fi-Netzwerk nutzen dürfen.

- `Kostenpflichtiges Öffentliches Netzwerk`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und deren Nutzung gegen Entgelt möglich ist. Informationen zu den Gebühren sind evtl. auf anderen Wegen abrufbar (z. B: IEEE 802.21, HTTP/HTTPS- oder DNS-Weiterleitung). Wählen Sie diesen Typ z. B. für Hotspots in Geschäften oder Hotels, die einen kostenpflichtigen Internetzugang anbieten.
- `Kostenloses öffentliches Netzwerk`: Beschreibt öffentliche Netzwerke, die für jedermann zugänglich sind und für deren Nutzung kein Entgelt anfällt. Wählen Sie diesen Typ z. B. für Hotspots im öffentlichen Nah- und Fernverkehr oder für kommunale Netzwerke, bei denen der Wi-Fi-Zugang eine inbegriffene Leistung ist.
- `Persönliches Geräte-Netzwerk`: Beschreibt Netzwerke, die drahtlose Geräte im Allgemeinen verbinden. Wählen Sie diesen Typ z. B. bei angeschlossenen Digital-Kameras, die via WLAN mit einem Drucker verbunden sind.
- `Netzwerk für Notdienste`: Beschreibt Netzwerke, die für Notdienste bestimmt und auf diese beschränkt sind. Wählen Sie diesen Typ z. B. bei angeschlossenen ESS- oder EBR-Systemen.
- `Test oder experimentell`: Beschreibt Netzwerke, die zu Testzwecken eingerichtet sind oder sich noch im Aufbaustadium befinden.
- `Wildcard`: Platzhalter für bislang undefinierte Netzwerk-Typen.

- **HESSID-Modus**: Geben Sie an, woher das Gerät seine HESSID für das homogene ESS bezieht. Als homogenes ESS bezeichnet man den Verbund einer bestimmten Anzahl von Access Points, die alle dem selben Netzwerk angehören. Als weltweit eindeutige Kennung (HESSID) dient die MAC-Adresse eines angeschlossenen Access Points. Die SSID taugt in diesem Fall nicht als Kennung, da in einer Hotspot-Zone unterschiedliche Netwerkbetreiber die gleiche SSID vergeben haben können, z. B. durch Trivialnamen wie "HOTSPOT". Mögliche Werte für den HESSID-Modus sind:

  - `BSSID`: Wählen Sie diesen Eintrag, um die BSSID des Gerätes als HESSID für Ihr homogenes ESS festzulegen.
  - `Benutzer`: Wählen Sie diesen Eintrag, um eine HESSID manuell zu vergeben.

- `Keiner`: Wählen Sie diesen Eintrag, um Schnittstelle keinem homogenen ESS zuzuordnen und aus dem Geräteverbund zu isolieren.

- **HESSID-MAC**: Sofern Sie als **HESSID-Modus** die Einstellung `Benutzer` gewählt haben, tragen Sie hier die HESSID Ihres homogenen ESS in Form einer 6-oktettigen MAC-Adresse ein. Wählen Sie für die HESSID die BSSID eines beliebigen Access Apoints in Ihrem homogenen ESS in Großbuchstaben und ohne Trennzeichen, z. B. `008041AEFD7E` für die MAC-Adresse 00:80:41:ae:fd:7e.

  Hinweis: Sofern Ihr Gerät nicht in mehreren homogenen ESS vertreten ist, ist die HESSID für alle Schnittstellen identisch!

- **ANQP-Profil**: Wählen Sie aus der Liste ein ANQP-Profil aus. ANQP-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.
- **Hotspot 2.0 Profile**: Wählen Sie aus der Liste ein Hotspot-2.0-Profil aus. Hotspot-2.0-Profile legen Sie im Konfigurationsmenü über die gleichnamige Schaltfläche an.

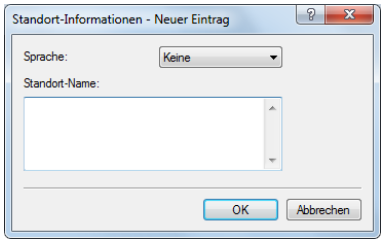
ANQP-Datenpakete konfigurieren

Standort-Informationen und -Gruppe

Über die Tabelle **Standort-Informationen** sowie den nachgelagerten Dialogabschnitt zur **Standort-Gruppe** und zum **Standort-Typ-Code** verwalten Sie die Angaben zum Standort des Access Points.

Mit Angaben zu den **Standort-Informationen** unterstützen Sie einen Nutzer bei der Auswahl des richtigen Hotspots im Falle einer manuellen Suche. Verwenden in einer Hotspot-Zone mehrere Betreiber (z. B. mehrere Cafés) die gleiche SSID, kann der Nutzer mit Hilfe der Standort-Informationen die passende Lokalität eindeutig identifizieren.

Über die **Standort-Gruppe** und den **Standort-Typ-Code** ordnen Sie dagegen Ihr Gerät – im Gegensatz zu den frei definierbaren Standort-Informationen – in eine vorgegebene Kategorie ein.



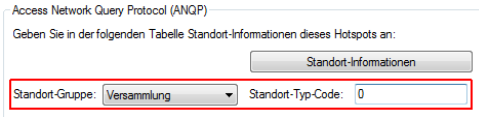
Um die Einträge in der Tabelle **Standort-Informationen** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Sprache**: Sie haben die Möglichkeit, für jede Sprache individuelle Informationen zum Standort des Access Points zu anzugeben. Ihre Nutzer bekommen dann die zur ihrer Sprache passenden Standort-Namen angezeigt. Ist eine Sprache für einen Nutzer nicht vorhanden, entscheidet seine Station, z. B. anhand der Default-Sprache.
- **Standort-Name**: Tragen Sie hier für die ausgewählte Sprache eine kurze Beschreibung zum Standort des Gerätes ein, z. B.

```
Eiscafé Valenzia
Am Markt 3
12345 Musterstadt
```

Die **Standort-Gruppe** beschreibt das Umfeld, in dem Sie den Access Point einsetzen. Sie definieren sie global für alle Sprachen. Die möglichen Werte, festgelegt durch den Venue Group Code, werden vom 802.11u-Standard vorgegeben.

Über den **Standort-Typ-Code** haben Sie die Möglichkeit, die Standort-Gruppe weiter zu spezifizieren. Auch hier sind die Werte durch den Standard spezifiziert. Die möglichen Typ-Codes entnehmen Sie bitte der nachfolgenden Tabelle.



Standort-Gruppe	***Code = Standort-Typ-Code***
Unspezifiziert	

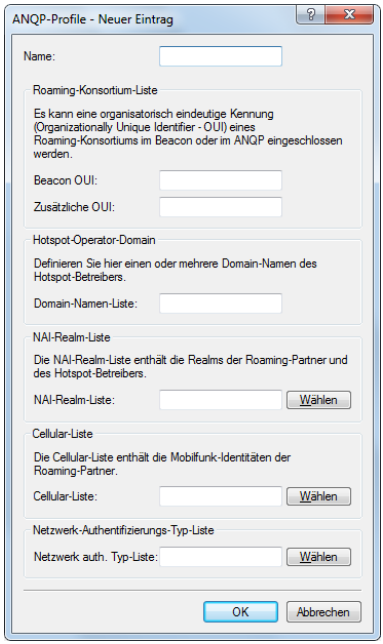
Standort-Gruppe	*Code = Standort-Typ-Code*
Versammlung	▶ 0 = Unspezifizierte Versammlung ▶ 1 = Bühne ▶ 2 = Stadion ▶ 3 = Passagier-Terminal (z. B. Flughafen, Busbahnhof, Fähranleger, Bahnhof) ▶ 4 = Amphitheater ▶ 5 = Vergnügungspark ▶ 6 = Andachtsstätte ▶ 7 = Kongresszentrum ▶ 8 = Bücherei ▶ 9 = Museum ▶ 10 = Restaurant ▶ 11 = Schauspielhaus ▶ 12 = Bar ▶ 13 = Café ▶ 14 = Zoo, Aquarium ▶ 15 = Notfallleitstelle
Geschäft	▶ 0 = Unspezifiziertes Geschäft ▶ 1 = Arztpraxis ▶ 2 = Bank ▶ 3 = Feuerwache ▶ 4 = Polizeiwache ▶ 6 = Post ▶ 7 = Büro ▶ 8 = Forschungseinrichtung ▶ 9 = Anwaltskanzlei
Ausbildung	▶ 0 = Unspezifizierte Ausbildung ▶ 1 = Grundschule ▶ 2 = Weiterführende Schule ▶ 3 = Hochschule
Fabrik und Industrie	▶ 0 = Unspezifizierte Fabrik und Industrie ▶ 1 = Fabrik
Institutional	▶ 0 = Unspezifizierte Institution ▶ 1 = Krankenhaus ▶ 2 = Langzeit-Pflegeeinrichtung (z. B. Seniorenheim, Hospiz) ▶ 3 = Entzugsklinik ▶ 4 = Einrichtungsverbund ▶ 5 = Gefängnis
Handel	▶ 0 = Unspezifizierter Handel ▶ 1 = Ladengeschäft ▶ 2 = Lebensmittelmarkt ▶ 3 = KFZ-Werkstatt ▶ 4 = Einkaufszentrum

Standort-Gruppe	*Code = Standort-Typ-Code*
	▶ 5 = Tankstelle
Wohnheim	▶ 0 = Unspezifiziertes Wohnheim ▶ 1 = Privatwohnsitz ▶ 2 = Hotel oder Motel ▶ 3 = Studentenwohnheim ▶ 4 = Pension
Lager	▶ 0 = Unspezifiziertes Lager
Dienste und sonstiges	▶ 0 = Unspezifizierter Dienst und sonstiges
Fahrzeug	▶ 0 = Unspezifiziertes Fahrzeug ▶ 1 = Personen- oder Lastkraftwagen ▶ 2 = Flugzeug ▶ 3 = Bus ▶ 4 = Fähre ▶ 5 = Schiff oder Boot ▶ 6 = Zug ▶ 7 = Motorrad
Außen	▶ 0 = Unspezifizierter Außenbereich ▶ 1 = Städtisches Wi-Fi-Netzwerk (Muni-Mesh-Netzwerk) ▶ 2 = Stadtpark ▶ 3 = Rastplatz ▶ 4 = Verkehrsregelung ▶ 5 = Bushaltestelle ▶ 6 = Kiosk

Tabelle 29: Übersicht möglicher Werte für Standort-Gruppen und -Typen

ANQP-Profile

Über diese Tabelle verwalten Sie die Profillisten für ANQP. **ANQP-Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren und sie in der Tabelle **Interfaces** unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. Angaben zu Ihren OIs, Domains, Roaming-Partnern und deren Authentifizierungsmethoden. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Um die Einträge in der Tabelle **ANQP-Profile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Name**: Vergeben Sie hierüber einen Namen für das ANQP-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die ANQP-Profile.
- **Beacon OUI**: Organizationally Unique Identifier, abgekürzt OUI, vereinfacht OI. Als Hotspot-Betreiber tragen Sie hier die OI des Roaming-Partners ein, mit dem Sie einen Vertrag abgeschlossen haben. Sind Sie als Hotspot-Betreiber gleichzeitig der Service-Provider, tragen Sie hier die OI Ihres Roaming-Konsortiums oder Ihre eigene OI ein. Ein Roaming-Konsortium besteht aus einer Gruppe von Service-Providern, die untereinander Vereinbarungen zum gegenseitigen Roaming getroffen haben. Um eine OI zu erhalten, muss sich ein solches Konsortium – ebenso wie ein einzelner Service-Provider – bei der IEEE registrieren lassen.

  Es besteht die Möglichkeit, bis zu 3 OIs parallel anzugeben, z. B. für den Fall, dass Sie als Betreiber Verträge mit mehreren Roaming-Partnern

haben. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.

Hinweis: Das Gerät strahlt die eingegebene(n) OI(s) in seinen Beacons aus. Soll das Gerät mehr als 3 OIs übertragen, lassen sich diese unter **Zusätzliche OUI** konfigurieren. Zusätzliche OIs werden allerdings erst nach dem GAS-Request einer Station übertragen; sie sind für die Stationen also nicht unmittelbar sichtbar!

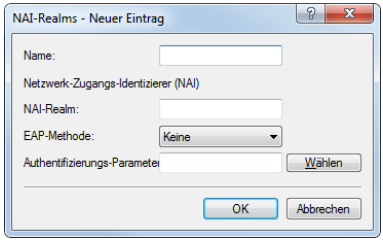
- **Zusätzliche OUI**: Tragen Sie hier die OI(s) ein, die das Gerät nach dem GAS-Request einer Station zusätzlich aussendet. Mehrere OIs trennen Sie durch eine kommaseparierte Liste, z. B. `00105E,00017D,00501A`.
- **Domain-Namen-Liste**: Tragen Sie hier eine oder mehrere Domains ein, über die Sie als Hotspot-Betreiber verfügen. Mehrere Domain-Namen trennen Sie durch eine kommaseparierte Liste, z. B. `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. Für Subdomains reicht aus, lediglich den obersten gültigen Domain-Namen anzugeben. Hat ein Nutzer z. B. providerX.org als Heimat-Provider in seinem Gerät konfiguriert, werden dieser Domain auch Access Points mit dem Domain-Namen wi-fi.providerX.org zugerechnet. Bei der Suche nach passenden Hotspots bevorzugt eine Station immer den Hostpot seines Heimat-Providers, um mögliche Roaming-Kosten über den Access Point eines Roaming-Partners zu vermeiden.
- **NAI-Realm-Liste**: Wählen Sie aus der Liste ein NAI-Realm-Profil aus. Profile für NAI-Realms legen Sie im Konfigurationsmenü über die Schaltfläche **NAI-Realms** an.
- **Cellular-Liste**: Wählen Sie aus der Liste eine Mobilfunk-Identität aus. Identitäten für Mobilfunknetzwerke legen Sie – wie bei einem Profil – im Konfigurationsmenü über die Schaltfläche **Cellular-Netzwerk Informations-Liste** an.
- **Netzwerk auth. Typ-Liste**: Wählen Sie aus der Liste einen Authentifizierungs-Profil aus. Profile zur Netzwerk-Authentifizierung legen Sie im Konfigurationsmenü über die Schaltfläche **Netzwerk-Authentifizierungs-Typen** an.

Zusätzliche haben Sie über die Telnet-Konsole bzw. das Setup-Menü die Möglichkeit, Ihren Nutzern auch den Typ der verfügbaren IP-Adresse anzuzeigen, den diese nach einer erfolgreichen Authentifizierung vom Netzwerk erhalten können. Sie erreichen die betreffenden Parameter **IPv4-Addr-Type**

und **IPv6-Addr-Type** über den Telnet-Pfad **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI-Realms

Über diese Tabelle verwalten Sie die Profillisten für die NAI-Realms. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Realms des Hotspot-Betreibers und seiner Roaming-Partner mitsamt der zugehörigen Authentifizierungs-Methoden und -Parameter. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob sie für den Hotspot-Betreiber oder einen seiner Roaming-Partner über gültige Anmeldedaten verfügen.

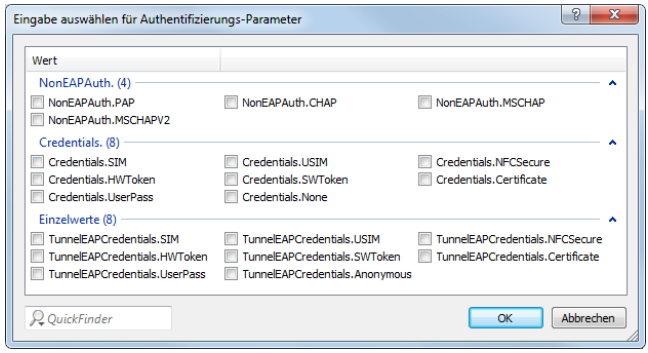


Um die Einträge in der Tabelle **NAI-Realms** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Name**: Vergeben Sie hierüber einen Namen für das NAI-Realm-Profil, z. B. den Namen des Service-Providers oder Dienstes, zu dem der NAI-Realm gehört. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **NAI-Realm-Liste**.
- **NAI-Realm**: Geben Sie hier den Realm für das Wi-Fi-Netzwerk an. Der NAI-Realm selbst ist ein Identifikationspaar aus einem Benutzernamen und einer Domäne, welches durch reguläre Ausdrücke erweitert werden kann. Die Syntax für einen NAI-Realm wird in IETF RFC 2486 definiert und entspricht im einfachsten Fall `<username>@<realm>`; für `user746@providerX.org` lautet der entsprechende Realm also `providerX.org`.
- **EAP-Methode**: Wählen Sie aus der Liste eine Authentifizierungsmethode für den NAI-Realm aus. EAP steht dabei für das Authentifizierungs-Protokoll (Extensible Authentication Protocol), gefolgt vom jeweiligen Authentisierungsverfahren. Mögliche Werte sind:

- `EAP-TLS`: Authentifizierung via Transport Layer Security (TLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch ein digitales Zertifikat erfolgt, das der Nutzer installiert.
- `EAP-SIM`: Authentifizierung via Subscriber Identity Module (SIM). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das GSM Subscriber Identity Module (die SIM-Karte) der Station erfolgt.
- `EAP-TTLS`: Authentifizierung via Tunneled Transport Layer Security (TTLS). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch einen Benutzernamen und ein Passwort erfolgt. Zur Sicherheit wird die Verbindung bei diesem Verfahren getunnelt.
- `EAP-AKA`: Authentifizierung via Authentication and Key Agreement (AKA). Wählen Sie diese Einstellung, wenn die Authentifizierung über den betreffenden NAI-Realm durch das UTMS Subscriber Identity Module (die USIM-Karte) der Station erfolgt.
- `Keine`: Wählen Sie diese Einstellung, wenn der betreffende NAI-Realm keine Authentifizierung erfordert.

▶ **Authentifizierungs-Parameter**:



Klicken Sie die Schaltfläche **Wählen** und selektieren Sie in dem sich öffnenden Eingabedialog die zur EAP-Methode passenden Authentifizierungs-Parameter, z. B. für `EAP-TTLS` `NonEAPAuth.MSCHAPV2`,`Credential.UserPass` oder für EAP-TLS `Credentials.Certificate`. Mögliche Werte sind:

Parameter	*Sub-Parameter*	*Erläuterung*
NonEAPAuth.		Bezeichnet das Protokoll, welches der Realm für die Phase-2-Authentifizierung erfordert:

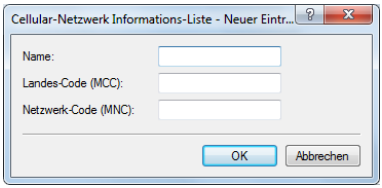
Parameter	*Sub-Parameter*	*Erläuterung*
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, ursprüngliche CHAP-Implementierung, spezifiziert im RFC 1994
	MSCHAP	CHAP-Implementierung von Microsoft v1, spezifiziert im RFC 2433
	MSCHAPV2	CHAP-Implementierung von Microsoft v2, spezifiziert im RFC 2759
Credentials.		Beschreibt die Art der Authentifizierung, die der Realm akzeptiert:
	SIM	SIM-Karte
	USIM	USIM-Karte
	NFCSecure	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate	Digitales Zertifikat
	UserPass	Benutzername und Passwort
	None	Keine Zugangsdaten erforderlich
TunnelEAPCredentials.*		
	SIM*	SIM-Karte
	USIM*	USIM-Karte
	NFCSecure*	NFC-Chip
	HWToken*	Hardware-Token
	SoftToken*	Software-Token
	Certificate*	Digitales Zertifikat
	UserPass*	Benutzername und Passwort
	Anonymous*	Anonyme Anmeldung

Tabelle 30: Übersicht der möglichen Authentifizierungs-Parameter

*) Der betreffende Parameter oder Sub-Parameter ist im Rahmen der Passpoint™-Zertifizierung für zukünftige Einsatzzwecke reserviert worden, findet gegenwärtig jedoch keine Verwendung.

Cellular-Netzwerk Informations-Liste

Über diese Tabelle verwalten Sie die Identitätslisten für die Mobilfunknetze. Mit diesen Listen haben Sie die Möglichkeit, bestimmte ANQP-Elemente zu gruppieren. Hierzu gehören die Netzwerk- und Landes-Codes des Hotspot-Betreibers und seiner Roaming-Partner. Stationen mit SIM- oder USIM-Karte nutzen diese Liste, um anhand der hier hinterlegten Angaben festzustellen, ob der Hotspot-Betreiber zu ihrer Mobilfunkgesellschaft gehört oder einen Roaming-Vertrag mit ihrer Mobilfunkgesellschaft hat.



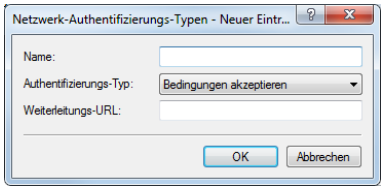
Um die Einträge in der Tabelle **Cellular-Netzwerk Informations-Liste** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Name**: Vergeben Sie hierüber einen Namen für die Mobilfunk-Identität, z. B. ein Kürzel des Netzanbieters in Kombination mit dem verwendeten Mobilfunkstandard. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Cellular-Liste**.
- **Landes-Code (MCC)**: Geben Sie hier den Mobile Country Code (MCC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen, z. B. 262 für Deutschland.
- **Netzwerk-Code (MNC)**: Geben Sie hier den Mobile Network Code (MNC) des Hotspot-Betreibers oder seiner Roaming-Partner ein, bestehend aus 2 oder 3 Zeichen.

Netzwerk-Authentifizierungs-Typen

Über diese Tabelle verwalten Sie Adressen, an die das Gerät Stationen für einen zusätzlichen Authentifizierungsschritt weiterleitet, nachdem sich die Station bereits beim Hotspot-Betreiber oder einem seiner Roaming-Partner erfolgreich authentisiert hat. Pro Authentifizierungs-Typ ist nur eine Weiterleitungsangabe erlaubt.

Hinweis: Denken Sie daran, das ASRA-Bit in der Tabelle **Interfaces** zu setzen, wenn Sie einen zusätzlichen Authentifizierungsschritt einrichten!



Um die Einträge in der Tabelle **Netzwerk-Authentifizierungs-Typen** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

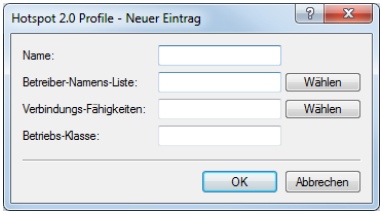
- **Name**: Vergeben Sie hierüber einen Namen für den Listeneintrag, z. B. `AGB akzeptieren`. Dieser Name erscheint später im ANQP-Profil in der Auswahl für die **Netzwerk auth. Typ-Liste**.
- **Authentifizierungs-Typ**: Wählen Sie aus der Auswahlliste den Kontext, vor dem die Weiterleitung gilt. Mögliche Werte sind:
  - `Bedingungen akzeptieren`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer die Nutzungsbedingungen des Betreibers akzeptieren muss.
  - `Online Registrierung`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, bei dem ein Benutzer erst online registrieren muss.
  - `HTTP-Weiterleitung`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via HTTP weitergeleitet wird.
  - `DNS-Weiterleitung`: Es ist ein zusätzlicher Authentifizierungsschritt eingerichtet, zu dem ein Benutzer via DNS weitergeleitet wird.
- **Weiterleitungs-URL**: Geben Sie die Adresse an, an die das Gerät Stationen für den zusätzlichen Authentifizierungsschritt weiterleitet.

Hotspot 2.0 konfigurieren

Hotspot 2.0 Profile

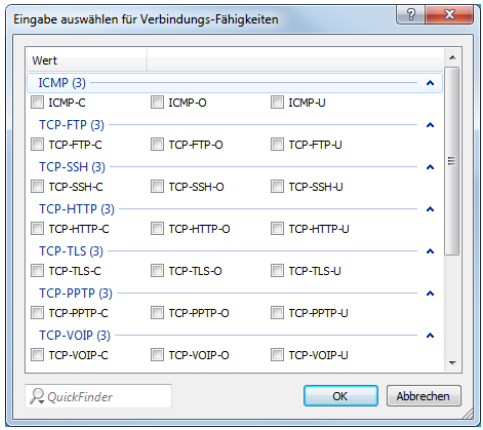
Über diese Tabelle verwalten Sie die Profillisten für Hotspot 2.0. **Hotspot 2.0 Profile** bieten Ihnen die Möglichkeit, bestimmte ANQP-Elemente (die der Hotspot-2.0-Spezifikation) zu gruppieren und sie in der Tabelle **Interfaces**

unabhängig voneinander logischen WLAN-Schnittstellen zuzuweisen. Zu diesen Elementen gehören z. B. der betreiberfreundliche Name, die Verbindungs-Fähigkeiten, die Betriebsklasse und die WAN-Metriken. Ein Teil der Elemente ist in weitere Profillisten ausgelagert.



Um die Einträge in der Tabelle **Hotspot 2.0 Profile** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

- **Name**: Vergeben Sie hierüber einen Namen für das Hotspot-2.0-Profil. Dieser Name erscheint später innerhalb der Interfaces-Tabelle in der Auswahlliste für die Hotspot-2.0-Profile.
- **Betreiber-Namens-Liste**: Wählen Sie aus der Liste das Profil eines Hotspot-Betreibers aus. Profile für Hotspot-Betreiber legen Sie im Konfigurationsmenü über die Schaltfläche **Betreiber-Liste** an.
- **Verbindungs-Fähigkeiten**:



Klicken Sie die Schaltfläche **Wählen** und geben Sie in dem sich öffnenden Eingabedialog für jeden Dienst die Verbindungs-Fähigkeit an. Stationen nutzen diese Liste, um anhand der hier hinterlegten Angaben vor einem

Netzbeitritt festzustellen, ob Ihr Hotspot die benötigten Dienste (z. B. Internetzugang, SSH, VPN) überhaupt erlaubt. Aus diesem Grund sollten so wenig Einträge wie möglich den Status "unbekannt" tragen. Mögliche Statuswerte für die einzelnen Dienste sind "closed" (`-C`), "open" (`-O`) oder "unknown" (`-U`):

- `ICMP`: Geben Sie an, ob Sie den Austausch von Informations- und Fehlermeldungen via ICMP erlauben.
- `TCP-FTP`: Geben Sie an, ob Sie Dateiübertragungen via FTP erlauben.
- `TCP-SSH`: Geben Sie an, ob Sie verschlüsselte Verbindungen via SSH erlauben.
- `TCP-HTTP`: Geben Sie an, ob Sie Internetverbindungen via HTTP/HTTPS erlauben.
- `TCP-TLS`: Geben Sie an, ob Sie verschlüsselte Verbindungen via TLS erlauben.
- `TCP-PPTP`: Geben Sie an, ob Sie das Tunneln von VPN-Verbindungen via PPTP erlauben.
- `TCP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (TCP) erlauben.
- `UDP-IPSEC-500`: Geben Sie an, ob Sie IPsec via UDP und Port 500 erlauben.
- `UDP-VOIP`: Geben Sie an, ob Sie Internettelefonie via VoIP (UDP) erlauben.
- `UDP-IPSEC-4500`: Geben Sie an, ob Sie IPsec via UDP und Port 4500 erlauben.
- `ESP`: Geben Sie an, ob Sie ESP (Encapsulating Security Payload) für IPsec erlauben.

Wenn Sie nicht wissen, ob in Ihrem Netzwerk ein Dienst verfügbar und seine Ports offen oder geschlossen sind, oder Sie gegenüber einer Station bewusst keine Angabe zum Status machen wollen, wählen Sie eine `-U`-Einstellung.

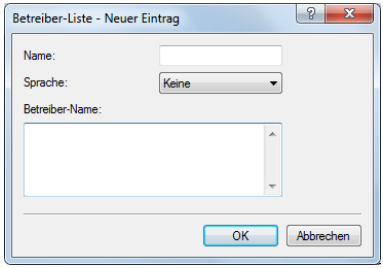
Hinweis: Über diesen Dialog legen Sie keine Berechtigungen fest! Die Angaben dienen den Stationen lediglich dazu, den Netzbeitritt über Ihr Gerät zu entscheiden. Spezifische Zugangsberechtigungen für Ihr Netzwerk konfigurieren Sie über andere Gerätefunktionen, wie z. B. die Firewall/QoS.

- **Betriebs-Klasse**: Geben Sie hier den Code für die globale Betriebsklasse des Access Points an. Über die Betriebs-Klasse teilen Sie einer Station mit, auf welchen Frequenzbändern und Kanälen Ihr Access-Point verfügbar ist. Beispiel:
  - 81: Betrieb bei 2,4 GHz mit Kanälen 1–13
  - 116: Betrieb bei 40 MHz mit Kanälen 36 und 44

  Die für Ihr Gerät passende Betriebsklasse entnehmen Sie bitte dem IEEE Standard 802.11-2012, Anhang E, Tabelle E-4: Global operating classes; erhältlich unter *standards.ieee.org*.

Betreiber-Liste

Über diese Tabelle verwalten Sie die Klartext-Namen der Hotspot-Betreiber. Ein Eintrag in dieser Tabelle bietet Ihnen die Möglichkeit, einen benutzerfreundlichen Betreiber-Namen an die Stationen zu senden, den diese dann anstelle der Realms anzeigen können. Ob sie das allerdings tatsächlich tun, ist abhängig von der Implementierung.



Um die Einträge in der Tabelle **Betreiber-Liste** zu bearbeiten, klicken Sie auf die Schaltfläche **Hinzufügen…**. Die Einträge im Bearbeitungsfenster haben folgende Bedeutung:

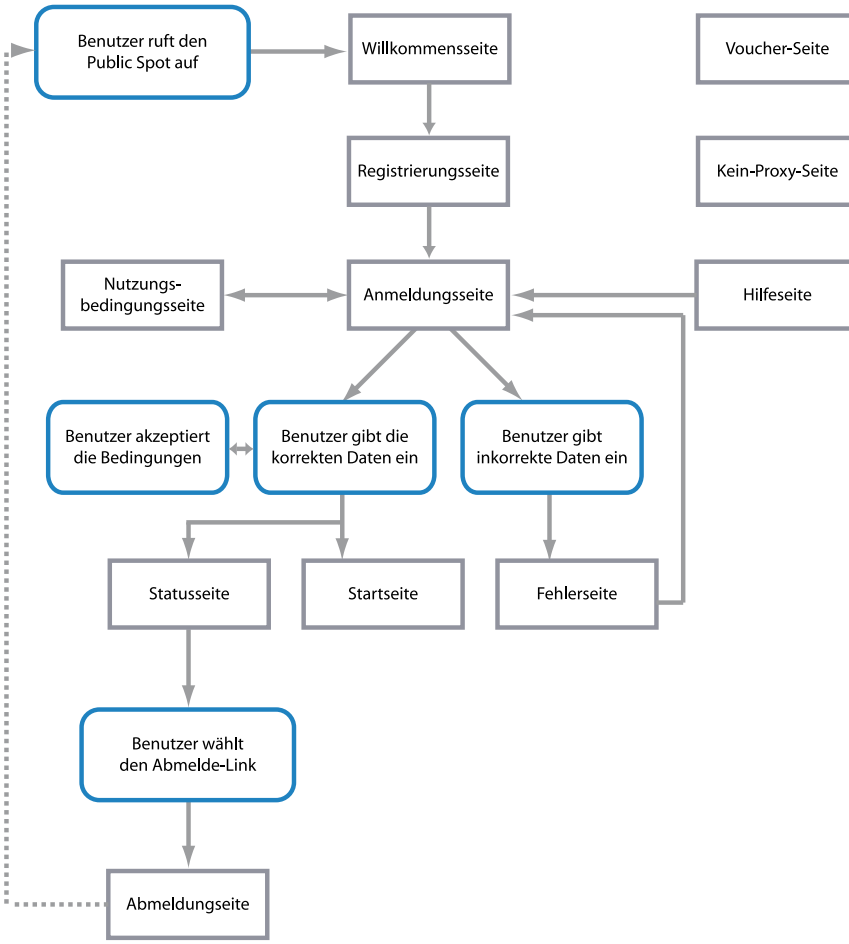
- **Name**: Vergeben Sie hierüber einen Namen für den Eintrag, z. B. eine Indexnummer oder Kombination aus Betreiber-Name und Sprache.
- **Sprache**: Wählen Sie aus der Liste eine Sprache für den Hotspot-Betreiber aus.
- **Betreiber-Name**: Geben Sie hier den Klartext-Namen des Hotspot-Betreibers ein.

14.2.5 Geräteeigene und individuelle Voucher- und Authentifizierungsseiten (Templates)

Standardmäßig greift Ihr Gerät für die Anmeldeseite und alle übrigen Authentifizierungsseiten, die Ihre Benutzer vor, während und nach einer Public Spot-Sitzung angezeigt bekommen, auf geräteintern vorinstallierte Standardseiten (Templates) zurück. Sie haben jedoch auch die Möglichkeit, die einzelnen Webseiten Ihren Bedürfnissen entsprechend anzupassen und individuell zu gestalten. Sie benötigen dazu grundlegende HTML-Kenntnisse im Umgang mit DIV-Containern und Cascading Style Sheets (CSS), um die Struktur und das Layout der einzelnen Seiten gezielt zu verändern.

Mögliche Authentifizierungsseiten

Das nachfolgende Flussdiagramm zeigt Ihnen eine Übersicht und das Zusammenspiel aller vorhandenen Authentifizierungsseiten des Public Spot-Moduls. Die Abbildung orientiert sich dabei am Beispiel der Authentisierung mittels Zugangsdaten. Je nach Anmeldungsmodus und eventuell auftretender Fehler kann das Zusammenspiel von dem nachfolgend Gezeigten jedoch leicht abweichen:



Die Seiten **Willkommen** bzw. **Anmeldung** sind jene Seiten, die ein Benutzer angezeigt bekommt, wenn er erstmalig auf das Internet bzw. den Public Spot zugreift.

- Die Seite **Willkommen** ist dabei der Anmeldungsseite vorangestellt und in fast allen Anmeldungsmodi optional: Sie können diese Seite z. B. dafür verwenden, um einen Benutzer zu begrüßen, auf Informationen zum lokalen Angebot zu verweisen oder ihm eine Kurzanleitung zur Verwendung des Public Spot bereitzustellen, bevor er auf die Startseite mit dem Anmeldeformular gelangt. Nur wenn Sie den "Login nach Einverständnis-

erklärung" als Anmeldungsmodus gewählt haben, ist eine individuelle Willkommensseite – welche die Einverständniserklärung beinhaltet – Pflicht, da sie an die Stelle des Anmeldeformulars auf der Anmeldungsseite tritt.

Wichtig: Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen keine Willkommensseite. Wenn Sie eine solche Seite einrichten, ohne zuvor eine entsprechende Vorlage ins Gerät oder auf einen externen Server zu laden, gelangt der Benutzer entweder direkt auf die Anmeldungsseite oder erhält eine Fehlermeldung (je nach Anmeldungsmodus).

- Die **Anmeldung** beinhaltet das Anmeldeformular, sofern für die Anmeldung am Public Spot die Authentisierung mittels Zugangsdaten und ggf. Anforderung der selben erforderlich ist.
- Die Seite mit den **Nutzungsbedingungen** ist nur dann zugänglich, wenn Sie die Bestätigung Ihrer Nutzungsbedingungen für den ausgewählten Anmeldungsmodus erforderlich gemacht haben. In diesem Fall erscheint unterhalb des Anmeldeformulars eine Checkbox mit einem zusätzlichen Link, der die Nutzungsbedingungen in einem Pop-Up öffnet.

Wichtig: Die Standardseiten, die in Ihrem Gerät vorinstalliert sind, umfassen für die Nutzungsbedingungs-Seite lediglich einen Platzhalter und keine generischen Nutzungsbedingungen.

Nachdem sich der Benutzer mit seinen Zugangsdaten (sofern erforderlich) autorisiert hat, überprüft das Gerät die Korrektheit der Angaben und stellt daraufhin entweder eine **Fehler**-Seite, die den Benutzer wieder auf die Anmeldeseite zurückführt, oder die **Start**-Seite dar.

- Die **Fehler**-Seite wird dabei lediglich gegenüber unauthentifizierten Public Spot-Benutzern ausgegeben und ist damit mehr oder weniger direkt mit dem Anmeldevorgang verknüpft. Typische Situationen, in denen ein Benutzer die Fehlerseite erhält, sind z. B. der unauthorisierte Zugriff auf den Public Spot, ein erreichtes Benutzerlimit sowie die fehlgeschlagene Authentifizierung durch Eingabe falscher Zugangsdaten oder Fehler beim Authentifizierungsserver. Sofern Sie eine zu überwachende Gegenstelle eingerichtet haben, erscheint die Seite außerdem immer dann, wenn das Public Spot-Modul einen Wegfall der WAN-Verbindung registriert, um einen mögliche Benutzer über die fehlende Verfügbarkeit des Netzwerks vorab

zu informieren (siehe *Fehlerseite bei Wegfall der WAN-Verbindung einrichten* auf Seite 1489).

Bereits authentifizierte Benutzer hingegen erhalten unabhängig von der Fehlerseite immer eine entsprechende Fehlermeldung von ihrem Browser.

- Sofern bei der Anmeldung keine Fehler auftraten, verifiziert die **Start**-Seite die erfolgreiche Anmeldung und leitet den Benutzer nach einigen Sekunden Wartezeit auf diejenige Internetseite weiter, die er ursprünglich erreichen wollte.

Zusätzlich öffnet sich nach einer erfolgreichen Anmeldung ein kleines Pop-Up, die **Status**-Seite:

- Die **Status**-Seite zeigt dem Benutzer aktuelle Informationen zu seiner Sitzung an (z. B. die bisherige Nutzungszeit, die gesendeten und empfangenen Datenmenge sowie Gültigkeitsdauer seines Kontos). Sie beinhaltet auch einen Link zum Schließen der aktuellen Sitzung und Beenden des Accountings. Klickt ein Benutzer auf diesen Link, gelangt er auf die Seite **Abmeldung**.
- Die Seite **Abmeldung** bestätigt einem Benutzer die erfolgreiche Abmeldung vom Public Spot.

Die verbleibenden Seiten **Rückfall-Fehler**, **Kein Proxy** und **Hilfe** sind isoliert und nicht unmittelbar mit dem Anmeldevorgang verknüpft.

- Die **Rückfall-Fehler**-Seite erscheint immer dann, wenn das Gerät eine benutzerdefinierte Template-Seite nicht ausliefern kann und der Rückfall auf die HiLCOS-interne Standardseite fehlt. Die Auslieferung scheitert z. B., wenn Sie innerhalb der Seiten-Tabelle einen falschen Datei-Pfad angegeben haben oder die Template-Seite noch nicht im Gerät vorhanden ist.
- Die **Kein-Proxy**-Seite erscheint immer dann, wenn ein Benutzer versucht, eine HTTP-Verbindung über den Port 8080 an Stelle des normalen HTTP-Ports 80 aufzubauen. Der Port 8080 wird in Intranets typischerweise für HTTP-Proxies verwendet. Da Proxies aber als statische IP-Adresse in den Browsereinstellungen hinterlegt werden, diese sich jedoch nicht über DHCP konfigurieren lassen, liesse sich der Proxy nicht erreichen. Die Seite hat daher nur den Zweck, dem Benutzer eine Anleitung zum Deaktivieren seiner Proxy-Einstellungen zu bieten, bevor er fortfahren kann.
- Die **Hilfe**-Seite ist lediglich ein Platzhalter, um bestimmte Informationen (z. B. Details zur Anmeldung oder Erhaltbarkeit von Vouchern) in die

übrigen Authentifizierungsseiten (z. B. die Willkommensseite) einzubetten. Die vorinstallierten Seiten beinhalten keine Hilfe-Seite und auch keinen Link, der auf diese Seite verweist. Um die Hilfe-Seite zu nutzen, müssen Sie demnach eine individuelle Vorlagenseite einrichten.

Keine Authentifizierungsseite stellt die Seite **Voucher** dar: Hierbei handelt es sich um die grafische Vorlage für den Voucher-Druck. Indem Sie dafür eine eigene Vorlage hochladen, können Sie Tickets z. B. im Corporate Design Ihres Unternehmens ausgeben.

Vorinstallierte Standardseiten

Ihr Gerät enthält im Lieferzustand bereits einen Satz vorinstallierter Seiten, mit denen sich ein funktionsfähiger Public Spot-Betrieb bereitstellen lässt.

Die nachfolgende Tabelle gibt Ihnen eine schnellen Überblick über die im HiLCOS enthaltenen Standardseiten:

Seitenbezeichnung	***Vorinstalliert?***
Willkommen…	nein
Anmeldung…	ja
Fehler…	ja
Start…	ja
Status…	ja
Abmeldung…	ja
Hilfe…	nein
Kein Proxy…	nein
Voucher…	ja
Nutzungsbedingungen…	nein
Rückfall-Fehler…	ja
Anmeldung(E-Mail)…	ja
Registrierung(E-Mail)…	ja
Anmeldung(E-Mail zu SMS)…	ja

Seitenbezeichnung	*Vorinstalliert?*
Registrierung(E-Mail zu SMS)…	ja

Tabelle 31: Übersicht aller vorinstallierten Standardseiten

Die Seiten wurden mit der Absicht entwickelt, so simpel wie möglich zu sein, und verwenden daher keine komplexen Techniken wie z. B. Java Skript oder dynamisches HTML. Durch die Verwendung von schlichtem XHTML und CSS für allein die notwendigen Elemente ist sichergestellt, dass sie auf einer Vielzahl von Browsern und Bildschirmgrößen korrekt angezeigt werden.

Als Betreiber eines Hotspots möchten Sie ggf. aber etwas anspruchsvollere Seiten darstellen oder eine möglichst neutrale Seite ohne Herstellerbezug anzeigen. Das Public Spot-Modul bietet Ihnen daher die Möglichkeit, einzelne Standardseiten wahlweise zu Personalisieren oder durch selbstgestaltete Seiten zu ersetzen. Letzteres erreichen Sie entweder mittels HTTP-Umleitungen oder Vorlagen, die Sie in das Gerät laden, und welche das Gerät dann wie ein intelligenter HTML-Preprozessor bearbeitet. Diese Seitenvorlagen lassen sich direkt in den Flash-Speicher laden, wodurch Sie auf einen externen HTTP-Server verzichten können.

Zusätzliche Sprachen für die Authentifizierungsseiten

HiLCOS 8.90 erweitert die vom Public Spot-Modul ausgegeben Authentifizierungsseiten (d. h. alle vorinstallierten Standardseiten bis auf die Voucher-Seite) um die Sprachunterstützung für Französisch, Spanisch, Italienisch und Niederländisch. Somit haben Sie die Möglichkeit, einem breiteteren internationalen Nutzerspektrum einen Public Spot-Zugang in der jeweiligen Landessprache anzubieten. Die Ausgabe der entsprechenden Sprache erfolgt wie bisher über die Spracheinstellungen des Webbrowsers, mit denen der Nutzer den Public Spot aufruft.

Hinweis: Die Mehrsprachigkeit bezieht sich ausschließlich auf die 8.90-internen Standardseiten. Mehrsprachige inidividuelle Vorlagenseiten lassen sich jedoch unter Zuhilfenahme eines externen Servers realisieren.

Personalisierung der Standardseiten

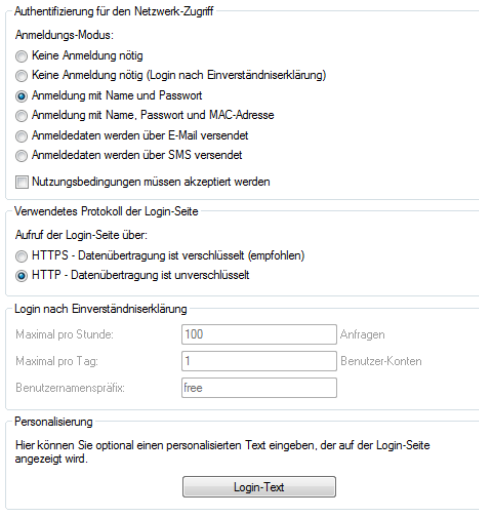
Als Alternative zu den benutzerdefinierten Seiten bietet Ihnen das Gerät die Möglichkeit, die vorinstallierten Standardseiten in begrenztem Umfang zu personalisieren. Hierzu gehören z. B. die Eingabe eines Login-Textes, welcher Ihren Benutzern innerhalb des Anmeldeformulars angezeigt wird, oder das Austauschen der Header-Grafik (dem sogenannten Kopfbild). Auf diese Weise können Sie schnell einen individuellen Public Spot-Betrieb bereitstellen, ohne sich eingehend mit dem Thema der Webseitenerstellung zu beschäftigen.

Individueller Text auf der Anmeldeseite

Sie haben innerhalb des Public Spot-Moduls die Möglichkeit, einen individuellen Text anzugeben, welcher auf der Anmeldeseite innerhalb der Box des Anmeldeformulars eingeblendet wird. Dieser **Login-Text** ist in mehreren Sprachen hinterlegbar; welche Sprache das Gerät letztlich ausgibt, hängt von den Spracheinstellungen des vom Benutzer verwendeten Webbrowsers ab. Wenn Sie für eine Sprache keinen individuellen Login-Text spezifizieren, greift das Gerät auf den englischen Login-Text zurück (sofern vorhanden).

Um einen individuellen Text auf der Anmeldeseite einzurichten, führen Sie dazu die nachfolgenden Schritte aus.

1. Öffnen Sie in LANconfig den Konfigurationsdialog für das betreffende Gerät.
2. Wechseln Sie in den Dialog **Public Spot** > **Anmeldung**, klicken Sie **Login-Text** und wählen Sie eine Sprache aus.



3. Tragen Sie in dem sich öffnenden Dialog den Text ein, den Sie Ihren Public Spot Nutzern anzeigen möchten. Erlaubt ist ein HTML-String mit max. 254 Zeichen, bestehend aus:

```
[Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&amp;'()+-,/:;&lt;=>?[\]^_.#*
```

   LANconfig transformiert eingegebene Umlaute automatisch in ihre entsprechenden Umschreibungen (ü zu ue; ß zu ss; usw.). Um Umlaute einzugeben, müssen Sie deren HTML-Äquivalente verwenden (z. B. `&uuml;` für ü), da der Text unmittelbar in die Webseite eingebunden wird. Über HTML-Tags haben Sie außerdem die Möglichkeit, den Text zusätzlich zu strukturieren und zu formatieren. Beispiel:

```
Herzlich Willkommen!<br/><i>Bitte f&uuml;llen Sie das Formular aus.</i>
```

4. Klicken Sie **OK**, um die Eingabe abzuschließen, und laden Sie die Konfiguration zurück in das Gerät.

Nach dem erfolgreichen Schreiben der Konfiguration erscheint der Login-Text beim nächsten Aufruf der Public Spot-Seite.

Individuelle Kopfbilder für variable Bildschirmbreiten

Bestandteil der im Gerät vorinstallierten Seiten ist eine Header-Grafik (Kopfbild genannt), die Ihren Benutzern beim Aufruf des Public Spots oberhalb des Anmelde-Formulars anzeigt wird. Sie können dieses Kopfbild nach Belieben ändern, um z. B. eine dem Einsatzumfeld oder Ihrem Coporate Design angemessene Grafik einzubinden. Sie benötigen dafür keine externen Webserver, sondern können über das Dateimanagement in WEBconfig bzw. die Konfigurationsverwaltung in LANconfig die Grafik direkt ins Gerät laden.

Eine Besonderheit des Kopfbildes ist dabei, dass es im Gerät in zwei unterschiedlichen Variaten vorliegt: Einmal als Großbild für Bildschirme bzw. Browser-Fenster mit einer horizontalen Auflösung >800 px (normale Monitore, Laptops, Tablet-PCs usw.) und einmal als Kleinbild für Bildschirme mit einer geringeren horizontalen Auflösung (PDAs, Mobiltelefone usw.). Auf diese Weise haben Sie die Möglichkeit, Kopfbilder für unterschiedliche Zielgruppen bereitzustellen und diesen stets ein für Ihr Gerät geeignetes Anmelde-Formular anzubieten.

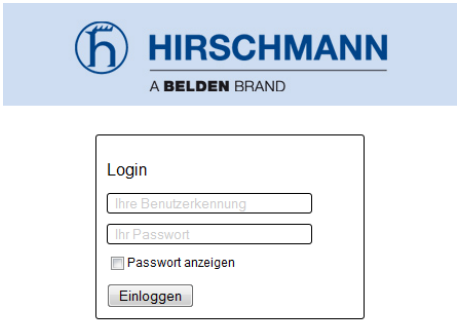


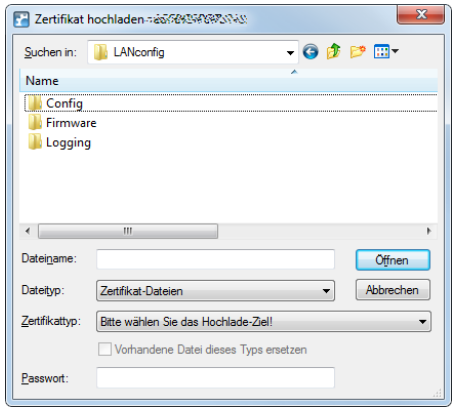
Abbildung 17: Anmeldeseite für breite Bildschirme

Abbildung 18: Anmeldeseite für schmale Bildschirme

Die möglichen Auflösungen werden durch die CSS-Datei des Gerätes vorgegeben. Für die vorinstallierten Standardgrafiken betragen sie 800x150 px für das Großbild und 258x52 px für das Kleinbild. Der Dateityp muss entweder JPG, GIF oder PNG sein.

Um ein neues Kopfbild als Groß- oder Kleinvariante ins Gerät zu laden, führen Sie die nachfolgenden Schritte aus.

1. Starten Sie LANconfig und markieren Sie das betreffende Gerät.
2. Klicken in der Menüleiste auf **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen**. Der Dialog **Zertifikat hochladen** öffnet sich.



3. Stellen Sie den **Dateityp** auf **Alle Dateien** und wählen Sie den **Zertifikattyp**, den Sie hochladen möchten.
   - **Public Spot - Kopfbild Seiten**: Zertifikattyp für das Großbild
   - **Public Spot - Kopfbild Box**: Zertifikattyp für das Kleinbild

4. Wählen Sie Ihr individuelles Kopfbild aus und klicken Sie auf **Öffnen**. LANconfig beginnt daraufhin mit dem Dateiupload.

Nach dem erfolgreichen Upload erscheint das neue Kopfbild beim nächsten Aufruf der Public Spot-Seite.

Hinweis: Sie können das Zusammenspiel von großem und kleinen Kopfbild überprüfen, indem Sie den Public Spot mit einem Browserfenster >800 px aufrufen und dann die Fensterbreite verkleinern. Durch die eingesetzten CSS-Techniken schaltet die Webseite automatisch zwischen Groß- und Kleinbild um.

Hersteller-Logo und -Kopfbild im Voucher ein-/ausblenden

Ein vom Gerät ausgegebener Voucher enthält standardmäßig das von der Public Spot-Startseite bekannte Kopfbild und Logo. Sie haben die Möglichkeit, die Einbindung dieser Grafiken über die Option **Public-Spot** > **Assistent** > **Kopfbild und Logo mitdrucken** direkt im Gerät zu deaktivieren, ohne dafür ein individuell angepasstes Vouchers-Template einzusetzen, welches diese Grafiken entfernt. In dem Fall gibt das Gerät lediglich einen textneutralen Voucher aus.

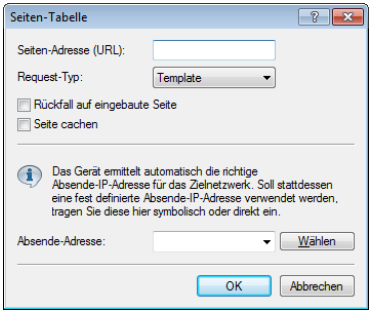
Konfiguration benutzerdefinierter Seiten

Sofern Sie die vorinstallierten Seiten durch selbstgestaltete Webseiten ersetzen möchten, können Sie diese entweder direkt im Gerät oder auf einem externen HTTP-Server ablegen. Anspruchsvollere HTML-Seiten benötigen ggf. mehr Speicherplatz, als im Gerät zur Verfügung steht. Darüber hinaus bietet Ihnen die Bereitstellung der Webseiten durch einen externen Server noch weitere Vorteile:

- Änderungen lassen sich zentral durchführen. Dadurch reduziert sich der Aufwand, die Anmeldeseiten bei Einsatz mehrerer Geräte in jedem Gerät ändern zu müssen.
- Der Server kann dynamische Seiten bereitstellen, deren Erscheinungsbild davon beeinflusst wird, welche Informationen ihm das Gerät liefert. Auf diese Informationen wird in den folgenden Kapiteln noch näher eingegangen.

Der Speicherort der Vorlagenseiten geben Sie im LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** > **Seiten-Adresse (URL)** ein. Es stehen Ihnen drei Protokolle für die URL zur Auswahl:

- `http://`…: Lädt die Seite über HTTP von einem externen Server herunter. Das Überschreiben des Standard-TCP-Ports sowie das Angeben von Benutzerdaten ist möglich
- `https://`…: Verhält sich genau wie HTTP, aber verwendet SSL um die Verbindung zu verschlüsseln.
- `file://`…: Verwendet eine Vorlage aus dem lokalen Speicher des Geräts.



Sie können beliebige Dateinamen verwenden. Sofern Sie sich für die Ablage der Templateseiten im lokalen Speicher des Geräts entscheiden, verwendeten Sie die speziell für den jeweiligen Zweck reservierten URLs. Durch Angabe der lokalen URL als **Seiten-Adresse (URL)** z. B. wird eine geräteeigene Standardseite durch eine ins Gerät geladene Seite ersetzt.

Lokale URL im Gerät	***Seitenbezeichnung***
file://pbspot_template_welcome	Willkommen…
file://pbspot_template_login	Anmeldung…
file://pbspot_template_error	Fehler…
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Abmeldung…
file://pbspot_template_help	Hilfe…
file://pbspot_template_noproxy	Kein Proxy…
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Nutzungsbedingungen…

Lokale URL im Gerät	*Seitenbezeichnung*
file://pbspot_template_fallback	Rückfall-Fehler…
file://pbspot_template_reg_email	Registrierung(E-Mail)…
file://pbspot_template_login_email	Anmeldung(E-Mail)…
file://pbspot_template_reg_sms	Registrierung(E-Mail zu SMS)…
file://pbspot_template_login_sms	Anmeldung(E-Mail zu SMS)…

Tabelle 32: Übersicht der reservierten Dateinamen für Vorlagenseiten

*) Vorlagenseite für den Voucher-Druck, keine Authentifizierungsseite

Hinweis: Durch das Hochladen benutzerdefinierter Webseiten werden die im Geräte vorinstallierten Webseiten nur ersetzt, nicht jedoch überschrieben. Sie können durch Löschen der lokalen URL jederzeit wieder zu den geräteeigenen Standardseiten zurückkehren.

Hinweis: Um eine Möglichst hohe Kompatibilität mit den verschienenen Anzeigegeräten und Web-Browsern zu erreichen, sollten Sie nach Möglichkeit auf den Einsatz von Frames verzichten. Auch spezielle Inhalte (JavaScript, Plug-In-Elemente) können zu einer fehlerhaften Anzeige führen.

Login-Seiten in Abhängigkeit vom Anmeldungsmodus

Die nachfolgende Tabelle liefert Ihnen darüber hinaus eine Übersicht, welche Login-Seite das Gerät in welchem Anmeldungsmodus ausgibt. Sofern für einen Anmeldungsmodus keine individuelle Seitenvorlage eingerichtet ist; verwendet das Public Spot-Modul dafür die 8.90-interne Standardseite:

Anmeldungsmodus	*Seitenbezeichnung*
Keine Anmeldung nötig	–
Keine Anmeldung nötig (Login nach Einverständniserklärung)	Willkommen…
Anmeldung mit Name und Passwort	Anmeldung…
Anmeldung mit Name, Passwort und MAC-Adresse	Anmeldung…
Anmeldedaten werden über E-Mail versendet	▶ Registrierung(E-Mail)… ▶ Anmeldung(E-Mail)…

Anmeldungsmodus	*Seitenbezeichnung*
Anmeldedaten werden über SMS versendet	▶ Registrierung(E-Mail zu SMS)… ▶ Anmeldung(E-Mail zu SMS)…

Tabelle 33: Übersicht der Login-Seiten der einzelnen Anmeldungsmodi

Besondere Template-Seiten für Smart Ticket

Während das Public Spot-Modul in HiLCOS-Versionen vor 8.90 noch eine zentrale Login-Seite für sämtliche Anmeldemodi verwendet, haben Sie ab HiLCOS 8.90 die Möglichkeit, für die Smart-Ticket-Funktion (die selbstständige Benutzeranmeldung via E-Mail/SMS) gesonderte Template-Seiten ins Gerät zu laden. Dazu konfigurieren Sie für die Anmeldung über E-Mail/SMS je zwei Seiten: **Registrierung(…)** und **Anmeldung(…)**.

- Auf der Registrierungsseite geben Benutzer zunächst ihre persönlichen Daten (E-Mail-Adresse oder Mobilfunknummer) ein, um sich beim Public Spot zu registrieren und dessen Zugangsdaten anzufordern.
- Auf der Anmeldungsseite geben Benutzer die ihnen zugesendeten Zugangsdaten ein, um sich schlussendlich am Public Spot zu authentisieren.

Die nachfolgende Tabelle liefert Ihnen eine Übersicht aller damit in Verbindung stehenden Abhängigkeiten, die Sie für das erstellen eigener Seitenvorlagen (Templates) benötigen:

Anmeldungsmodus	*Seitenbezeichnung*	*Lokale URL im Gerät*	*Seitenvorlagen-Bezeichner*
Anmeldedaten werden über E-Mail versendet	Registrierung(E-Mail)…	file://pbspot_template_reg_email	<regemailform>
	Anmeldung(E-Mail)…	file://pbspot_template_login_email	<loginemailform>
Anmeldedaten werden über SMS versendet	Registrierung(E-Mail zu SMS)…	file://pbspot_template_reg_sms	<regsmsform>

Anmeldungsmodus	*Seitenbezeichnung*	*Lokale URL im Gerät*	*Seitenvorlagen-Bezeichner*
	Anmeldung(E-Mail zu SMS)…	file://pbspot_template_login_sms	<loginsmsform>

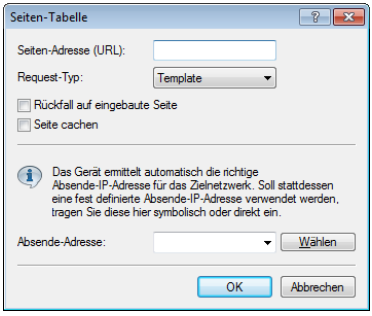
Tabelle 34: Übersicht der Abhängigkeiten der SmartTicket-Anmeldeseiten

Einrichten einer individuellen Vorlagenseite

Über eine individuelle Vorlagenseite (auch Template-Seite genannt) haben Sie Möglichkeit, die HiLCOS-eigenen Vorlagenseiten durch eigene Webseiten zu ersetzen. Die HiLCOS-eigenen Vorlagenseiten werden dabei nicht überschrieben, sondern lediglich gegen Ihre eigene Seite ausgetauscht, sodass Sie bei Bedarf auf diese standardmäßig installierten Seiten zurückgreifen können.

Die nachfolgenden Schritte zeigen Ihnen am Beispiel einer **Login**-Seite, wie Sie mit Hilfe von LANconfig eine individuelle Vorlagenseite korrekt einrichten.

1. Laden Sie Ihre individuell erstellte Fehlerseite wahlweise auf einen externen HTTP(S)-Server oder als **Public Spot - Login-Seite (*.html, *.htm)** in den Speicher des Gerätes.
2. Öffnen Sie den Konfigurationsdialog des Gerätes in LANconfig, wechseln Sie in den Dialog **Public-Spot** > **Server** und wählen Sie **Seiten-Tabelle** > **Anmeldung**.



3. Tragen Sie unter **Seiten-Adresse (URL)** wahlweise die URL der Anmeldungsseite auf dem externen Server oder den gerätelokalen Dateiverweis ein (`file://pbspot_template_login`).
4. Nehmen Sie bei Bedarf weitere optionale Einstellungen vor.

- **Request-Typ**: Sofern Sie einen externen Server einsetzen, haben Sie die Möglichkeit die Art des Seitenaufrufs verändern. Standardmäßig (in der Einstellung **Template)** lädt das Gerät eine extern gespeicherte HTM(L)-Seite von der angegebenen URL zur weiteren Verarbeitung durch den internen HTTP-Server. Wenn Sie die Einstellung zu **Redirect** ändern, lagert das Gerät die Seiten-Erzeugung an den externen Server aus (siehe auch *Benutzerdefinierte Seiten via HTTP Redirect* auf Seite 1557).
- **Rückfall auf eingebaute Seite**: Sofern Sie einen externen Server einsetzen und als Template-Typ **Request** gewählt haben, besteht die Möglichkeit, dass das Public Spot-Modul im Falle von HTTP(S)-Fehlern (z. B. Unerreichbarkeit des Servers) die HiLCOS-eigene Vorlagenseite benutzt, um ggf. einen Weiterbetrieb des Public Spots zu ermöglichen (siehe auch *Auto-Fallback* auf Seite 1558. Wenn Sie diese Einstellung nicht aktivieren, zeigt der Public Spot stattdessen die Rückfall-Fehler-Seite an.
- **Seite cachen**: Auf einigen Geräten haben Sie die Möglichkeit, lokale und externe Templates zu cachen. Mehr dazu erfahren Sie unter *Template Caching* auf Seite 1555.
- **Absende-Adresse**: Über diese Einstellung definieren Sie optional die Loopback-Adresse, die das Gerät benutzt, um sich mit dem externen HTTP(S)-Server zu verbinden. Standardmäßig schickt der Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über verschiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

5. Schließen Sie den Dialog sowie den allgemeinen Konfigurationsdialog mit jeweils einem Klick auf **OK**. LANconfig schreibt die getätigten Einstellungen daraufhin zurück in das Gerät.

Fertig!

Template Caching

Bei der Konfiguration benutzerdefinierter Template-Seiten haben Sie auf Geräten mit hinreichend großem Arbeitsspeicher (z. B. Public Spot-Gateways)

die Möglichkeit, Templates im Gerät zu cachen. Das Caching verbessert die Performance des Public Spot-Moduls insbesondere in größeren Szenarien, indem das Gerät einmal geladene Templates und daraus erzeugte HTML-Seiten intern zwischenspeichert.

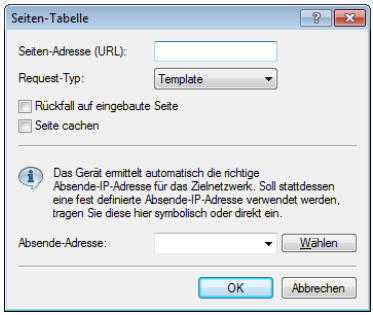
Das Caching ist möglich für:

- Templates abgelegt im lokalen Dateisystem
- Templates abgelegt auf externen HTTP(S)-Servern über statische URLs

Templates auf externen Servern, die mittels Template-Variablen referenziert werden, werden vom Gerät nicht gecached.

Template Caching aktivieren

Um das Caching für eine Seitenvorlage zu aktivieren, setzen Sie in LANconfig unter **Public-Spot** > **Server** > **Seiten-Tabelle** > **<Name der Vorlagenseite>** die Einstellung **Seite cachen**.



Im Setup-Menü finden Sie den dazugehörigen Paramter unter **Public-Spot-Modul** > **Seitentabelle** > **Template-Cache** .

Template Cache löschen

Das Gerät löscht bzw. aktualisiert im Cache gespeicherte Templates automatisch, sobald Sie eine neue Template-Datei in das Dateisystem Ihres Gerätes laden (bei lokaler Speicherung) bzw. die Cache-Zeit für ein HTTP(S)-Template abläuft (bei Speicherung auf externem einem Server). Hierzu wertet das Gerät den `Cache-Control`-Header eines HTTP(S)-Templates aus, um die maximale Cache-Zeit zu erfahren.

Wichtig: Sofern kein `Cache-Control`-Header gesetzt ist, wird die Webseite nicht gecached und direkt wieder verworfen. Achten Sie beim Einrichten eines individuellen Templates somit darauf, das entsprechende META-Tag in Verbindung mit einer sinnvollen Cache-Zeit (in Sekunden) zu setzen, z. B. `<meta http-equiv="cache-control" content="max-age=60">`. Die Dauer der Cache-Zeit ist dabei vom Szenario abhängig; es gibt keine konkreten Empfehlungen.

Sie haben aber auch die Möglichkeit, den Template Cache über eine Aktion manuell zu löschen. Starten Sie dazu im Status-Menü unter **Public-Spot** die Aktion **Flush-Template-Cache**.

Benutzerdefinierte Seiten via HTTP Redirect

Sofern Sie benutzerdefinierte Seiten als Umleitung realisieren (Request-Typ: Redirect), setzt Ihr Gerät diese wie folgt um: Immer, wenn Ihr Gerät eine betreffende Seite an einen Client liefern muss, erweitert es die URL gemäß der im vorangegangenen Kapitel vorgestellten Platzhalter und sendet eine HTTP-Antwort 307 (temporäre Umleitung) mit dieser URL an den Client.

Umleitungen sind besonders dann sinnvoll, wenn Sie eine Willkommensseite verwenden und alle Authentifizierungen auf einem externen Gateway erfolgen sollen. In diesem Fall können die Clients sofort zu diesem Gateway umgeleitet werden. Dieses Feature wird oft gemeinsam mit der externen Gerätekontroller verwendet.

Benutzerdefinierte Seiten über Seitenvorlagen

Alternativ kann das Gerät auch selbst als Client auftreten und die erweiterte URL verwenden um, um über eine HTTP-Verbindung die benutzerdefinierte Seite herunterzuladen. Der interne Preprozessor übernimmt die Bearbeitung der Seite und sendet das Ergebnis anschließend an den Public Spot-Nutzer. Diese Vorverarbeitung erlaubt es, Session-spezifische Daten zu verarbeiten, obwohl der Server eine statische Seite bereithält. Das Gerät verwendet Syntax-Befehle, wie sie bei Web-Browsern bekannt sind. Allerdings beherrscht es allerdings nur eine Teilmenge der möglichen Befehle:

- Die Benutzer-Authentifizierung erfolgt über die Form `user:password@host/...`

- Das Gerät kann nicht-fatale HTTP-Fehler, wie z. B. Redirects, nicht automatisch bereinigen. Stellen Sie also sicher, dass der Zugriff auf die Seite diese Seite auch direkt ausgibt.

Sie können symbolische Namen anstatt IP-Adressen für die Server-Hosts verwenden, solange der DNS korrekt konfiguriert ist. Dieser Mechanismus lässt sich daher in vielerlei Hinsicht als ein Proxy begreifen, der HTML-Seiten einholt und dann an die Clients weiterreicht. Der größte Unterschied ist dabei, dass die URL der Seiten im Gerät und nicht vom Client des Public Spot-Benutzers festgelegt werden.

Auto-Fallback

Für jeden Eintrag in der Seiten-Tabelle lässt sich individuell festlegen, ob eine Fallback-Funktion benutzt werden soll oder nicht. Diese Fallback-Funktion hat nur dann eine Bedeutung, wenn eine Seite als Vorlage (Request-Typ: Template) und nicht als Umleitung (Request-Typ: Redirect) definiert ist. Beim Herunterladen einer Seite über HTTP können eine Reihe von Fehlern auftreten:

- Das Nachschlagen eines Hosts beim DNS kann fehlschlagen.
- Die TCP/HTTP-Verbindung zum Server kann fehlschlagen.
- Der HTTP-Server kann eine Fehlermeldung ausgeben (wie z. B. 404, wenn eine ungültige URL angefragt wurde).

Standardmäßig gibt das Gerät solche Fehler an den Benutzer weiter, damit dieser eine erneute Anfrage starten oder den Betreiber des Public Spots davon in Kenntnis setzen kann. Alternativ kann das Konfigurieren einer Fallback-Funktion sicherstellen, dass der Hotspot weiter funktioniert, indem das Gerät stattdessen die standardmäßig installierten Seiten verwendet. Sie aktivieren die Fallback-Funktion im LANconfig über die Einstellung **Rückfall auf eingebaute Seite**.

Weitergegebene HTTP-Attribute

Wie bereits erwähnt kann das Gerät in einige Punkten als eine Art HTTP-Proxy gesehen werden, dass die Anmelde- und Status-Seite einholt. HTTP-Proxies sollten bestimmte Attribute intakt lassen, wenn Sie Anfragen des Clients weiterleiten:

- Das Gerät leitet Cookies zwischem dem Client und dem Server weiter. Cookie-Werte des Clients können also den Server transparent erreichen, und der Server kann Cookies auf dem Client setzen. Der Einsatz von

Cookies ist notwendig, wenn die vom Server gesendeten Dateien aus ASP-Skripten stammen, da ASP die Session-ID in einem Cookie hinterlegt.

- Das Gerät wird den `User-Agent`-Wert des Clients unverändert weiterleiten. Dadurch kann der Server verschiedene Seiten je nach Browser und Betriebssystem ausgeben. PDAs und Mobiltelephone erwarten für kleine Bildschirme optimierte Seiten.
- Das Gerät wird eine `X-Forwarded-For`-Zeile in die HTTP-Anfrage anfügen um die IP-Adresse des Clients zu übermitteln..
- WEBconfig versucht die eigene Sprache anhand der durch `Accept-Languages` gelieferten Sprachpräferenz auszurichten und dann anhand der internen Datenbank auszugeben (momentan nur Englisch und Deutsch). Die gewählte Sprache wird dem Server durch ein weiteres `Accept-Languages`-Tag gemeldet, damit dieser eine Seite in der korrekten Sprache anbieten kann. Beim Übertragen der Seite prüft das Gerät, ob die Seite ein Language-Tag enthält. Wird es nicht gefunden, ersetzt das Gerät die Spracheinstellungen in der Vorlage mit der tatsächlich genutzten Sprache.

URL-Platzhalter (Template-Variablen)

Die URLs in der Seiten-Tabelle brauchen keine konstante Adresse darstellen. Sie haben die Möglichkeit, bestimmte Platzhalter – auch Template-Variablen genannt – in die Adresse zu integrieren, die dann mit den Parametern einer Public Spot-Sitzung gefüllt werden, wenn das Gerät die Seiten vom Server anfordert. Die Platzhalter haben dabei ein ähnliches Format wie in der Programmiersprache C; also ein Prozentzeichen, welchem unmittelbar ein einzelner, kleingeschriebener Buchstabe folgt. Folgende Platzhalter sind definiert:

%a

Fügt die IP-Adresse des Geräts ein. Dieser Platzhalter liefert nur dann einen Wert, wenn der **Request-Typ** in der **Seiten-Tabelle** auf `Template` gesetzt ist.

Hinweis: Bitte beachten Sie, dass dieser Platzhalter keine erreichbare Adresse erzeugt, wenn das Gerät sich hinter einem Router mit aktiviertem NAT befindet.

%c

Fügt die LAN-MAC-Adresse des Public Spot-Gerätes als 12-stelligen Hexadezimal-String ein. Die Ausgabe erfolgt im Format 'aa:bb:cc:dd:ee:ff'.

%d

Geben Sie den URL-Parameter "%d" als Circuit-ID an, z. B. `http://ipaddress/?circuit=%d&nas=%i`. Diese Variable ersetzt das Public Spot Modul mit der Circuit-ID, die im DHCP-Request des Clients erkannt wurde.

Dafür ist es erforderlich, dass auf dem AP "DHCP Snooping" so konfiguriert ist, dass der AP die Circuit-ID in der Public Spot-Stationstabelle des WLCs abfragen kann.

Somit ist es möglich, die Public Spot-Willkommensseite auf den angemeldeten Clients je nach Standort zu verändern.

%e

Fügt die Seriennummer des Geräts ein.

%i

Fügt die NAS-Port-Id ein. 'NAS' steht in diesem Zusammenhang für 'Network Access Server'. Diese Variable überträgt das Interface des Gerätes, über das sich ein Client anmeldet. Bei einem WLC oder Router ohne WLAN entspräche dies einer physischen Schnittstelle wie z. B. `LAN-1`, bei einem Standalone-Access-Point hingegen der SSID.

%l

Fügt den Hostnamen des Geräts ein.

%m

Fügt die MAC-Adresse des Clients als 12-stelligen Hexadezimal-String ein. Die individuellen Bytes werden durch zwei Doppelpunkte getrennt.

%n

Fügt den Namen des Geräts ein, wie er im Setup-Menü unter **Name** konfiguriert ist.

%o

Fügt die URL der Internetseite ein, die der Benutzer ursprünglich angefordert hat. Nach erfolgreicher Authentifizierung leitet das Gerät den Benutzer an diese URL weiter.

%p

Fügt die IP-Adresse des Public Spot-Gerätes in dem ARF-Kontext des jeweiligen Clients ein.

Sofern Ihr Gerät also in verschiedenen IP-Netzwerken aktiv ist, können Sie über diese Variable die IP-Adresse angeben, welche das Gerät in dem Netz benutzt, in dem auch der Client anzutreffen ist.

%r

Fügt die IP-Adresse des Clients ein (aus Sicht des Public Spot-Gerätes in dem jeweiligen ARF-Kontext).

%s

Fügt die WLAN SSID des Netzwerks ein, über das sich der Client verbunden hat. Diese Funktion ist besonders dann interessant, wenn sie MultiSSID verwenden, da der Server hierüber die Möglichkeit erhält, in Abhängigkeit von der SSID verschiedene Seiten auszugeben. Sollte der Client über einen anderen Access Point, welcher sich mit dem Gerät über ein Punkt-zu-Punkt-WLAN verbindet, verbunden sein, fügt dieser Platzhalter die SSID des ersten WLANs ein. Wenn der Client über Ethernet verbunden ist, produziert dieser Platzhalter einen leeren Wert.

%t

Fügt das Routing-Tag ein, mit dem die Datenpakete des Clients versehen werden.

%v

Sofern dem anfragenden Client eine individuelle VLAN-ID zugewiesen wurde, überträgt diese Variable die Quell-VLAN-ID.

%0-9

Fügt eine einzelne Zahl im Bereich von 0 bis 9 ein.

%%

Fügt ein einzelnes Prozentzeichen ein.

Um die Variablen für ein Template zu verwenden, ergänzen Sie in der Seiten-Tabelle die angegebene **Seiten-Adresse (URL)** um die betreffemden Parameter. In den nachfolgenden URLs würde `%i` gemäß dem o. g. Beispielwert durch `LAN-1` ersetzt werden:

Beispiel: `http://192.168.1.1/willkommen.php?nas=%i`

Beispiel: `http://192.168.1.1/%i_willkommen.html`

Seitenvorlagen-Tags und Syntax

Nachdem das Gerät die Seite vom Server empfangen hat, führt es einige Transformationen an den Seitenvorlagen durch, bevor es die Seite an den Client weitergibt. Diese Transformationen ersetzen die vordefinierten HTML-Tag-Platzhalter mit Daten der aktuellen Session (z. B. der aktuelle Ressourcenverbrauch in der Status-Seite). Eine vom Server bereitgestellte Seite sollte daher eher als eine Vorlage für eine HTML-Seite betrachtet werden. Die HTML-Syntax wurde deshalb für die Platzhalter gewählt, weil dadurch das Erstellen der Seiten mit Hilfe handelsüblicher HTML-Editoren möglich ist, ohne die Syntax zu verletzen.

Insgesamt sind drei Platzhalter-Tags definiert:

- `<pblink **identifier**>**text**</pblink>`

  Markiert **text** als einen klickbaren Link zu **identifier**, typischerweise um eine andere Seite zu verknüpfen. Bitte beachten Sie, dass `</pblink>` nur ein Alias für `</a>` ist, da eine solch symetrische Definition zu weniger Probleme mit den gängigen HTML-Editoren führt. Das folgende Fragment definiert z. B. einen Link zur Hilfe-Seite:

```
Bitte klicken Sie <pblink helplink>hier</pblink> um weitere Hilfe
aufzurufen.
```

- `<pbelem **identifier**>`

  Fügt den unter **identifier** als Bezeichner angegebenen Wert an diesem Ort ein. Zum Beispiel fügt die folgende Zeile das Zeitguthaben des Benutzers ein:

```
Session wird in <pbelem sesstimeout> Sekunden beendet.
```

- `<pbcond **identifier(s)**>**code**</pbcond>`

  Fügt nur dann **code** in die Seite ein, wenn alle Bezeichner TRUE sind, dass heisst numerische Werte sind nicht Null und Zeichenfolgen sind nicht leer. Bitte beachten Sie, dass sich diese Abhängigkeiten nicht ineinander verschachteln lassen. Vom vorherigen Beispiel ausgehend, zeigt die fol-

gende Zeile nur dann an, wieviel Zeit einem Benutzer noch bleibt, wenn dieser ein Limit hat:

```
<pbcond sesstimeout>Session wird in <pbelem sesstimeout> Sekunden
beendet.</pbcond>
```

Seitenvorlagen-Bezeichner

Für die Gestaltung benutzerdefinierter Template-Seiten stehen Ihnen die nachfolgenden Bezeichner zur Verfügung. Das Gerät unterscheidet dabei nicht zwischen Groß- und Kleinschreibung.

Hinweis: Bitte beachten Sie, dass nicht alle Bezeichner für alle Ausdrücke verfügbar sind. Nicht alle Bezeichner stehen auf allen Seiten zur Verfügung.

ACCOUNTEND

Gültig für: `<pbelem>`

Dieser Bezeichner fügt auf einem Voucher Informationen zur Gültigkeit des Vouchers ein, d. h. ab wann und bis wann der erstellte Zugang gültig ist.

APADDR

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet die IP-Adresse des Public Spots aus Sicht des Clients. Kann für benutzerdefinierte Anmeldeseiten verwendet werden, wenn das `LOGINFORM`-Element nicht benutzt wird.

AUTOPRINT

Gültig für: `<pbelem>`

Dieser Bezeichner fügt ein Java-Skript in die Seite ein mit der Anweisung, den Druck-Dialog zu öffnen, um die angezeigte Seite auszudrucken. Beachten Sie, dass Sie den `pbelem`-Tag in diesem Fall mit einem separaten `script` abschließen **müssen**, also `<pbelem autoprint></script>`.

BANDWIDTHPROFNAME

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet das Bandbreiten-Profil, mit dem der Benutzer verknüpft ist.

Hinweis: Dieser Bezeichner ist ab HiLCOS-Version 9.12 verfügbar. Templates mit diesem Bezeichner sind für HiLCOS-Versionen vor 9.12 nicht geeignet.

COMMENT

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet auf einem Voucher den optionalen Kommentar, sofern Sie im Setup-Wizard dafür einen entsprechenden Text eingetragen haben.

HELPLINK

Gültig für: `<pblink>`

Dieser Bezeichner beinhaltet die URL der Hilfeseite.

LOGINEMAILFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via E-Mail erhaltenenen Zugangsdaten.

LOGINERRORMSG

Gültig für: `<pbelem>`

Dieser Bezeichner liefert die Fehlermeldung des HiLCOS im Falle einer gescheiterten Anmeldung sowie bei Wegfall der WAN-Verbindung. Dieser Bezeichner steht nur auf der allgemeinen Fehlerseite und der Rückfall-Fehlerseite zur Verfügung.

Hinweis: Um die Fehlermeldung des RADIUS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **SERVERMSG**.

LOGINFORM

Gültig für: `<pbelem>`

Dieser Bezeichner beinhaltet für die Anmeldung über Benutzername und Passwort (und ggf. MAC-Adresse) das HTML-Formular zur Authentisierung am Public Spot.

LOGINLINK

Gültig für: <pblink>

Dieser Bezeichner beinhaltet die URL der Anmeldungsseite.

LOGINSMSFORM

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zur Authentisierung am Public Spot mit den via SMS erhaltenenen Zugangsdaten.

LOGOFFLINK

Gültig für: <pblink>

Dieser Bezeichner beinhaltet die URL der Abmeldungsseite.

ORIGLINK

Gültig für: <pbelem> <pblink> <pbcond>

Dieser Bezeichner beinhaltet die URL, die vom Benutzer angefordert wurde, bevor der Authentifizierungsprozess begonnen wurde. Ist diese Adresse nicht bekannt, ist der Bezeichner leer.

PASSWORD

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet auf einem Voucher das Password für den Public Spot-Zugang.

REDIRURL

Gültig für: <pbelem> <pblink> <pbcond>

Dieser Bezeichner hält eine mögliche Umleitungs-URL aus der Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf Fehler- und Startseite verwenden.

REGEMAILFORM

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via E-Mail (Registrierung).

REGSMSFORM

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet für die Anmeldung über Smart-Ticket das HTML-Formular zum Anfordern der Zugangsdaten via SMS (Registrierung).

RXBANDWIDTH

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet die maximale Empfangsbandbreite des Bandbreitenprofils.

Hinweis: Dieser Bezeichner ist ab HiLCOS-Version 9.12 verfügbar. Templates mit diesem Bezeichner sind für HiLCOS-Versionen vor 9.12 nicht geeignet.

RXBYTES

Gültig für: <pbelem>

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen hat.

RXTXBYTES

Gültig für: <pbelem>

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät in dieser Session vom Client empfangen und wieviele Daten es an den Client gesendet hat. Er gibt somit die Summe aus TXBYTES und RXBYTES aus.

SERVERMSG

Gültig für: <pbelem> <pbcond>

Dieser Bezeichner hält die Authentifizierungsantwort des RADIUS-Servers bereit (sofern es diese gab). Lässt sich nur auf der Fehler- und der Startseite verwenden. Im Falle einer gescheiterten Anmeldung enthält dieser Bezeichner die Fehlermeldung des RADIUS-Servers.

Hinweis: Um die Fehlermeldung des HiLCOS-Servers im Falle einer gescheiterten Anmeldung abzurufen, verwenden Sie den Bezeichner **LOGINERRORMSG**.

SESSIONSTATUS

Gültig für: <pbelem>

Dieser Bezeicher gibt eine Text-Repräsentation über das aktuelle Verhältnis des Clients zum Gerät aus (ob authentifiziert oder nicht).

SESSIONTIME

Gültig für: <pbelem>

Dieser Bezeichner gibt die Zeit in Sekunden an, die seit der Anmeldung am Public Spot verstrichen ist.

SESSTIMEOUT

Gültig für: <pbelem> <pbcond>

Dieser Bezeichner gibt die noch verbleibende Zeit der aktuellen Sitzung an. Nach Ablauf dieser Zeit beendet das Gerät die aktuelle Sitzung automatisch. Für eine Sitzung ohne Zeitlimit ist dieser Bezeichner gleich Null.

SSID

Gültig für: <pbelem> <pbcond>

Dieser Bezeichner enthält auf einem Voucher die SSID, für die der Public Spot-Zugang erstellt wurde.

STATUSLINK

Gültig für: <pbelem> <pblink>

Dieser Bezeichner beinhaltet die URL der Abmeldeseite. Innerhalb des <pblink>-Elements wird automatisch eine Referenz generiert, die ein neues Browser-Fenster öffnet.

TXBANDWIDTH

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet die maximale Sendebandbreite des Bandbreitenprofils.

Hinweis: Dieser Bezeichner ist ab HiLCOS-Version 9.12 verfügbar. Templates mit diesem Bezeichner sind für HiLCOS-Versionen vor 9.12 nicht geeignet.

TXBYTES

Gültig für: <pbelem>

Dieser Bezeichner gibt an, wieviele Daten in Bytes das Gerät während der aktuellen Sitzung zum Client gesendet hat.

USER NAME

Gültig für: <pbcond>

Über diesen Bezeichner haben Sie die Möglichkeit, auf der Voucher-Seite konditionalen HTML-Code einzufügen, den das Gerät nur bei bestimmten Benutzern bzw. Administratoren ausgibt. USER gilt dabei als Präfix und **muss** dem Benutzernamen (NAME) mit einem Leerzeichen vorangestellt werden. Um also bei Aufruf der Voucher-Seite eine HTML-Ausgabe speziell für den Benutzer 'root' zu erzeugen, verwenden Sie die folgende Syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

In größeren Public Spot-Szenarien mit zentraler Verwaltung – z. B. auf einem WLAN-Controller – lässt sich diese Abhängigkeit auch zur Standortlokalisierung einsetzen: Dazu erstellen Sie für jeden der betreffenden Access Points einen eigenen Public Spot-Admin und spezifizieren für die einzelnen Administratoren einen konditionalen Voucher-Text.

USERID

Gültig für: <pbelem>

Dieser Bezeichner beinhaltet die User-ID (in Form des Benutzernamens), mit der die aktuelle Sitzung gestartet wurde. Der Bezeichner ist undefiniert, wenn der Client (noch) nicht eingeloggt ist.

VOLLIMIT

Gültig für: <pbelem> <pbcond>

Dieser Bezeichner gibt die verbleibende Datenmenge an, die dem Benutzer noch zur Verfügung steht, bevor das Gerät die aktuelle Sitzung

automatisch beendet. Für eine Sitzung ohne Datenlimit ist dieser Bezeichner gleich Null.

VOUCHERIMG

Gültig für: `<pbelem>`

Dieser Bezeichner fügt das Seitenbanner Bild (in Groß) in die Seite ein.

Grafiken in benutzererstellten Seiten

Beinahe alle Webseiten beinhalten Bilder, die vom Browser des Clients unabhängig von der eigentlichen HTML-Seite heruntergeladen werden. Bei den vorinstallierten Seiten sind auch die dazugehörigen Grafikdateien im Gerät gespeichert. Das Gerät passt dabei automatisch die notwendigen Rechte an, damit auch nicht-authentifizierte Clients problemlos auf die Bilder zugreifen können. Bei benutzerdefinierten Seiten wird jedoch jeder Zugriff auf die referenzierten (geräteexternen) Bilder wie ein normaler Internetzugriff behandelt, und würde Benutzer daher automatisch wieder auf die Willkommens- oder Startseite führen.

Um dieses Verhalten zu verhindern, sollten Sie darauf achten, dass die Server, die die Grafikdateien bereithalten, zu den **Freien Servern** gehören. Freie Server sind Adressen, deren Zugang nicht beschränkt ist; die also auch von nicht-authentifizierten Clients aufrufbar sind und die von der Accounting-Funktion nicht mit dem übrigen Datenverkehr verrechnet werden.

Das Kapitel *Anmeldungsfreie Netze* auf Seite 1464 erhält weitere Informationen, wie Sie einen freien Server konfigurieren. Bitte beachten Sie, dass, wenn eine benutzererstellte Seite als eine Umleitung definiert ist, das Ziel dieser Umleitung ebenfalls zu den Freien Servern gehören sollte.

Template-Vorschau über WEBconfig

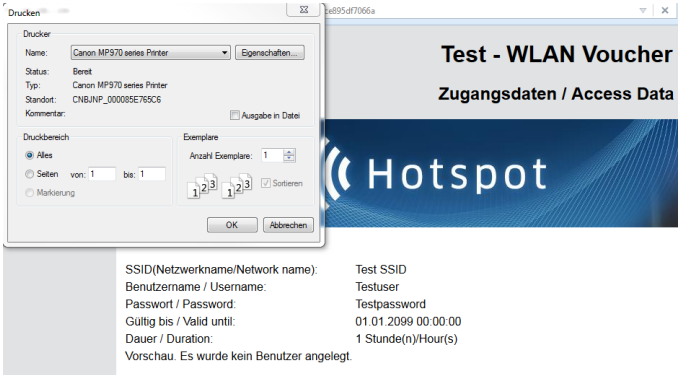
Um Änderungen an den Public Spot-Vorlagen verfolgen zu können, wechseln Sie in WEBconfig zur Ansicht **Extras** > **Public-Spot Template-Vorschau**.

Wählen Sie ein Template zum Anzeigen aus der Liste aus.

Hinweis: Das ausgewählte Template wird im gleichen Browserfenster angezeigt. Über die "Zurück"-Funktion Ihres Browsers gelangen Sie zum WEBconfig zurück.

Einige Templates beinhalten einen Javascript-Code. Dieser Code wird beim Aufrufen des jeweiligen Templates ausgeführt. So enthält das Template "Voucher-Seite" z. B. den Code zum Ausdrucken, sobald die Seite angezeigt wird.

Auf dieser Seite sind Testdaten hinterlegt. Es wird jedoch kein entsprechender Benutzer angelegt. Sie haben also die Möglichkeit, das Template zu testen und auszudrucken.

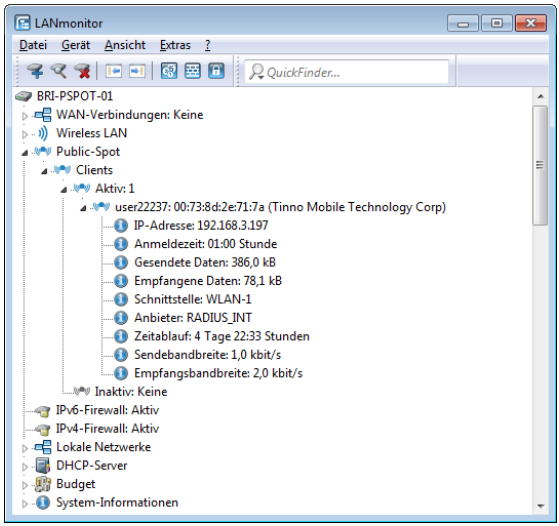


Hinweis: Sofern kein Template vorliegt oder gefunden werden kann, erscheint eine Fehlermeldung im WEBconfig.

14.2.6 Public Spot-Clients anzeigen

Sie haben die Möglichkeit, sich im LANmonitor detaillierte Informationen zu Public Spot-Clients anzeigen zu lassen.

1. Öffnen Sie den Menüzweig **Public-Spot** > **Clients**.
2. Doppelklicken Sie auf **Aktiv**, um aktive Clients anzuzeigen, oder auf **Inaktiv**, um inaktive Clients anzuzeigen.
3. Doppelklicken Sie auf einen Client, um detaillierte Informationen zu diesem abzurufen.



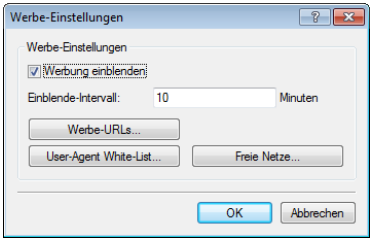
14.2.7 Public Spot-Benutzern Werbung einblenden

Sie haben die Möglichkeit, Public Spot-Benutzern in konfigurierbaren Zeitabständen Werbung einzublenden. Der Public Spot zeigt die Werbung im normalen Browser-Fenster des Benutzers an und nicht über Pop-ups, da alle modernen Browser Pop-ups in der Regel blocken. In der Public Spot-Stationstabelle gibt es somit drei Zustände für einen Client:

- Authentifiziert: Der Client ist angemeldet und darf surfen.
- Unauthentifiziert: Der Client ist nicht angemeldet und darf nicht surfen.
- Werbung: Der Client wird beim nächsten Aufruf einer URL auf eine Werbeseite umgeleitet.

Dabei haben Sie die Möglichkeit, über eine Whitelist bestimmte Netze und User-Agents von den Werbe-Einblendungen auszunehmen.

1. Wählen Sie in der Geräte-Konfiguration den Menüzweig **Public-Spot** > **Server** aus und klicken Sie dort auf **Werbe-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Werbung einblenden**.



   Sie haben jetzt die Möglichkeit, den Einblende-Intervall zu verändern und weitere Einstellungen vorzunehmen.
3. Geben Sie unter **Einblende-Intervall** ein Intervall in Minuten, nach dem der Public Spot einen Benutzer auf eine Werbe-URL umleitet. Bei einem Intervall von `0` erfolgt die Umleitung direkt nach der Anmeldung.
4. Klicken Sie auf **Werbe-URLs**, um eine Werbe-URL hinzuzufügen. Wenn Sie mehrere Werbe-URLs hinzufügen, blendet der Public Spot diese im festgelegten Intervall nacheinander ein.
5. Optional: Klicken Sie auf **User-Agent White-List**, um User-Agents hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt.
6. Optional: Klicken Sie auf **Freie Netze**, um Netze hinzuzufügen, die der Public Spot von Werbe-Einblendungen ausnimmt. Hier besteht beispielsweise die Möglichkeit, die automatischen Such-URLs der Browser eingeben, z. B. `*.google.com`. Normalerweise sendet ein Browser jede Tastatureingabe in der Adressleiste an eine Suchmaschine; durch das Setzen der Ausnahme reagiert die Werbeseite aber nicht auf diesen Zugriff.

   Hinweis: Anmeldungsfreie Netze sind generell werbefrei. Eine explizite Aufnahme derartiger Netze in die Whitelist ist somit nicht erforderlich.

7. Schließen Sie alle Dialoge durch einen Klick auf **OK**.

Public Spot-Benutzer werden nach Ablauf des Einblende-Intervalls auf eine Werbe-URL umgeleitet, sofern ihr User-Agent nicht auf der White-List steht oder sie sich innerhalb eines Freien Netzes bewegen.

Der Zeitpunkt der Werbe-Einblendungen bezieht sich auf die Session-Zeit eines aktiven Public Spot-Clients. Sendet ein Client eine bestimmte Zeit keine Daten, so verschiebt sich auch der Zeitpunkt, zu dem der Public Spot das nächste Mal Werbung einblendet.

14.3 Zugriff auf den Public Spot

14.3.1 Voraussetzungen für die Anmeldung

- Gerät mit Netzwerkadapter
- Betriebssystem mit TCP/IP-Protokoll (automatischer Bezug der IP-Adresse per DHCP ist eingeschaltet)
- Web-Browser (Unterstützung von JavaScript und Frames)
- Direkter Internetzugriff (Proxy-Verwendung ausgeschaltet)
- Notwendige Informationen zum Zugriff auf das WLAN (Netzwerkname, Verschlüsselungs-Informationen)
- Gültige Benutzerdaten (Kennung und Passwort)

Informationen für den WLAN-Zugang

Für den Zugang zum WLAN sind maximal zwei Angaben erforderlich:

- **Netzwerkname des WLAN (SSID)**

  Wenn die Basis-Stationen des Public-Spots für den Betrieb als Closed-Network konfiguriert sind, muss ein Benutzer den exakten Netzwerknamen des WLANs (die SSID) kennen.

- **WLAN-Verschlüsselung**

  Obwohl Gastzugänge auch mit aktivierter WLAN-Verschlüsselung wie z. B. WPA denkbar sind, werden Public-Spots in der Regel ohne WLAN-Verschlüsselung betrieben. Für den Zugriffsschutz sorgt dabei die Benutzeranmeldung mit Username und Passwort. Die Datensicherheit bei der Über-

tragung über den Public Spot muss vom Endanwender selbst bereitgestellt werden (z. B. über einen VPN-Client).

Informationen für den LAN-Zugang

Sofern Sie die IP-Adressen in Ihrem Netzwerk automatisch (z. B. via DHCP) vergeben, benötigen Benutzer lediglich:

- eine Anschlussdose, auf welcher der Public Spot aufgelegt ist.
- ein LAN-Kabel, um Ihren LAN-Adapter mit der Anschlussdose zu verbinden.

Informationen für die Authentifizierung

Folgende Daten müssen dem Benutzer für die Anmeldung vorliegen:

- Benutzerkennung
- Passwort
- MAC-Adresse

  Wenn Sie an den Basis-Stationen des Public-Spots den Authentifizierungs-Modus "MAC+Benutzer+Passwort" gewählt haben, müssen Sie als Betreiber zusätzlich die MAC-Adressen der Endgeräte Ihrer Benutzer kennen. Ein Endgerät übermittelt seine eigene MAC-Adresse automatisch während der gesamten Kommunikation mit dem Public Spot. Der Benutzer muss sie daher nicht bei jeder Anmeldung manuell eingeben, sondern dem Betreiber nur einmal vor der Benutzung mitteilen.

14.3.2 Anmelden am Public Spot

1. Wählen Sie sich in das WLAN des Public-Spots ein (für WLAN-Verbindungen) oder verbinden Sie sich über das Ethernet-Kabel mit dem Netzwerk (für LAN-Verbindungen).
   Die notwendigen Einstellungen für diese Einwahl erfolgen je nach Mobilgerät bzw. WLAN-Adapter auf mehr oder weniger komfortable Art und Weise. Bei vielen Geräten wird der Netzwerkname (SSID) des gewünschten WLANs in einem Konfigurationsprogramm des WLAN-Adapters angegeben. Bei einigen Produkten ist auch die Ansicht aller Access Points in Funkreichweite möglich, aus denen Sie einfach die gewünschte auswählen können.

Die notwendigen Einstellungen für die Verbindung über einen LAN-Adapter erhält ein Nutzer – je nach Konfiguration – automatisch durch das Netzwerk bzw. einen angeschlossenen DHCP-Server oder vom Netzwerk-Administrator.

2. Starten Sie Ihren Web-Browser.

   Sobald der Web-Browser auf eine beliebige Internet-Seite zugreift, schaltet sich automatisch der Public Spot dazwischen und präsentiert seine Anmeldeseite. Je nachdem, welche Firmware-Version Sie verwenden und welchen Anmeldemodus Sie gewählt haben, besitzt die Anmeldeseite bzw. das darin angezeigte Anmeldeformular ein unterschiedliches Erscheinungsbild. Im Nachfolgenden wird die Anmeldung über einen Vouchers (bzw. mittels Benutzername und Passwort) angenommen.

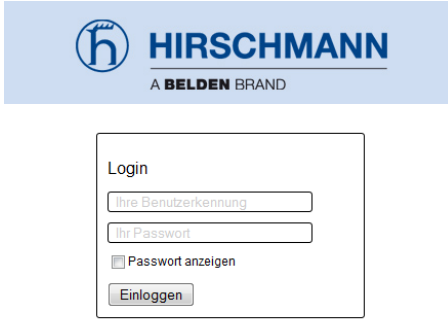


   Abbildung 19: Anmeldeseite für breite Bildschirme

3. Geben Sie die vollständige **Benutzerkennung** und das **Passwort** in die entsprechenden Felder ein und bestätigen Sie Ihre Eingabe mit **Einloggen**.

   Hinweis: Für die Anmeldung sollten Sie einen Web-Browser mit aktivierter JavaScript-Unterstützung verwenden, damit das Popup-Fenster mit den Statusmeldungen über die Sitzung geöffnet werden kann.

   Bei erfolgreicher Anmeldung am Public Spot öffnet sich ein zusätzliches Fenster, das die wichtigsten Informationen der aktuellen Sitzung anzeigt. Auch die Abmeldung erfolgt über dieses Fenster. Daher sollte es während der gesamten Sitzung nach Möglichkeit geöffnet bleiben (z. B. in minimierter Darstellung).

Schlägt die Anmeldung fehl, öffnet sich eine Fehlerseite mit der Aufforderung, zur Anmeldeseite zurückzukehren und die Authentisierung zu wiederholen. Das Eingabeformular übernimmt dabei einen Teil der zuvor eingegebenen Daten, um dem Benutzer z. B. im Falle von Tippfehlern die Eingabe zu erleichtern.

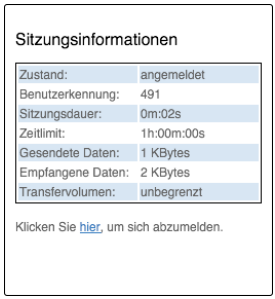
14.3.3 Informationen zur Sitzung

Das Fenster mit den Sitzungsinformationen aktualisiert sich automatisch regelmäßig. Neben Zustand und verwendeter Benutzerkennung sind vor allem die angebotenen Informationen über Verbindungszeit und übertragenes Datenvolumen von Interesse.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie es durch Eingabe folgender Adresszeile im Web-Browser öffnen:

`http://<IP-Adresse des Public Spots>/authen/status`

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen.



14.3.4 Abmelden vom Public Spot

Im Sitzungsinformations-Fenster können Sie sich vom Public Spot abmelden. Klicken Sie dazu auf **hier** in der unteren Textzeile des Fensters.

Falls das Sitzungsinformations-Fenster nicht geöffnet ist, können Sie sich auch durch Eingabe folgender Adresszeile im Web-Browser abmelden:

`http://<IP-Adresse des Public Spots>/authen/logout`

Alternativ können Sie auch über die Kurz-URL `http://logout` die Sitzungsseite öffnen und sich darüber vom Public Spot abmelden.

Hinweis: Der Betreiber kann seinen Public Spot so einstellen, dass dieser einen Benutzer nach 60 Sekunden Unerreichbarkeit automatisch abmeldet. Fragen Sie im Zweifel beim Betreiber des Public-Spots nach, ob er die automatische Abmeldung (*Stationsüberwachung*) aktiviert hat.

14.3.5 Rat und Hilfe

Im folgenden Abschnitt finden Sie Lösungen für die häufigsten Probleme, die bei der Benutzung eines Public Spots auftreten können.

Die Anmeldeseite des Public Spots erscheint nicht

- Der Internet-Zugang muss so eingestellt sein, dass er direkt über den Netzwerkadapter und nicht über eine DFÜ-Einwahlverbindung erfolgt. Prüfen Sie daher die Verbindungseinstellungen in Ihrem Web-Browser. Wenn Sie den Microsoft Internet Explorer verwenden, so müssen unter **Extras** > **Internetoptionen** > **Verbindungen** die eingetragenen DFÜ-Konfigurationen deaktiviert sein.
- Der Internet-Zugang muss direkt erfolgen, also ohne Umweg über einen Proxy-Server. Beim Microsoft Internet Explorer schalten Sie dazu die Verwendung des Proxy-Servers im Menü **Extras** > **Internetoptionen** > **Verbindungen** > **LAN-Einstellungen…** aus.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Ihr Netzwerkadapter den Public Spot überhaupt finden kann. Für die Suche nach einem Access Point bietet Ihr WLAN-Adapter geeignete Hilfsmittel an.
- Sofern Sie die Verbindung über einen WLAN-Adapter herstellen: Prüfen Sie, ob Sie Ihren Netzwerkadapter ausreichend für den Zugang zum Public Spot-Netz konfiguriert haben.
  - Vermutlich müssen Sie den Netzwerknamen des WLAN angeben.
  - Bei Einsatz eines verschlüsselten Public Spots ist zusätzlich auch die Eingabe des passenden WPA- oder WEP-Schlüssels erforderlich.

- Prüfen Sie, ob Ihr Netzwerkadapter auf den automatischen Bezug einer IP-Adresse (DHCP) eingeschaltet ist. Ihm darf keine feste IP-Adresse zugewiesen sein.

Hinweis: Wenn Ihr Netzwerkadapter auf eine feste IP-Adresse konfiguriert ist, dann kann durch die Umstellung auf den automatischen Adressbezug per DHCP der Verlust wichtiger Konfigurationswerte ausgelöst werden. Notieren Sie sich vor der Umstellung alle Werte, die in den Netzwerkeinstellungen aufgeführt sind (IP-Adresse, Standard-Gateway, DNS-Server usw.).

Die Anmeldung funktioniert nicht

- Achten Sie auf die vollständige und richtige Eingabe der Benutzerdaten. Bei allen Eingaben ist auf korrekte Groß- und Kleinschreibung zu achten.
- Ist die Feststelltaste (CAPS-LOCK) an Ihrem Gerät aktiviert? Dadurch wird die Groß- und Kleinschreibung vertauscht. Deaktivieren Sie die Feststelltaste und wiederholen Sie die Eingabe Ihrer Anmeldedaten.
- Möglicherweise überprüft der Betreiber des Public Spots nicht nur Benutzername und Kennung, sondern auch die sogenannte MAC-Adresse (physikalische Adresse) Ihres Netzwerkadapters. Vergewissern Sie sich in diesem Fall beim Public Spot-Betreiber, dass er Ihre korrekte MAC-Adresse kennt.

Es sind keine weiteren Anmeldeversuche mehr möglich

Wenn der Public Spot nach einer Reihe von erfolglosen Anmeldeversuchen die Kommunikation mit Ihnen abbricht, so deaktivieren Sie für mindestens 60 Sekunden den WLAN-Adapter (oder Ihr komplettes Gerät) bzw. trennen den LAN-Adapter vom Netz, und versuchen Sie es danach erneut.

Das Sitzungsinformations-Fenster wird nicht angezeigt

Zur Anzeige des Sitzungsinformations-Fensters geben Sie in der Adresszeile Ihres Web-Browsers folgende Zeile ein:

`http://<IP-Adresse des Public Spots>/authen/status`

Der Public Spot-Betreiber gibt Ihnen die `<IP-Adresse des Public Spots>` auf Nachfrage an.

Der Public Spot fordert ohne Grund die Neuanmeldung (WLAN)

Beim Wechsel in den Funkbereich eines anderen Access Points (Roaming) wird die erneute Anmeldung erforderlich. Wenn Sie sich im Überschneidungsbereich zweier Access Points befinden, kann es sogar zu einem regelmäßigen Verbindungswechsel zwischen beiden Access Points kommen. Die Angabe des Roaming Secret ermöglicht die Übergabe einer Public Spot-Sitzung an anderen Access Point ohne Neuanmeldung.

- LANconfig: **Public-Spot** > **Benutzer** > **Roaming Secret**

14.4 Tutorials zur Einrichtung und Verwendung des Public Spots

Die folgenden Tutorials beschreiben beispielhaft, wie Sie das Public Spot-Modul sinnvoll einsetzen können.

14.4.1 Virtualisierung und Gastzugang über WLAN Controller mit VLAN

In vielen Unternehmen ist es erwünscht, den Besuchern für die mitgebrachten Notebooks o. ä. einen Internetzugang über WLAN anzubieten. In einem größeren Netzwerk mit mehreren Access Points kann die Konfiguration der nötigen Einstellungen zentral im WLAN Controller erfolgen.

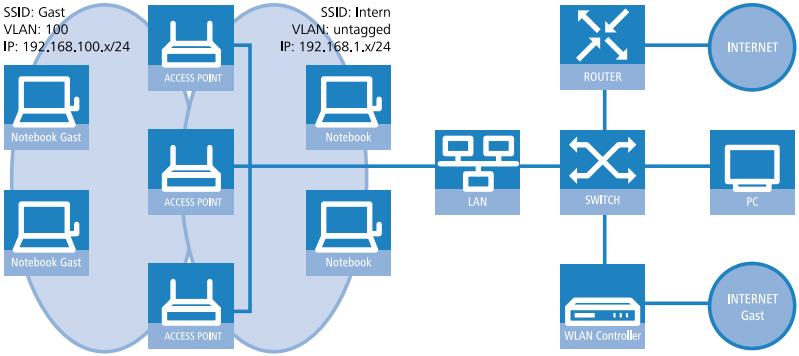
Ziele

- Nutzung der WLAN-Infrastruktur für interne Mitarbeiter und Gäste
- Nutzung der gleichen physikalischen Komponenten (Kabel, Switche, Access Points)
- Trennung der Netzwerke über VLAN und ARF

- Auskopplung der Datenströme zu bestimmten Zielnetzwerken:
  - Gäste: nur Internet
  - Interne Mitarbeiter: Internet sowie alle lokalen Geräte und Dienste
- Gäste melden sich über ein Webformular am WLAN an.
- Interne Mitarbeiter nutzen die WLAN-Verschlüsselung zur Authentifizierung.

Aufbau

- Die Verwaltung der Access Points erfolgt zentral über den WLC.
- Der WLC dient als DHCP-Server für die WLAN-Clients des Gastnetzes.
- Für das Gastnetz wird der Internetzugang vom WLC (z. B. separater DSL Zugang oder Internetzugang über Firmen-DMZ) bereitgestellt.
- Die kabelgebundene Infrastruktur basiert auf gemanagten VLAN-fähigen Switches:
  - Das VLAN-Management der Access Points erfolgt über den WLC.
  - Das VLAN-Management der Switches erfolgt separat über die Switch-Konfiguration.
- Die Access Points werden innerhalb des internen VLANs betrieben.



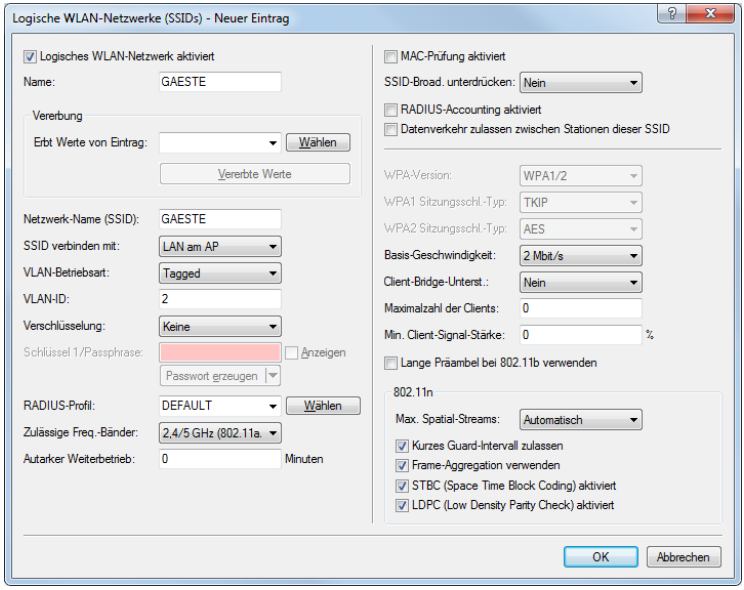
WLAN-Konfiguration des WLAN Controllers

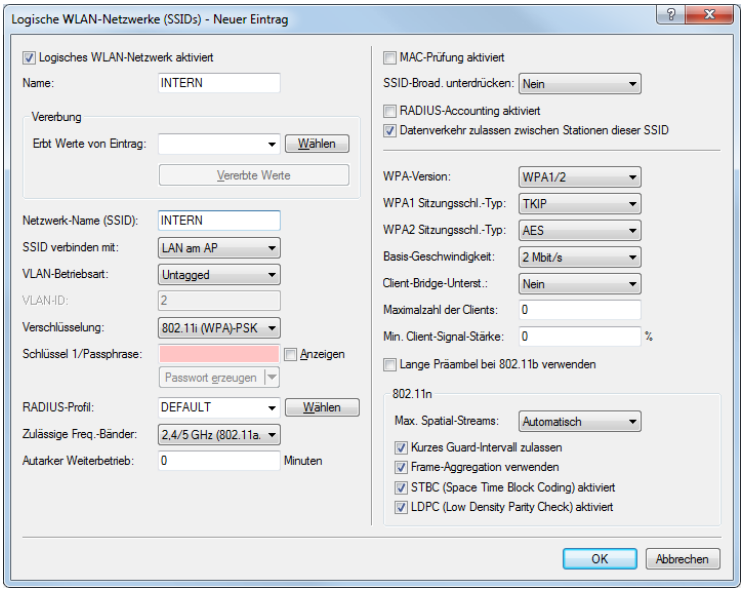
Bei der WLAN-Konfiguration definieren Sie die benötigten WLAN-Netzwerke und weisen sie zusammen mit den physikalischen WLAN-Einstellungen den vom Controller verwalteten Access Points zu.

1. Erstellen Sie ein logisches WLAN für die Gäste und eines für die internen Mitarbeiter.

   - Das WLAN mit der SSID `GAESTE` erhält die VLAN-ID `100` (VLAN-Betriebsart **Tagged**) und verwendet **Keine** Verschlüsselung.
   - Das WLAN mit der SSID `INTERN` erhält keine VLAN-ID (VLAN-Betriebsart **Untagged**, d. h. Datenpakete werden ohne VLAN-Tag in das Ethernet übertragen) und verwendet eine Verschlüsselung nach WPA, z. B. **802.11i (WPA)-PSK**.

   - LANconfig: **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**

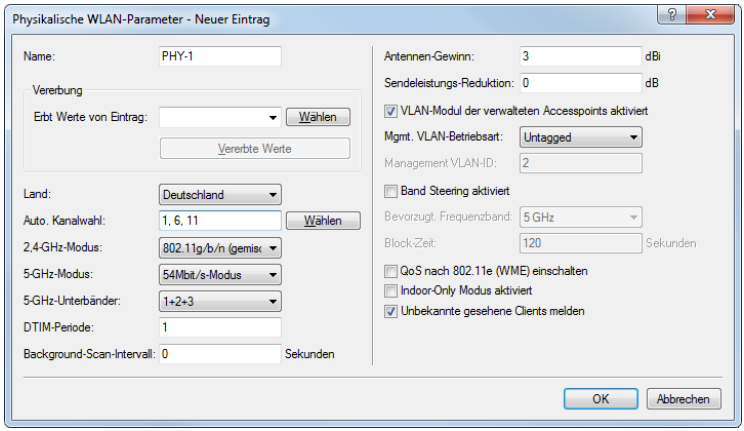




Hinweis: Wenn Sie die **VLAN-Betriebsart** auf **Untagged** stellen, graut LANconfig das Eingabefeld **VLAN-ID** im oben gezeigten Hinzufügen-/Bearbeiten-Dialog aus. Die dazugehörige Tabelle **Logische WLAN-Netzwerke (SSIDs)** zeigt als zugewiesene VLAN aber trotzdem den im ausgegrauten Feld ausgewiesenen Wert an. Dieser Eintrag ist lediglich programmintern, da der zulässige Wertebereich zwischen 2 und 4094 liegt. Letztlich entscheidend ist die VLAN-Betriebsart: Wenn diese auf **Untagged** steht, wird in keinem Fall eine VLAN-ID übertragen.

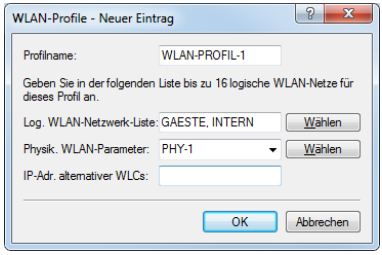
2. Erstellen Sie einen Satz von physikalischen Parametern für die verwendeten Access Points.
   Dabei wird die Management-VLAN-ID auf 1 gesetzt, um die VLAN-Nutzung generell zu aktivieren (jedoch ohne separates Management-VLAN für das Gerät; der Management-Datenverkehr wird ungetagged übertragen).

   ▶ LANconfig: **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**



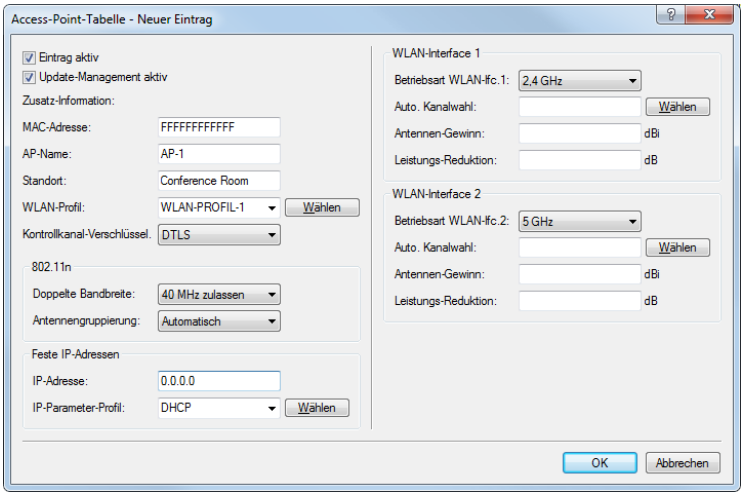
3. Erstellen Sie ein WLAN-Profil, welches Sie den Access Points zuweisen. Unter diesem WLAN-Profil vereinen Sie die beiden zuvor erstellten logischen WLAN-Netzwerke und den zuvor erstellten Satz von physikalischen Parametern.

▶ LANconfig: **WLAN-Controller** > **Profile** > **WLAN-Profile**



4. Ordnen Sie das WLAN-Profil den vom Controller verwalteten Access Points zu.
Tragen Sie dazu die einzelnen Access Points mit der MAC-Adresse in die Access-Point-Tabelle ein. Alternativ können Sie über die Schaltfläche **Default** auch ein Standardprofil anlegen, das für alle Access Points gilt.

▶ LANconfig: **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**

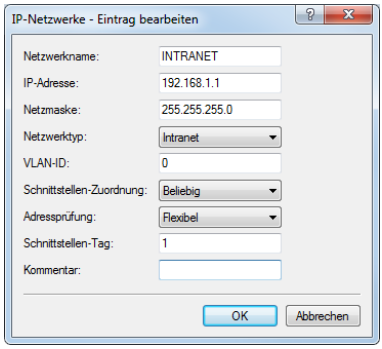


Konfiguration der IP-Netzwerke im WLAN Controller

Für die Trennung der Datenströme auf Layer 3 werden zwei verschiedene IP-Netzwerke verwendet (ARF – Advanced Routing and Forwarding).

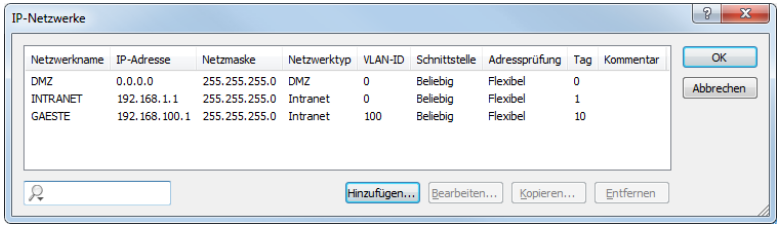
1. Stellen Sie für das interne Netzwerk das **INTRANET** auf die Adresse `192.168.1.1` ein.
   Dieses IP-Netzwerk verwendet die **VLAN-ID** `0`. Damit werden alle ungetaggten Datenpakete diesem Netzwerk zugeordnet (das VLAN-Modul des Controllers selbst muss dazu deaktiviert sein). Das **Schnittstellen-Tag** `1` wird für die spätere Auskopplung der Daten im virtuellen Router verwendet.

   ▶ LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



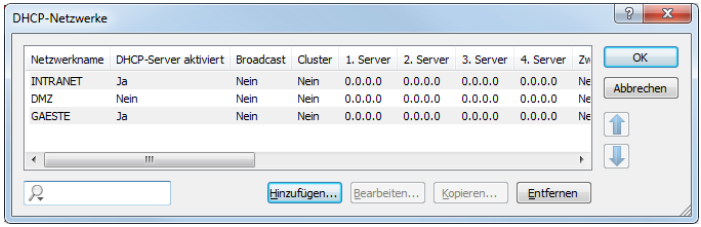
2. Legen Sie für die Gäste ein neues IP-Netzwerk mit der Adresse `192.168.100.1` an.
Dieses Netzwerk verwendet die **VLAN-ID** `100`. Damit werden alle Datenpakete mit dieser ID dem Gäste-Netzwerk zugeordnet. Auch hier dient das **Schnittstellen-Tag** `10` der späteren Verwendung im virtuellen Router.

▶ LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**

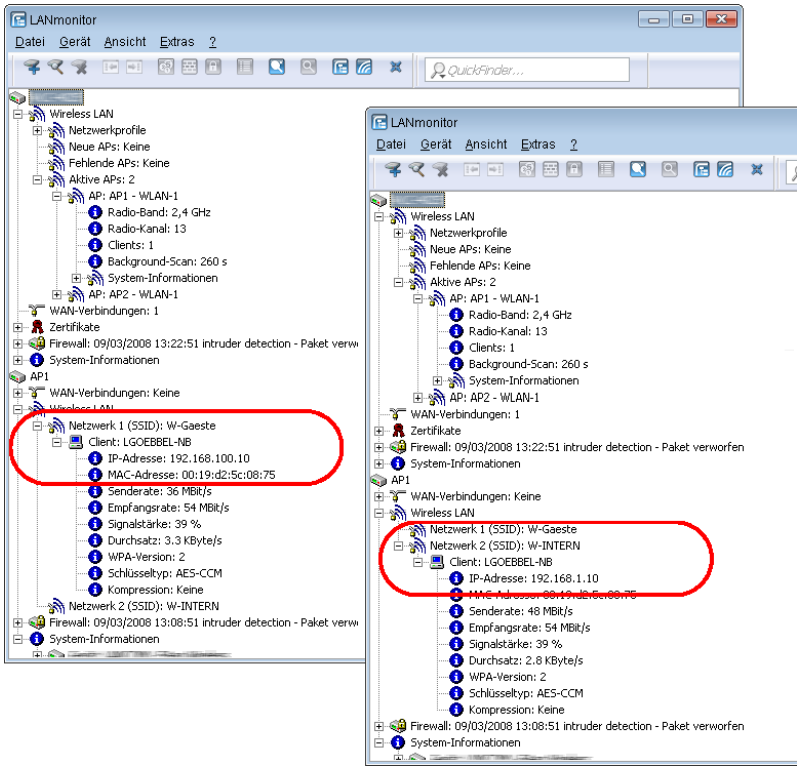


3. Aktivieren Sie für die beiden IP-Netzwerke den DHCP-Server.

▶ LANconfig: **TCP/IP** > **Allgemein** > **IP-Netzwerke**



Mit diesen Einstellungen können die WLAN-Clients der internen Mitarbeiter und der Gäste gezielt den jeweiligen Netzwerken zugeordnet werden.

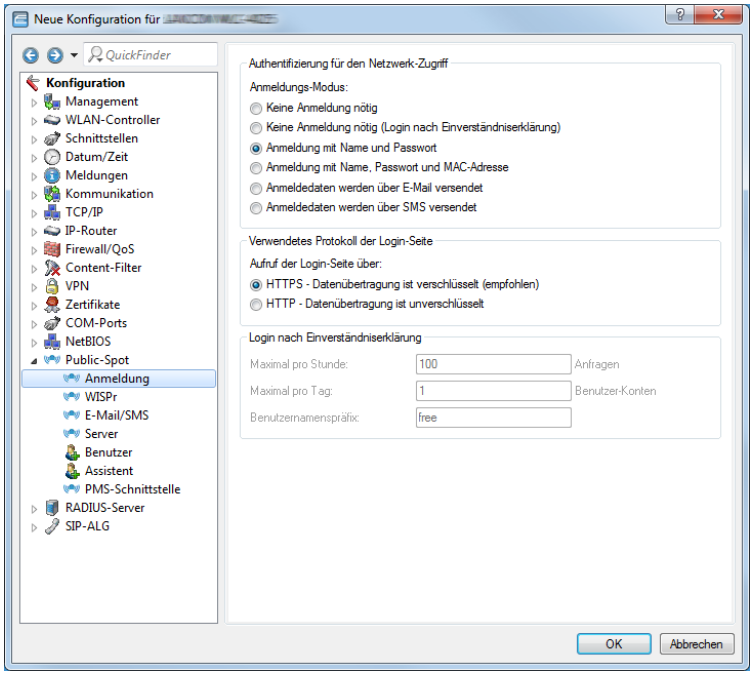


Konfiguration der Public Spot-Zugänge

Mit dem Public Spot bieten Sie einen kontrollierten Zugriffspunkt auf Ihr WLAN. Die Authentifizierung erfolgt durch Benutzerabfrage über ein Webinterface. Bei Bedarf können Sie den Zugang zeitlich begrenzen.

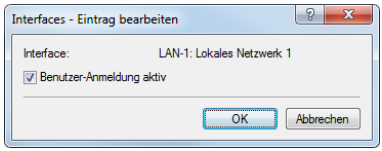
1. Aktivieren Sie die Authentifizierung für den Netzwerk-Zugriff mit Benutzername und Passwort.

   ► LANconfig: **Public-Spot** > **Anmeldung** > **Authentifizierung für den Netzwerk-Zugriff**



2. Aktivieren Sie die Benutzeranmeldung für das Controller-Interface, über das er mit dem Switch verbunden ist.

▶ LANconfig: **Public-Spot** > **Server** > **Interfaces**

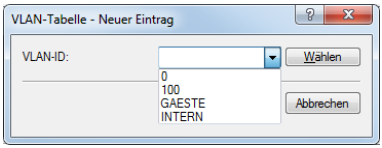


3. Regulieren Sie den Zugang zum Public Spot.

Mit dem Eintrag der VLAN-ID "100" für das Gäste-Netzwerk in der VLAN-Tabelle beschränken Sie die Public Spot-Verwendung auf Datenpakete aus diesem virtuellen LAN. Alle Datenpakete aus anderen VLANs werden ohne Anmeldung am Public Spot weitergeleitet. Achten Sie dabei auch darauf, dass der WEBconfig-Zugang über das Public Spot-Interface auf die Authentifizierungsseiten beschränkt ist (siehe *Konfigurationszugriff einschränken*).

Hinweis: Ohne die Einschränkung des Interfaces auf die VLAN-ID ist der Controller auf dem angegebenen physikalischen Ethernet-Port nicht mehr erreichbar!

- LANconfig: **Public-Spot** > **Server** > **VLAN-Tabelle**



4. Aktivieren Sie die Option zum Bereinigen der Benutzertabelle, damit das Gerät nicht mehr benötigte Einträge automatisch löscht.

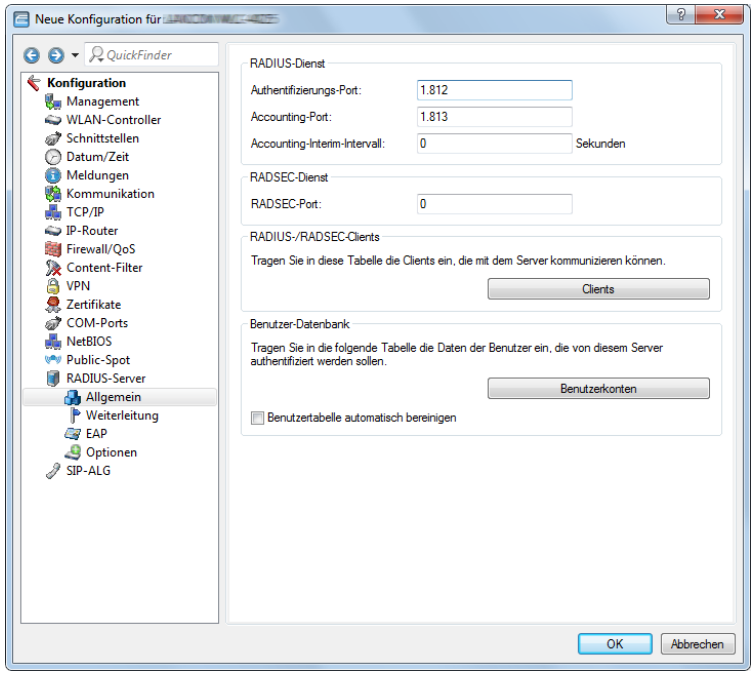
   - LANconfig: **RADIUS-Server** > **Allgemein** > **Benutzertabelle automatisch bereinigen**

Internen RADIUS-Server für Public Spot-Nutzung konfigurieren

Ab der HiLCOS-Version 7.70 speichert der Assistent die Public Spot-Zugänge in der Benutzerdatenbank des internen RADIUS-Servers. Um diese Public Spot-Zugänge nutzen zu können, **müssen** Sie den RADIUS-Server konfigurieren und das Public Spot-Modul auf die Nutzung des RADIUS-Servers einstellen.

1. Aktivieren Sie den RADIUS-Server durch das Eintragen von Authentifizierungs- und Accouting-Port, damit Sie die Benutzer-Datenbank im internen RADIUS-Server nutzen können.
   Verwenden Sie den **Authentifizierungs-Port** `1.812` und den **Accounting-Port** `1.813`.

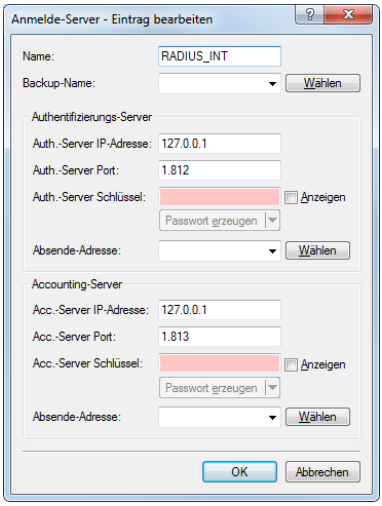
   - LANconfig: **RADIUS-Server** > **Allgemein** > **RADIUS-Dienst**



2. Erstellen Sie in der **Anmelde-Server**-Liste des Public Spots für den internen RADIUS-Server einen Eintrag unter **Name**, damit der Public Spot die Adresse des RADIUS-Servers kennt und er die Public Spot-Zugänge am internen RADIUS-Server des Gerätes authentifizieren kann. Tragen Sie dazu als Authentifizierungs- und Accouting-Server die IP-Adresse des Gerätes ein, in dem der RADIUS-Server aktiviert wurde. Übernehmen Sie außerdem den Authentifizierungs- und Accouting-Port von der Einstellung im RADIUS-Server ("1.812" und "1.813").

   Hinweis: Wenn der Public Spot und der RADIUS-Server vom gleichen Gerät bereitgestellt werden, tragen Sie hier die interne Loopback-Adresse des Geräts (127.0.0.1) ein.

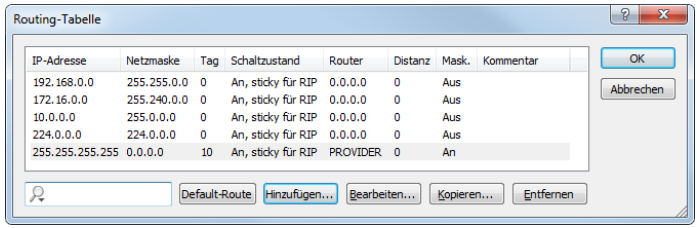
   ▶ LANconfig: **Public-Spot** > **Benutzer** > **Anmelde-Server**



Konfiguration des Internetzugangs für das Gästenetzwerk

1. Um den Benutzern des Gast-Netzes einen Internetzugang bereitzustellen, nutzen Sie z. B. den Assistenten für die Einrichtung eines Zugangs zum Providernetz.
2. Beschränken Sie den Zugang zum Providernetz.
   Damit dieser Zugang nur für die Benutzer im Gästenetzwerk zur Verfügung steht, vergeben Sie der entsprechenden Route das Routing-Tag "10". Damit können nur Datenpakete aus dem IP-Netzwerk "GAESTE" mit dem Schnittstellen-Tag "10" in das Netz des Providers übertragen werden. Das Routing zwischen dem Gäste-Netzwerk und dem internen Netzwerk ist aufgrund der unterschiedlichen Routing-Tags ausgeschlossen.

   ▶ LANconfig: **IP-Router** > **Routing** > **Routing-Tabelle**



3. Optional: Laden Sie im LANconfig ggf. über **Gerät** > **Konfigurations-Verwaltung** > **Zertifikat oder Datei hochladen** eine HTML-Vorlage und ein Bild als Vorlage für die Ausgabe der Vouchers in das Gerät.
   Das Bild kann als GIF, JPEG oder PNG vorliegen und darf maximal 64 KB groß sein.

14.4.2 Virtualisierung und Gastzugang über WLAN Controller ohne VLAN

"Overlay Netzwerk": Netzwerke für Access Points trennen ohne VLAN

Die Trennung von Netzwerken in einer gemeinsam genutzten physikalischen Infrastruktur basiert in vielen Fällen auf dem Einsatz von VLANs. Dieses Verfahren setzt allerdings voraus, dass die eingesetzten Switches VLAN-fähig sind und dass in allen Switches die entsprechenden VLAN-Konfigurationen durchgeführt werden. Der Administrator rollt die VLAN-Konfiguration in diesem Beispiel also über das gesamte Netzwerk aus.

Mit einem WLC können Sie die Netze auch mit minimalem Einsatz von VLANs trennen. Über einen CAPWAP-Datentunnel leiten die APs die Nutzdaten der angeschlossenen WLAN-Clients direkt zum WLC, der die Daten den entsprechenden VLANs zuordnet. Die VLAN-Konfiguration beschränkt sich dabei auf den WLC und einen einzigen zentralen Switch. Alle anderen Switches arbeiten in diesem Beispiel ohne VLAN-Konfiguration.

Hinweis: Mit dieser Konfiguration reduzieren Sie das VLAN auf den Kern der Netzstruktur (in der Grafik blau hinterlegt dargestellt). Darüber hinaus erfordern lediglich 3 der genutzten Switch-Ports eine VLAN-Konfiguration.

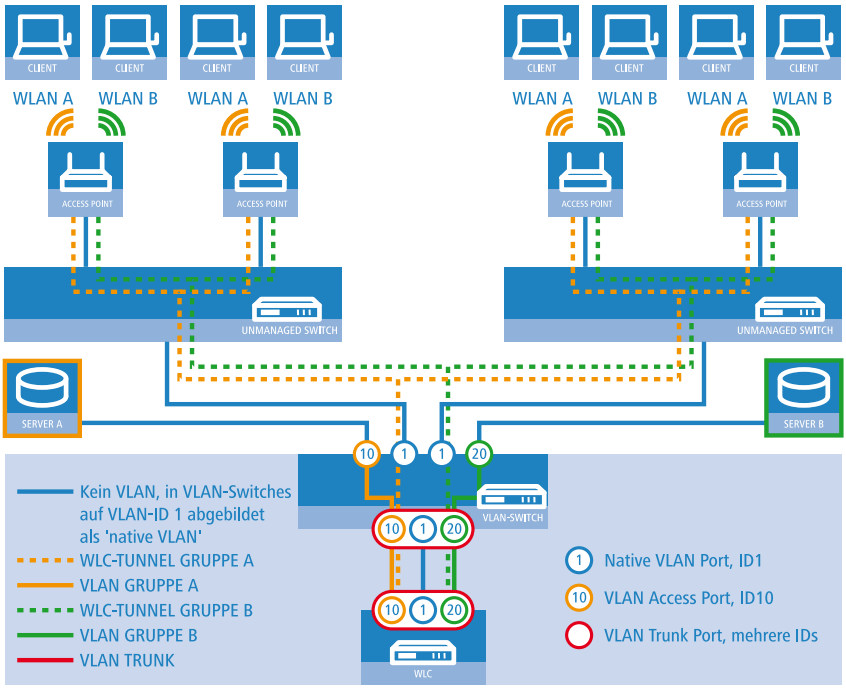


Abbildung 20: Anwendungsbeispiel Overlay-Netz

Die Grafik zeigt ein Anwendungsbeispiel mit den folgenden Komponenten:

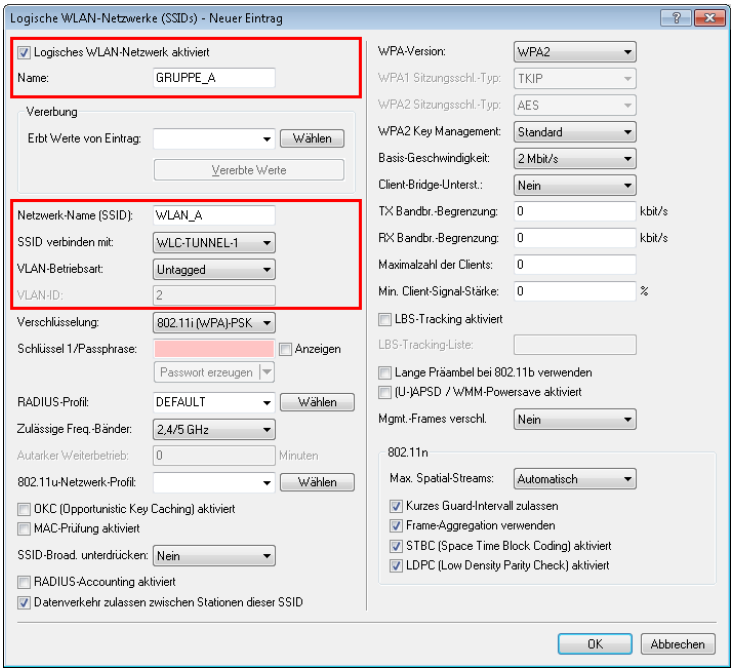
- Das Netz besteht aus zwei Segmenten mit jeweils einem eigenen (nicht unbedingt VLAN-fähigen) Switch.
- In jedem Segment stehen mehrere APs, angeschlossen an den jeweiligen Switch.
- Jeder AP bietet zwei SSIDs für die WLAN-Clients aus verschiedenen Benutzergruppen an, in der Grafik dargestellt in Grün und Orange.
- Jede der Benutzergruppen hat Zugang zu einem eigenen Server, der vor dem Zugriff aus anderen Benutzergruppen getrennt ist. Die Server sind nur durch die auf dem Switch konfigurierten Access-Ports über die entsprechenden VLANs erreichbar.
- Ein WLC verwaltet alle APs in Netz.
- Ein zentraler, VLAN-fähiger Switch verbindet die Switches der Segmente, die gruppenbezogenen Server und den WLC.

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an einer bestimmten SSID anmeldet, soll Zugang zu "seinem" Server haben – unabhängig vom verwendeten AP und unabhängig vom Segment, in dem er sich gerade befindet.

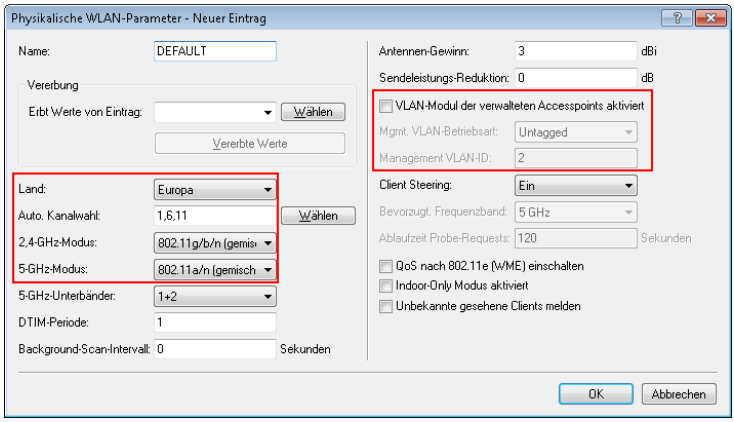
Hinweis: Die folgende Beschreibung basiert auf einer funktionsfähigen Grundkonfiguration des WLCs. Die Konfiguration des VLAN-Switches ist nicht Bestandteil dieser Beschreibung.

Konfiguration der WLAN-Einstellungen

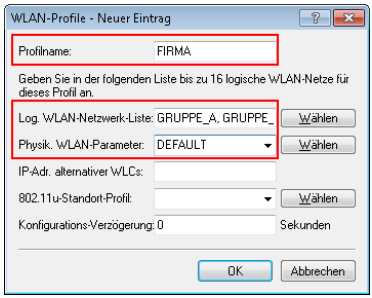
1. Erstellen Sie für jede SSID einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie diese SSID mit einem WLC-Tunnel, die erste SSID z. B. mit 'WLC-TUNNEL-1' und die zweite mit 'WLC-TUNNEL-2'. Stellen Sie die VLAN-Betriebsart jeweils auf 'Tagged' mit der VLAN-ID '10' für das erste logischen Netz und der VLAN-ID '20' für das zweite logischen Netz. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



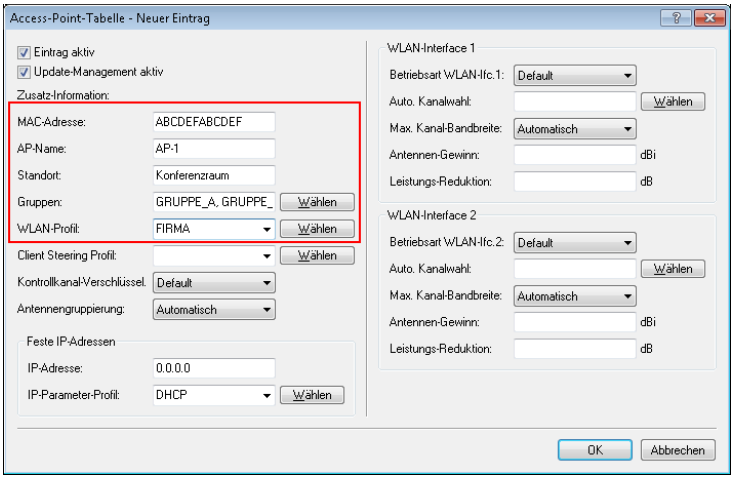
2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten Modus. Aktivieren Sie für dieses Profil der physikalischen WLAN-Parameter die Option, das VLAN-Modul auf den APs einzuschalten. Stellen Sie die Betriebsart für das Management-VLAN in den APs auf 'Ungetagged' ein. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.

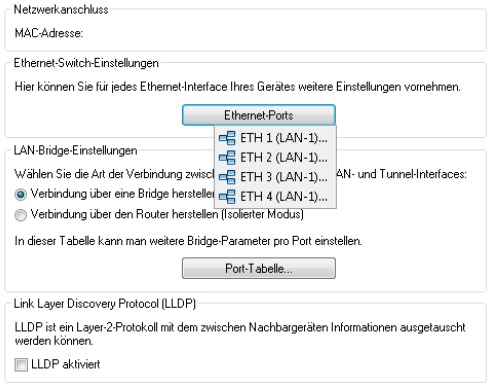


4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig.** > **Access-Point-Tabelle**.

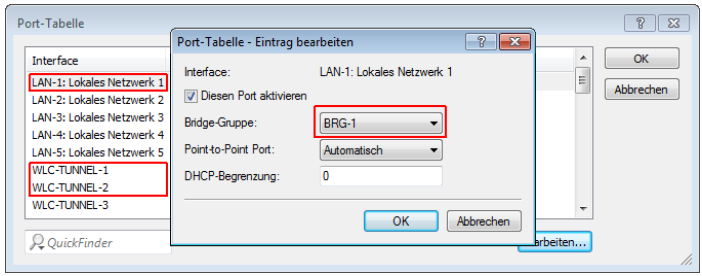


Konfiguration der Schnittstellen am WLC

5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie sicher, dass die anderen Ethernet-Ports nicht der gleichen LAN-Schnittstelle zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.

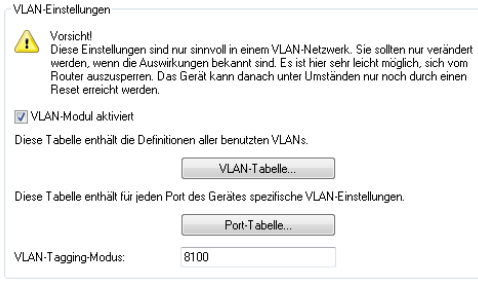


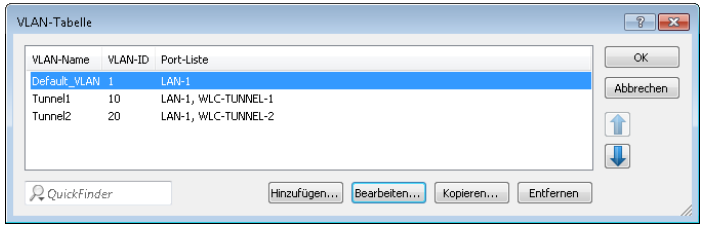
6. Ordnen Sie die logische LAN-Schnittstelle 'LAN-1' und die WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zu. Stellen Sie sicher, dass die anderen LAN-Schnittstellen nicht der gleichen Bridge-Gruppe zugeordnet sind. In LANconfig finden Sie diese Einstellungen unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.



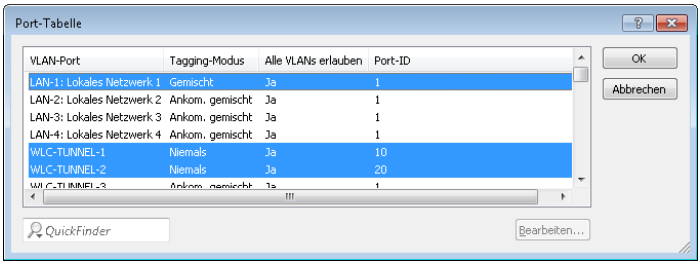
Hinweis: Die LAN-Schnittstellen und WLC-Tunnel gehören standardmäßig keiner Bridge-Gruppe an. Indem Sie die LAN-Schnittstelle 'LAN-1' sowie die beiden WLC-Tunnel 'WLC-Tunnel-1' und 'WLC-Tunnel-2' der Bridge-Gruppe 'BRG-1' zuordnen, leitet das Gerät alle Datenpakete zwischen LAN-1 und den WLC-Tunneln über die Bridge weiter.

7. Aktivieren Sie unter **Schnittstellen** > **VLAN**das VLAN-Modul des WLC und ordnen Sie unter **VLAN-Tabelle** dem gewünschten VLAN den oben gewählten LAN-Port (LAN-1) sowie den passenden WLC-Tunnel zu.





8. Stellen Sie unter **Schnittstellen** > **VLAN** > **Port-Tabelle** den Tagging-Modus der Tunnel-Interfaces sowie des LAN-Interfaces korrekt ein und setzen Sie die passende Port-VLAN-ID.



Je nach Schaltung des Switches konfigurieren Sie den Tagging-Modus des LAN-Interfaces auf 'Gemischt' oder 'Immer'.

Im Normalfall betreibt man die Tunnel-Interfaces im Modus 'Niemals', da Pakete hier (aus dem WLAN) immer ungetaggt ankommen und der WLC sie mit der Port-VLAN-ID versieht.

Wichtig: Bitte beachten Sie, dass bei Aktivierung des VLAN-Moduls die auf dem WLC angelegten ARF-Netze eine VLAN-ID erhalten müssen. Soll der WLC das Netz ohne VLAN-Tag erreichen, setzen Sie bei oben stehender VLAN-Konfiguration die '1' als VLAN-ID für das IP-Netz.

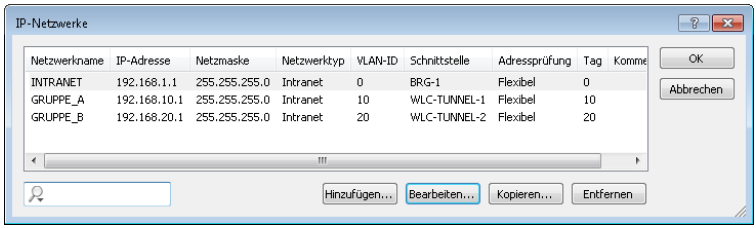
Hinweis:

Eine ähnliche Konfiguration ist möglich, indem Sie schon am Access Point ein VLAN-Tag für die durch den Tunnel zu leitenden Pakete setzen und das VLAN-Modul des WLC nicht nutzen.

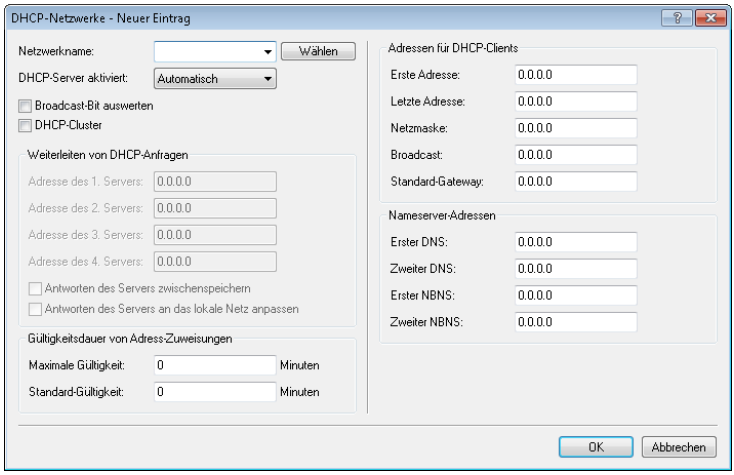
Dabei würde der WLC allerdings durch das Bridgen der verschiedenen WLC-Tunnel untereinander auch Broadcasts in alle Tunnel weiterleiten, was ab einer bestimmten Menge von Tunneln/SSIDs und APs zu Lastproblemen im Netz und auf dem WLC führen kann. Die vorliegende Konfiguration des VLAN-Moduls verhindert das.

9. Ergänzend konfigurieren Sie unter **IPv4** > **Allgemein** > **IP-Netzwerke** für die auf Layer 2 getrennten Netzwerke die IP-Einstellungen.

Wichtig: Damit das Gerät die Netzwerke nicht wieder auf Layer 3 verbindet, ist auch eine Trennung auf Layer 3 erforderlich, z. B. durch ein Schnittstellen-Tag oder durch die Firewall.



10. Der WLC kann optional als DHCP-Server für die APs fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET'. In LANconfig finden Sie diese Einstellungen unter **IPv4** > **DHCPv4** > **DHCP-Netzwerke**.



WLAN-Controller mit Public Spot

Dieses Szenario basiert auf dem ersten Szenrio (Overlay Netzwerk) und erweitert es um spezifische Einstellungen für eine Benutzer-Authentifizierung.

Die Durchleitung der Nutzdaten aus den WLANs über WLC-Tunnel bis zum WLC ermöglicht eine besonders einfache Konfiguration von Public Spots z. B. für Gäste parallel zu einem intern genutzten WLAN.

In diesem Beispiel haben die Mitarbeiter einer Firma Zugang zu einem eigenen WLAN (SSID), die Gäste erhalten über einen Public Spot ebenfalls Zugang zum Internet. Die APs in allen Bereichen des Gebäudes bieten die beiden SSIDs 'FIRMA' und 'GAESTE' an.

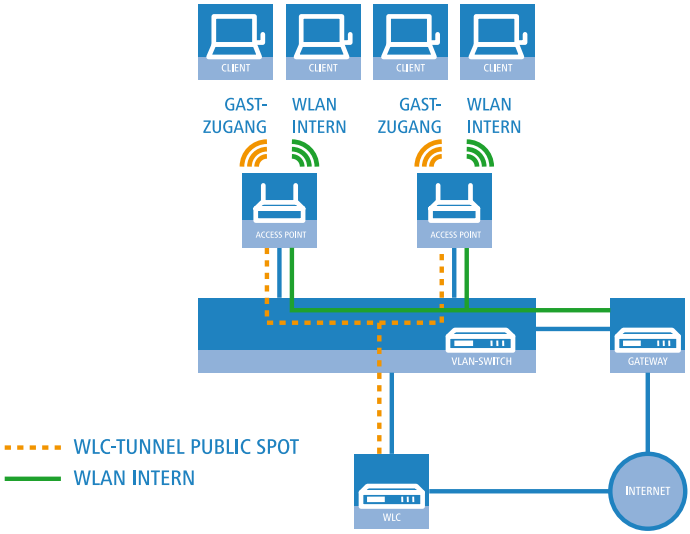
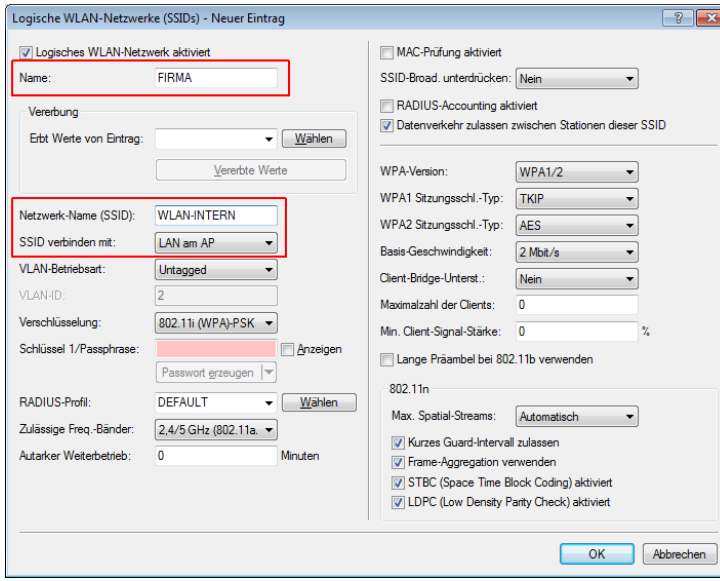
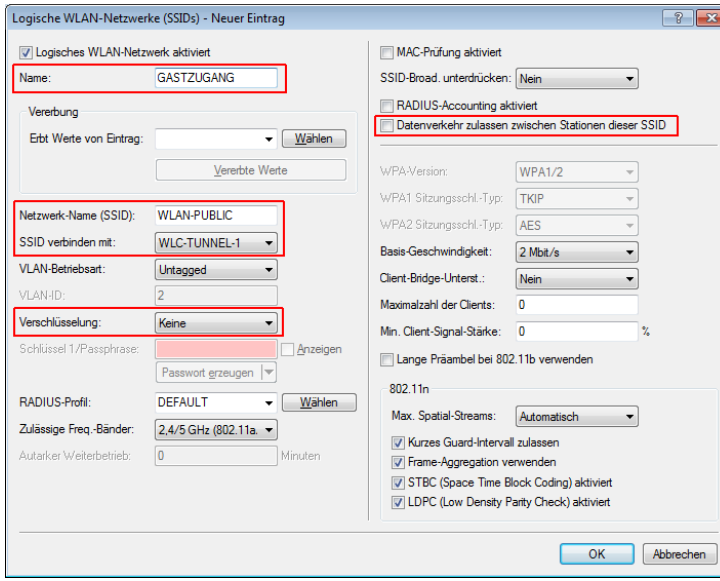


Abbildung 21: Anwendungsbeispiel WLAN-Controller mit Public Spot

Das Ziel der Konfiguration: Ein WLAN-Client, der sich an der internen SSID anmeldet, soll Zugang zu allen internen Ressourcen und zum Internet über das zentrale Gateway erhalten. Die APs koppeln die Nutzdaten der internen Clients lokal aus und leiten sie direkt in das LAN weiter. Die WLAN-Clients der Gäste melden sich am Public Spot an. Die APs leiten die Nutzdaten der Gäste-Clients über einen WLC-Tunnel direkt zum WLC, der über eine separate WAN-Schnittstelle Zugang zum Internet ermöglicht.

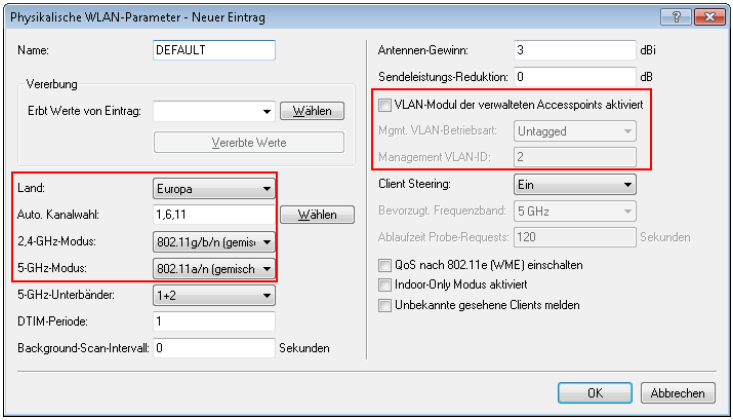
1. Erstellen Sie für das interne WLAN und das Gäste-WLAN jeweils einen Eintrag in der Liste der logischen Netzwerke mit einem passenden Namen und der zugehörigen SSID. Verbinden Sie die SSID für die interne Nutzung mit dem 'LAN am AP', die SSID für die Gäste mit z. B. mit 'WLC-TUNNEL-1'. Deaktivieren Sie bei der SSID für das Gästenetzwerk die Verschlüsselung, damit sich die WLAN-Clients der Gäste beim Public Spot anmelden können. Unterbinden Sie für diese SSID außerdem den Datenverkehr der Stationen untereinander (Interstation-Traffic). In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Logische WLAN-Netzwerke (SSIDs)**.



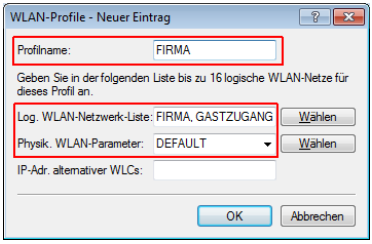


2. Erstellen Sie einen Eintrag in der Liste der physikalischen WLAN-Parameter mit den passenden Einstellungen für Ihre APs, z. B. für das Land 'Europa' mit den Kanälen 1, 6 und 11 im 802.11g/b/n und 802.11a/n gemischten

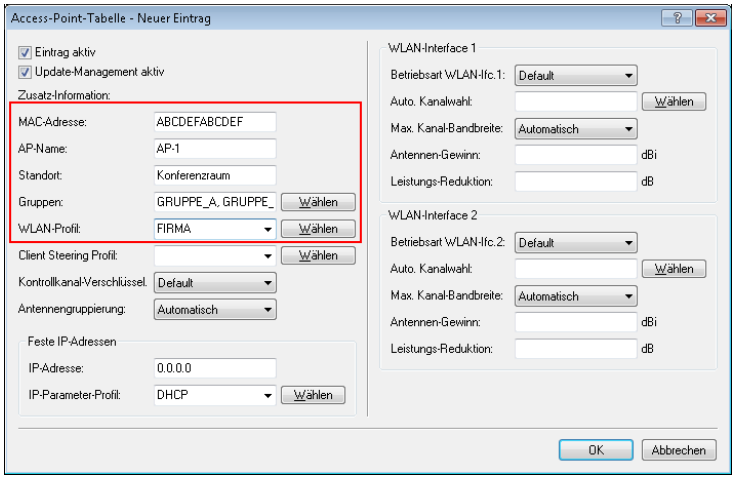
Modus. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **Physikalische WLAN-Parameter**.



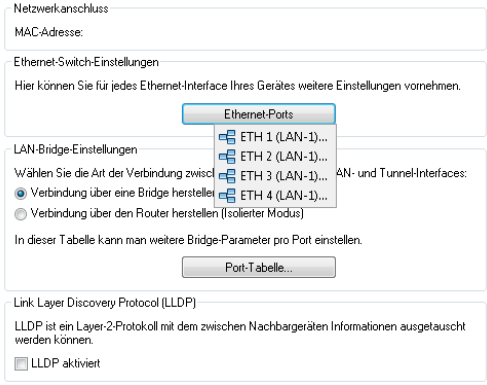
3. Erstellen Sie ein WLAN-Profil mit einem passenden Namen und ordnen Sie diesem WLAN-Profil die zuvor erstellten logischen WLAN-Netzwerke und die physikalischen WLAN-Parameter zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **Profile** > **WLAN-Profile**.



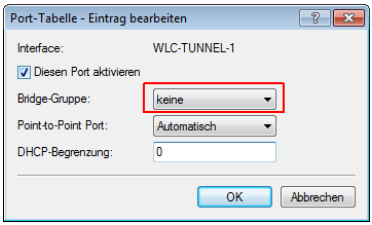
4. Erstellen Sie für jeden verwalteten AP einen Eintrag in der AP-Tabelle mit einem passenden Namen und der zugehörigen MAC-Adresse. Ordnen Sie diesem AP das zuvor erstellte WLAN-Profil zu. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **WLAN-Controller** > **AP-Konfig** > **Access-Point-Tabelle**.



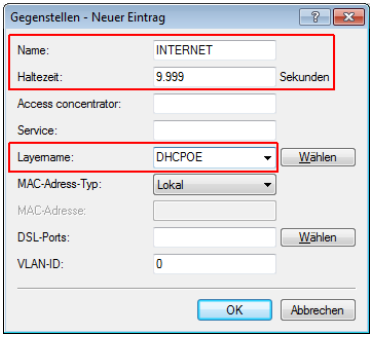
5. Ordnen Sie jedem physikalischen Ethernet-Port eine separate logische LAN-Schnittstelle zu, z. B. 'LAN-1'. Stellen Sie den 4. Ethernet-Port auf die logische LAN-Schnittstelle 'DSL-1' ein. Der WLC verwendet diese LAN-Schnittstelle später für den Internetzugang des Gästenetzes. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Ethernet-Ports**.



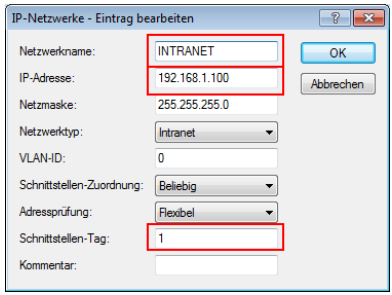
6. Überprüfen Sie, dass die logische LAN-Schnittstelle 'WLC-Tunnel 1' keiner Bridge-Gruppe zugeordnet ist. So stellen Sie sicher, dass die anderen LAN-Schnittstellen keine Daten zum Public Spot-Netzwerk übertragen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Schnittstellen** > **LAN** > **Port-Tabelle**.

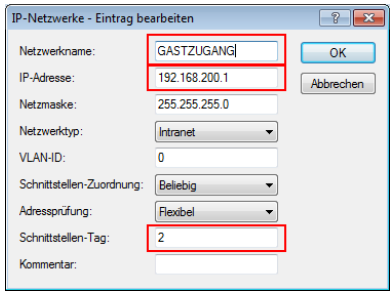


7. Erstellen Sie für den Internetzugang der Gäste einen Eintrag in der Liste der DSL-Gegenstellen mit der Haltezeit '9999' und dem vordefinierten Layer 'DHCPOE'. Dieses Beispiel setzt voraus, dass ein Router mit aktiviertem DHCP-Server den Internetzugang bereitstellt. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Kommunikation** > **Gegenstellen** > **Gegenstellen**.



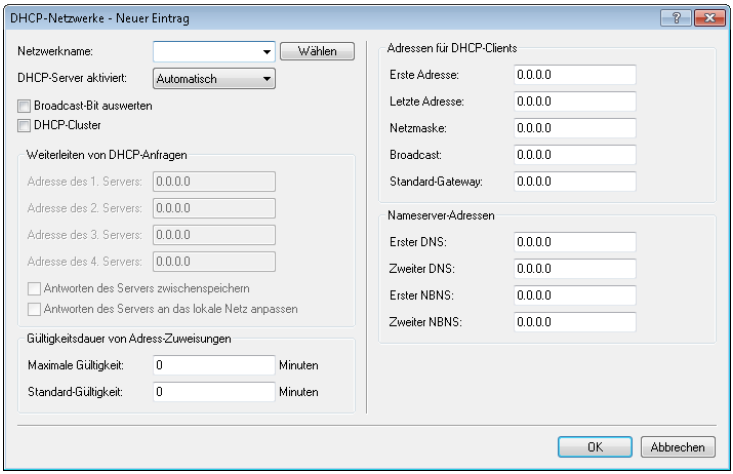
8. Erstellen Sie für die interne Nutzung das IP-Netzwerk 'INTRANET' z. B. mit der IP-Adresse '192.168.1.100' und mit dem Schnittstellen-Tag '1', für die Gäste das IP-Netzwerk 'GASTZUGANG' z. B. mit der IP-Adresse '192.168.200.1' und mit dem Schnittstellen-Tag '2'. Der virtuelle Router im WLC nutzt die Schnittstellen-Tags, um die Routen für die beiden Netzwerke zu trennen. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **Allgemein** > **IP-Netzwerke**.



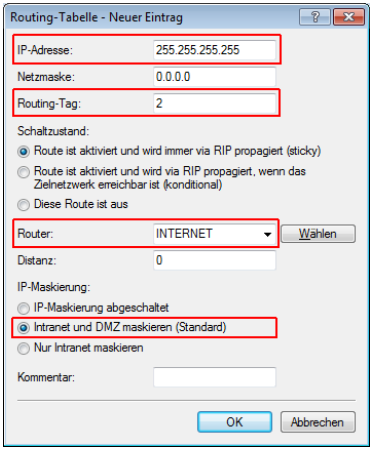


9. Der WLC kann als DHCP-Server für die APs und die angemeldeten WLAN-Clients fungieren. Aktivieren Sie dazu den DHCP-Server für das 'INTRANET' und den 'GASTZUGANG. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **TCP/IP** > **DHCP** > **DHCP-Netzwerke**.

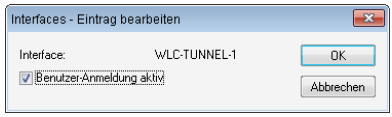
Hinweis: Die Aktivierung des DHCP-Servers ist für das Gästenetz zwingend, für das interne Netz optional. Für das interne Netz können Sie den DHCP Server auch anders realisieren.



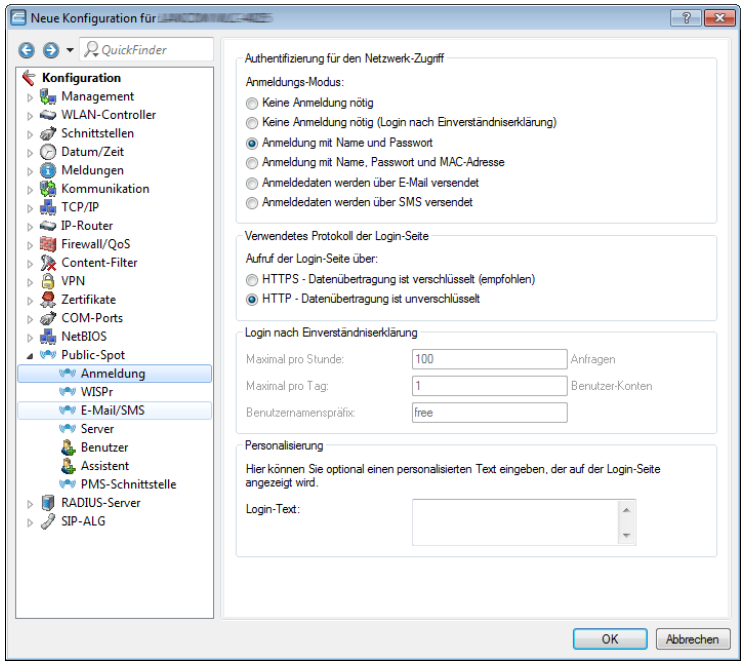
10. Erstellen Sie eine neue Standard-Route in der Routing-Tabelle, welche die Daten aus dem Gästenetzwerk auf den Internet-Zugang des WLCs leitet. Wählen Sie dazu das Routing-Tag '2' und den Router 'Internet'. Aktivieren Sie außerdem die Option 'Intranet und DMZ maskieren (Standard)'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **IP-Router** > **Routing** > **Routing-Tabelle**.



11. Aktivieren Sie die Public Spot-Anmeldung für die logische LAN-Schnittstelle 'WLC-Tunnel 1'. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Server** > **Interfaces**.



12. Aktivieren Sie im letzten Schritt die Anmeldung über den Public-Spot für den WLC. In LANconfig finden Sie diese Einstellung unter **Konfiguration** > **Public-Spot** > **Anmeldung**.



Neben der Konfiguration des WLCs konfigurieren Sie den Public Spot nach Ihren Wünschen entweder für die interne Benutzerliste oder für die Verwendung eines RADIUS-Servers.

14.4.3 Einrichtung eines externen RADIUS-Servers für die Benutzerverwaltung

In manchen Anwendungen sollen die Benutzerdaten nicht im Gerät gespeichert werden, sondern in einem externen, zentralen RADIUS-Server. In diesem Fall muss der Public Spot zur Überprüfung der Benutzerdaten mit diesem externen RADIUS-Server kommunizieren.

Hinweis: Beachten Sie, dass Ihnen bestimmte Funktionen (wie z. B. die Public Spot-Assistenten in WEBconfig) nicht zur Verfügung stehen, wenn Sie einen externen RADIUS-Server zur Benutzerverwaltung einsetzen!

Hinweis: Die folgende Anleitung setzt voraus, dass Ihnen die IP-Adresse eines funktionsfähigen RADIUS-Servers im Netzwerk bekannt ist.

Mit den folgenden Konfigurationsschritten richten Sie einen Public Spot für die Nutzung eines externen RADIUS-Servers ein:

1. Führen Sie die Schritte aus dem Abschnitt *Manuelle Installation* aus.

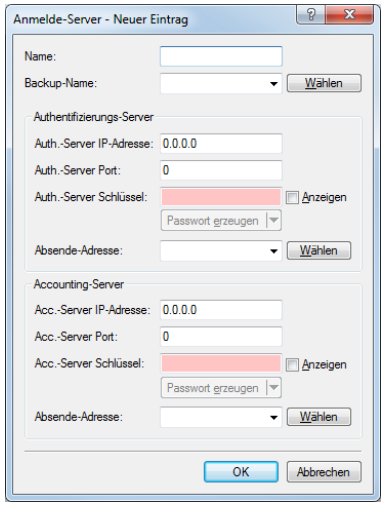
   Die exakte Uhrzeit im Gerät ist hier u. a. für die korrekte Steuerung von zeitlich begrenzten Zugängen notwendig.

   Hinweis: Wenn die Authentifizierung mit zusätzlicher Prüfung der physikalischen Adresse (MAC-Adresse) eingestellt ist, übermittelt der Public Spot bei der Anmeldung eines Benutzers die MAC-Adresse des Endgerätes an den RADIUS-Server. Dabei bleibt dem Public Spot verborgen, ob der Server die MAC-Adresse auch tatsächlich prüft oder nicht. Die korrekte Überprüfung der MAC-Adresse muss durch entsprechende Konfiguration des RADIUS-Servers gewährleistet sein.

2. Tragen Sie die Angaben zum RADIUS-Server ein.

   ▶ LANconfig: **Public-Spot** > **Benutzer** > **Anmelde-Server**

   Bei der Konfiguration eines Public Spots können die Benutzer-Anmeldedaten an einen oder mehrere RADIUS-Server weitergeleitet werden. Diese Server konfigurieren Sie unter **Public-Spot** > **Benutzer** > **Anmelde-Server**. Welche Anmeldedaten die einzelnen RADIUS-Server von den Benutzern benötigen, ist für das den Public Spot bereitstellende Gerät nicht wichtig, da dieses die Daten transparent an den RADIUS-Server weiterreicht.



Hinweis: Die angegebenen IP-Adressen müssen statisch sein. Außerdem muss der Public Spot die angegebenen Ziel-Adressen erreichen können. Für IP-Adressen außerhalb des eigenen Netzwerkes ist es daher erforderlich, einen Router mit Kontakt zum Ziel-Netzwerk als Gateway in den DHCP-Einstellungen des Public Spots einzutragen. Dieses Gateway müssen Sie als Default-Route in die Routing-Tabelle eintragen.

Hinweis: Zur Verbuchung der Verbindungsdaten durch den RADIUS-Server ist es erforderlich, die Angaben zum Accounting-Server vollständig einzutragen. Alternativ zur Verwendung eines RADIUS-Accounting-Servers können Sie sich die Verbindungsinformationen vom Public Spot auch per SYSLOG-Funktion ausgeben lassen.

3. Fertig!

Damit ist Ihr Public Spot betriebsbereit. Alle Benutzer, die über ein gültiges Konto am RADIUS-Server verfügen, können sich über das Web-Interface am Public Spot anmelden.

14.4.4 Interner und externer RADIUS-Server kombiniert

Für die Authentifizierung von Benutzern mit IEEE 802.1x wird in manchen Unternehmen ein externer RADIUS-Server eingesetzt. In einer Anwendung mit einem WLAN Controller und mehreren Access Points fungiert zunächst der WLAN Controller als RADIUS-Server für alle Access Points. Im WLAN Controller definieren Sie dazu die entsprechende Weiterleitung der RADIUS-Anfragen an den externen RADIUS-Server.

Hinweis: Die im folgenden beschriebenen Einstellungen sind nur dann notwendig, wenn Sie in Ihrem Gerät neben dem Public Spot einen externen RADIUS-Server nutzen.

Im Zusammenhang mit einem Public Spot für Gast-Zugänge sind weitere Einstellungen notwendig:

- Die Authentifizierungsanfragen der internen Mitarbeiter sollen an den externen RADIUS-Server weitergeleitet werden.
- Die Authentifizierungsanfragen der Public Spot-Zugänge sollen vom internen RADIUS-Server geprüft werden.

Realm-Tagging für das RADIUS-Forwarding

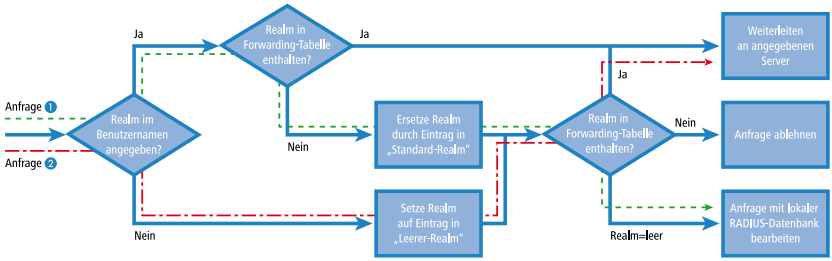
Die Authentifizierungsanfragen der beiden Benutzergruppen müssen separat behandelt werden. Damit der WLAN Controller diese beiden Gruppen unterscheiden kann, nutzt er sogenannte "Realms". Realms dienen der Adressierung von Domänen, innerhalb derer Benutzeraccounts gültig sind. Der WLAN Controller kann die Realms mit der Authentifizierungsanfrage an den internen RADIUS-Server übermitteln. Alternativ kann der RADIUS-Server nach folgenden Regeln die Realms der Benutzernamen verändern, um das RADIUS-Forwarding zu steuern:

- Der als "Standard-Realm" definierte Wert ersetzt einen vorhandenen Realm einer eingehenden Anfrage, wenn für diesen Realm keine Weiterleitung definiert ist.
- Der RADIUS-Server verwendet den unter "Leerer-Realm" definierten Wert **nur dann**, wenn der eingehende Benutzername **noch keinen** Realm enthält.

Über einen Eintrag in der Weiterleitungstabelle leitet der WLAN Controller alle Authentifizierungsanfragen mit einem bestimmten Realm an einen RADIUS-Server weiter. Wenn in der Weiterleitungstabelle kein passender Eintrag vorhanden ist, lehnt er die Anfrage ab.

Hinweis: Stellt der WLAN Controller nach der Ermittlung eines Realms einen leeren Realm fest, so prüft er die Authentifizierungsanfrage **immer** mit der internen RADIUS-Datenbank.

Das folgende Flussdiagramm zeigt schematisch die Arbeitsweise des RADIUS-Server bei der Verarbeitung von Realms:



Durch ein unterschiedliches Realm-Tagging können somit verschiedene RADIUS-Server angesprochen werden. Den Entscheidungsweg im RADIUS-Server des Gerätes können Sie im Diagramm für die beiden Anfragen verfolgen:

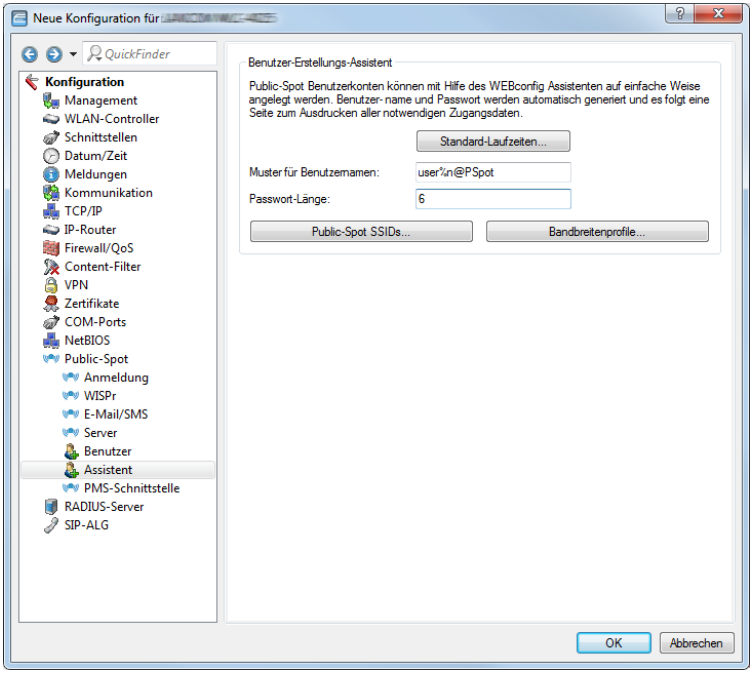
1. Da die Benutzernamen für die Gastzugänge automatisch erzeugt werden, wird für diese Benutzernamen der Realm "PSpot" verwendet. Da in der Weiterleitungstabelle kein entsprechender Eintrag vorhanden ist und der Standard-Realm leer ist, leitet der WLAN Controller alle Authentifizierungsanfragen mit diesem Realm an den internen RADIUS-Server weiter.
2. Um den Konfigurationsaufwand zu begrenzen, werden die internen Benutzer weiterhin ohne Realm geführt. Der RADIUS-Server im Gerät kann einen leeren Realm automatisch durch einen anderen Realm ersetzen, mit dem er die internen Benutzer identifiziert. In diesem Beispiel ersetzt er den leeren Realm durch die Domäne der Firma "firma.de". Mit den Angaben in der Weiterleitungstabelle können alle Authentifizierungsanfragen mit diesem Realm an den externen RADIUS-Server weitergeleitet werden.

Konfiguration für das RADIUS-Forwarding

Mit den folgenden Konfigurationsschritten können Sie die separate Behandlung der internen Benutzer und der Gastzugänge definieren.

1. Passen Sie im Public Spot das Muster für die Benutzernamen so an, dass ein eindeutiger Realm verwendet wird.
   Mit dem Muster "user%n@PSpot" generiert der Public-Spot z. B. Benutzernamen der Form "user12345@PSpot".

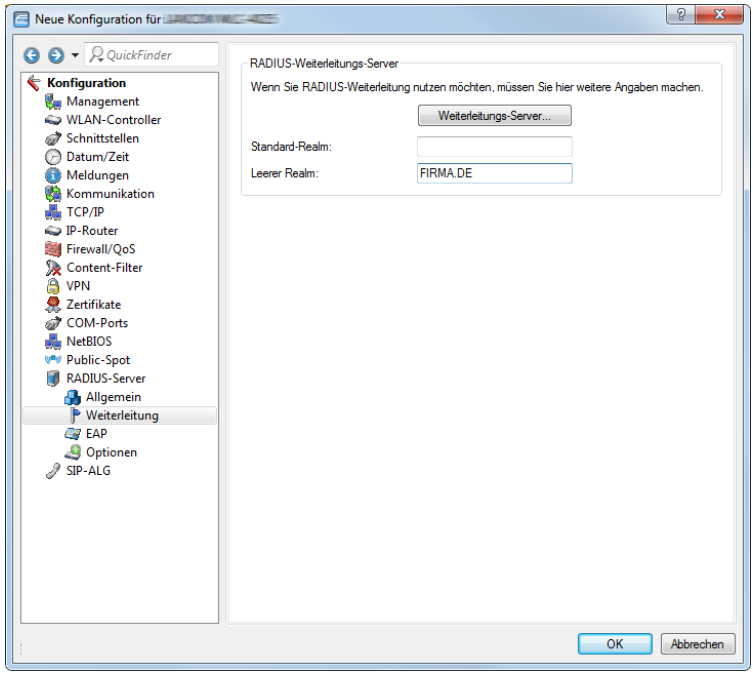
   ▶ **LANconfig: Public-Spot > Assistent > Benutzer-Erstellungs-Assistent**



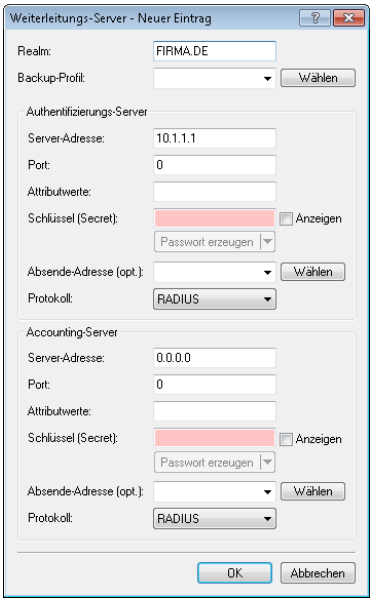
2. Tragen Sie im RADIUS-Server des WLAN Controllers einen "leeren Realm" ein (z. B. "FIRMA.DE").
   Dieser Realm wird für alle Benutzernamen verwendet, die ohne Realm eine Authentifizierungsanfrage bei dem WLAN Controller stellen. Das sind

in dieser Anwendung die internen Benutzer, für die kein Realm definiert ist. Damit der RADIUS-Server des WLAN Controllers für diese Benutzernamen auch keinen Realm einsetzt, müssen Sie den "Standard-Realm" unbedingt leer lassen.

- **LANconfig: RADIUS-Server > Weiterleitung > RADIUS-Weiterleitungs-Server**



3. Damit der WLAN Controller die Authentifizierungsanfragen der internen Benutzer an den externen RADIUS-Server weiterleiten kann, legen Sie einen passenden Eintrag bei den Weiterleitungen an.
   Mit dem Realm "FIRMA.DE" werden alle eingehenden RADIUS-Anfragen an die angegebene IP-Adresse weitergeleitet, die über diesen Realm verfügen.



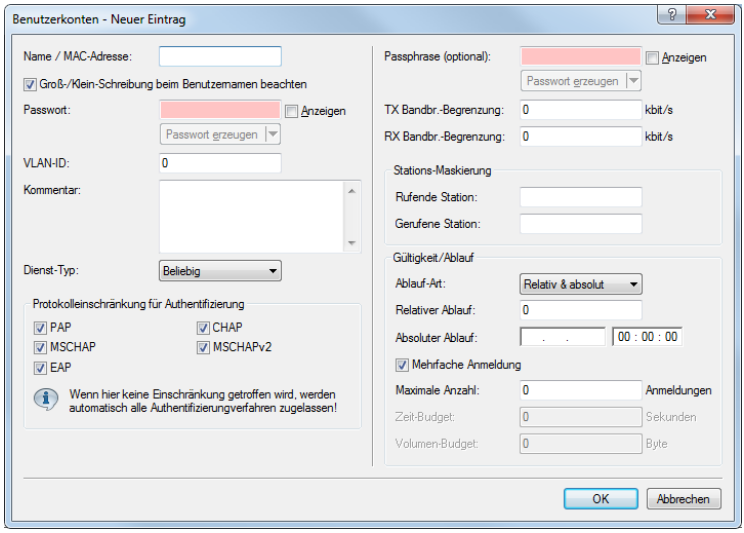
4. Die Authentifizierungsanfragen der Public Spot-Benutzer gehen mit dem Realm "@PSpot" beim WLAN Controller ein. Da für diesen Realm keine Weiterleitung definiert ist, werden die Benutzernamen automatisch in der internen RADIUS-Datenbank geprüft. Da die über den Assistenten angelegten Public Spot-Zugänge in dieser Datenbank gespeichert werden, können diese Anfragen wie gewünscht authentifiziert werden.

14.4.5 Prüfung von WLAN-Clients über RADIUS (MAC-Filter)

Bei der Nutzung von RADIUS zur Authentifizierung von WLAN-Clients können Sie neben einem externen RADIUS-Server auch die interne RADIUS-Benutzerdatenbank eines WLAN Controllers nutzen, um nur bestimmten WLAN-Clients anhand ihrer MAC-Adresse den Zugang zum WLAN zu erlauben.

Tragen Sie die zugelassenen MAC-Adressen über LANconfig in die RADIUS-Datenbank ein und aktivieren Sie alle Authentifizierungsmethoden. Wählen Sie als **Name / MAC-Adresse** und **Passwort** jeweils die MAC-Adresse in der Schreibweise 'AABBCC-DDEEFF'.

▶ LANconfig: **RADIUS-Server** > **Allgemein** > **Benutzerkonten**



14.4.6 Einrichtung eines externen SYSLOG-Servers

Je nach Anwendungsfall, ist für den Betrieb eines Public Spots das Speichern der Nutzungsdaten erforderlich. Diese Daten lassen sich z. B. in einem SYSLOG-Server speichern. SYSLOG-Server sind teilweise als freie Software verfügbar.

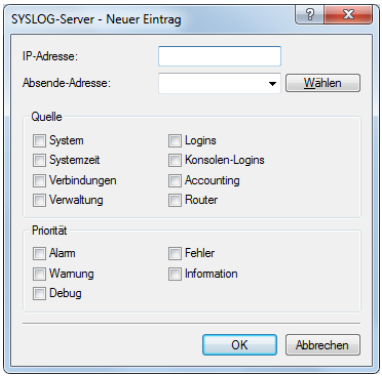
Zum Speichern der Nutzungsdaten aus einem Public Spot über SYSLOG wird der externe SYSLOG-Server in dem jeweiligen Public Spot konfiguriert. Daraufhin wird das Anlegen bzw. Löschen von Public Spot-Benutzern sowie der Anfang und das Ende von Public Spot-Sitzungen mit einer Nachricht an den SYSLOG-Server protokolliert. Beim Ende der Sitzung wird in dieser Nachricht – mit der Quelle "Login" und der Priorität "Information" – neben dem übertragenen Datenvolumen auch die verwendete IP-Adresse gemeldet.

Externen SYSLOG-Server konfigurieren

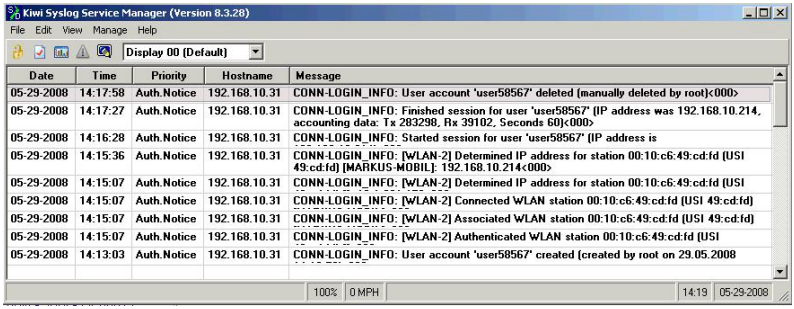
Ihr Gerät ist dazu in der Lage, das Anlegen und Löschen von neuen Public Spot-Benutzern sowie deren An- und Abmeldevorgänge zu protokollieren. Diese intern gespeicherten Informationen können Sie aber auch an einen externen SYSLOG-Server weiterleiten. Die nachfolgenden Schritte zeigen

Ihnen, wie Sie die Protokollierung mit einem auf einem externen SYSLOG-Server installierten Programm vornehmen (in diesem Beispiel "Kiwi").

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Wechseln Sie in den Dialog **Meldungen** > **Allgemein** und öffnen Sie die Tabelle **SYSLOG-Server**.
3. Fügen Sie einen neuen Eintrag hinzu. Definieren Sie dazu die **IP-Adresse** des Rechners, auf der der Syslog-Client installiert ist (z. B. `192.168.10.237`), und geben die **Quelle** (`Logins`, `Accounting`) sowie die **Priorität** (`Information`) an.



4. Schließen Sie die Dialoge und schreiben Sie die Konfiguration zurück auf Ihr Gerät.
5. Starten Sie das Auswertungsprogramm auf Ihrem Syslog Server (z. B. "Kiwi"). Sobald das Programm gestartet ist, zeichnet es das Anlegen und Löschen von neuen Public Spot-Benutzern sowie die An- und Abmeldungen von Public Spot-Benutzers auf.



14.5 Anhang

14.5.1 Allgemein übermittelte RADIUS-Attribute

Das RADIUS-Client-Modul wurde auf Basis der RFCs Nr. 2865 und Nr. 2866 implementiert.

Diese Spezifikationen definieren sogenannte Attribute, die teilweise zwingend implementiert werden müssen, teilweise aber auch optional sind. Die folgenden Übersichtsseiten zeigt, welche Attribute bei welchen Meldungen zwischen RADIUS-Server und Ihrem Gerät übertragen bzw. ausgewertet werden.

Meldungen an den und vom Authentifizierungs-Server

Übertragene Attribute

Wie bereits erwähnt, übermittelt Ihr Gerät in einer RADIUS-Anfrage weit mehr als ausschließlich Benutzername und -kennwort. RADIUS-Server können diese zusätzlichen Informationen komplett ignorieren oder lediglich eine Teilmenge davon verarbeiten. Viele dieser Attribute werden auch für den Serverzugang über Dial-in verwendet und sind in den RADIUS RFCs als Standard-Attribute definiert. Einige für den Hotspot-Betrieb wichtige Informationen lassen sich jedoch nicht mit den Standard-Attributen abbilden. Diese zusätzlichen Attribute werden als herstellerspezifisch mit der Herstellerkennung 2356 (Hirschmann Automation and Control GmbH) verwendet.

ID	*Bezeichnung*	*Bedeutung*	*Mögliche Werte in HiLCOS*
1	User-Name	Der vom Benutzer eingegebene Name.	
2	User-Password	Das vom Benutzer eingegebene Passwort.	
4	NAS-IP-Address	IP-Adresse Ihres Gerätes.	<IPv4-Adresse des Gerätes>
6	Service-Type	Art des Dienstes, den der Benutzer angefragt hat. Der Wert “1” steht dabei für Login.	
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>
30	Called-Station-Id	MAC-Adresse Ihres Gerätes.	<nn:nn:nn:nn:nn:nn>

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
31	Calling-Station-Id	MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen.	<nn:nn:nn:nn:nn:nn>
32	NAS-Identifier	Name Ihres Gerätes, sofern konfiguriert.	<Geräte-Name>
61	NAS-Port-Type	Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.	▶ **Id 19** kennzeichnet Clients aus dem WLAN. ▶ **Id 15** kennzeichnet Clients aus dem Ethernet.
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein. **Hinweis:** Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer verweist also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client.	z. B. ▶ LAN-1 ▶ WLAN-1-5 ▶ WLC-TUNNEL-27

Tabelle 35: Übersicht der vom Gerät an den Authentifizierungs-Server übertragenen RADIUS-Attribute

Ausgewertete Attribute

Ihr Gerät untersucht die Authentifizierungs-Antwort eines RADIUS-Servers auf Attribute, die es eventuell weiterverarbeiten kann. Die meisten Attribute haben allerdings nur dann eine Bedeutung, wenn die Antwort positiv war, sodass sie die anschließende Sitzung beeinflussen.

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
18	Reply-Message	Eine beliebige Zeichenfolge des RADIUS-Servers, die entweder ein gescheitertes Anmelden oder eine Willkommensnachricht beinhaltet. Diese Nachricht lässt sich über das SERVERMSG-Element in eine benutzerdefinierte Start- oder Fehlerseite integrieren.	
25	Class	Ein beliebiges Oktett oder Achtbitzeichen, das die Daten vom Authentifizerungs- / Accounting-Backend	

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
		enthält. Jedes Mal, wenn das Gerät eine RADIUS-Accounting-Anfrage stellt, wird dieses Attribut unverändert gesendet. Innerhalb einer Authentifizierungs-Antwort kann dieses Attribut mehrmals vorkommen, um z. B. eine Zeichenfolge zu übertragen, die länger als 255 Bytes ist. Das Gerät behandelt alle Vorkommen dieses Attributes in Accounting-Anfragen in der Reihenfolge, in der sie in der Authentifizierungs-Antwort aufgetreten sind.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Definiert eine Datenmenge in Bytes, nach der das Gerät die Sitzung automatisch beendet. Dieser Wert ist nützlich, um Volumen-limitierte Benutzerkonten zu erstellen. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Volumen-Limit angenommen. Ein Datenlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber sein Datenvolumen aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	Kann eine beliebige URL enthalten, die als zusätzlicher Link auf der Startseite angeboten wird. Dies kann die Startseite des Benutzers sein oder eine Seite mit zusätzlichen Informationen zum Benutzerkonto.	
26	Vendor 2356, Id 5 LCS-Account-End	Definiert einen absoluten Zeitpunkt (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00), nach dem der Account ungültig wird. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Datumslimit angenommen. Das Gerät startet keine Sitzung, wenn die interne Systemuhr nicht eingestellt ist oder der angegebene Zeitpunkt in der Vergangenheit liegt.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Enthält den Namen eines Public Spot-Benutzers für den Auto-Login. Der Auto-Login bezieht sich dabei auf die Tabelle der MAC-authentifizierten Benutzer, denen der Server automatisch einen Benutzernamen zuweist.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Definiert eine maximale Downstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Definiert eine maximale Upstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Definiert eine kommaseparierte Liste von Werbe-URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Definiert das Intervall in Minuten, nach dem der Public Spot einen Benutzer an eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.	
27	Session-Timeout	Definiert eine optionale Maximal-Dauer für die Sitzung in Sekunden. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Zeitlimit angenommen. Ein Zeitlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber seine verfügbare Zeit aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
28	Idle-Timeout	Definiert einen Zeitraum in Sekunden, nach dem das Gerät die Sitzung beendet, wenn es keine Pakete vom Client mehr empfängt. Dieser Wert überschreibt möglichweise eine unter **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung** lokal definierte Leerlauf-Zeitüberschreitung.	
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	
81	Tunnel-Private-Group-ID	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	
85	Acct-Interim-Interval	Definiert die Zeit zwischen aufeinander folgenden RADIUS-Accounting-Aktualisierungen. Dieser Wert wird nur dann ausgewertet, wenn auf dem RADIUS-Client lokal kein eigenes Accounting-Intervall festgelegt ist, Sie für das Public Spot-Modul also keinen **Update-Zyklus** festgelegt haben.	

Tabelle 36: Übersicht aller unterstützten RADIUS-Attribute

Hinweis: Beachten Sie, dass sich die Attribute für LCS-Account-Ende und Session-Zeitüberschreitung gegenseitig ausschließen und daher beide Attribute nicht in einer Antwort auftreten sollten. Sollten dennoch beide Attribute auftreten, wertet das Gerät das zuletzt auftretende Attribut aus.

Meldungen an/vom Accounting-Server

Übertragene Attribute

Der Satz von RADIUS-Attributen der einem RADIUS-Server in einer Accounting-Anfrage übergeben wird ähnelt einer Authentifizierungs-Anfrage. Dennoch werden einige spezifische Accounting-Attribute hinzugefügt. Die folgenden Attribute sind in allen RADIUS-Accounting-Anfragen vorhanden:

Übersicht der vom Gerät an den Accounting-Server übertragenen RADIUS-Attribute

1

User-Name

Name des Benutzerkontos, dass zur Authentifizierung verwendet wurde.

4

NAS-IP-Address

IP-Adresse Ihres Gerätes.

8

Framed-IP-Address

IP-Adresse, die dem Client zugewiesen wurde.

25

Class

Alle Class-Attribut-Werte, die der RADIUS-Authentifizierungs-Server in seiner Antwort geliefert hat.

30

Called-Station-Id

MAC-Adresse Ihres Gerätes

31

Calling-Station-Id

MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen (nn:nn:nn:nn:nn:nn).

32

NAS-Identifier

Name Ihres Gerätes, sofern konfiguriert.

40

Acct-Status-Type

Anfragetyp, welcher den Start oder den Stop des Accountings, oder ein Interim-Update signalisiert. Weitere Erläuterungen finden Sie im Kapitel *Anfragetypen*.

44

Acct-Session-Id

Eine Zeichenfolge, die den Client eindeutig identifiziert. Sie besteht aus der MAC-Adresse des Netzwerkadapters, dem Zeitpunkt der Anmeldung (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00) und der Sitzungszähler, den Ihr Gerät lokal verwaltet.

61

NAS-Port-Type

Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.

- **Id 19** kennzeichnet Clients aus dem WLAN
- **Id 15** kennzeichnet Clients aus dem Ethernet

87

NAS-Port-Id

Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein, wie z. B. `LAN-1`, `WLAN-1-5` oder `WLC-TUNNEL-27`.

Hinweis: Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client verweist.

Im Falle einer Accounting-Stop-Anfrage oder eines Interim-Updates beinhaltet die Anfrage zusätzlich folgendes Attribute:

42

Acct-Input-Octets

Die Summe aller vom Client empfangenen Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

43

Acct-Output-Octets

Die Summe aller zum Client gesendeten Daten-Bytes in dieser Sitzung, Modulo 2^{32}.

46

Acct-Session-Time

Die Gesamtdauer der Sitzung des Clients in Sekunden.

Hinweis: Wurde die Sitzung wegen einer Leerlauf-Zeitüberschreitung beendet, reduziert sich dieser Wert um die Leerlaufzeit.

47

Acct-Input-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung vom Client empfangen hat.

48

Acct-Output-Packets

Die Anzahl der Datenpakete, die Ihr Gerät während der Sitzung zum Client gesendet hat.

49

Acct-Terminate-Cause

Der Grund für den Abbruch oder das Ende der Accounting-Sitzung. Wird gesendet, wenn das der **Acct-Status-Type** den Wert `Start` oder `Stop` besitzt.

52

Acct-Input-Gigawords

Die oberen 32 Bits der Summe aller vom Client empfangenen Daten-Bytes während dieser Sitzung.

53

Acct-Output-Gigawords

Die oberen 32 Bits der Summe aller zum Client gesendeten Daten-Bytes während dieser Sitzung.

55

Event-Timestamp

Der Zeitpunkt, an dem diese Accounting-Anfrage gestartet wurde (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00). Dieses Attribut ist nur dann vorhanden, wenn die Systemuhr Ihres Gerätes eine gültige Zeit aufweist.

Hinweis: Beachten Sie, dass das RADIUS-Accounting erst nach der erfolgreichen Anmeldung eines Clients mit der Abrechnung beginnt; also die für die Authentifizierung benötigte Zeit nicht aufgezeichnet wird. Über die *Traffic-Limit-Option* können Sie den Datenverkehr während der Authentifizierungsphase einschränken. Die finale Accounting-Stop-Anfrage enthält natürlich ebenso das Termination-Cause-Attribute (49).

Ausgewertete Attribute

Ihr Gerät wertet die Antworten von RADIUS-Accounting-Servern derzeit nicht aus.

14.5.2 Durch WISPr übermittelte RADIUS-Attribute

Wenn Sie WISPr aktivieren und einen externen RADIUS-Server verwenden, übermittelt der Public Spot die Attribute (Access-Request):

- **Location-ID**
- **Location-Name**
- **Logoff-URL**

Bei diesen Attributen handelt es sich um einen Auszug der vorangegangenen Abschnitt konfigurierten Werte. Über sie kann ein Provider oder Roaming-Broker den Ort des Clients zu Abrechnungszwecken identifizieren. Es werden Vendor Specific Attributes (VSA) mit der IANA Private Enterprise Number (PEN) 14122 verwendet.

Von einem externen RADIUS-Server verarbeitet der Public Spot die Attribute (Access-Accept):

- **Redirection-URL**: URL, zu der ein Client nach der Anmeldung weitergeleitet werden soll. Diese Funktion wird nicht von allen Smart-Clients unterstützt.
- **Bandwidth-Max-Up**: Maximale Bandbreite der Upload-Geschwindigkeit, die der Client erhalten soll.
- **Bandwidth-Max-Down**: Maximale Bandbreite der Download-Geschwindigkeit die der Client erhalten soll.
- **Session-Terminate-Time**: Zeitpunkt, zu dem der Client automatisch de-authentifiziert werden soll. Dieses Attribut besitzt nach ISO 8601 das Format `YYYY-MM-DDThh:mm:ssTZD`. Falls TZD nicht angegeben wird, wird der Client nach Ortszeit des Public Spots de-authentifiziert.
- **Session-Terminate-End-Of-Day**: Der Wert dieses Attributs kann entweder 0 oder 1 sein. Er gibt an, ob der Client am Ende des Abrechnungstages vom Public Spot de-authentifiziert werden soll.

Für das Accounting verwendet der Public Spot die Attribute:

- **Location-ID**
- **Location-Name**

14.5.3 Experteneinstellungen zur PMS-Schnittstelle

Zusätzlich zu den Einstellungsmöglichkeiten, die Ihnen LANconfig für die PMS-Schnittstelle bietet, haben Sie die Möglichkeit, über das Setup-Menü eine Reihe weiterer Parameter zu konfigurieren. Diese Parameter umfassen einerseits Werte, die das Gerät zur internen Synchronisation mit Ihrem PMS-System benötigt und normalerweise nicht verändert werden. Andererseits finden Sie im Setup-Menü auch erweiterte Einstellungen, mit denen Sie das Leistungsspektrum der PMS-Schnittstelle weiter ausbauen können, z. B. durch die kostenfreie Nutzung eines Public Spots für Gäste mit VIP-Status bei einem ansonsten kostenpflichtigen Zugang.

Die nachfolgenden Seiten bieten Ihnen eine Übersicht sämtlicher Parameter für die PMS-Schnittstelle, die nicht über LANconfig konfigurierbar sind.

Accounting

In diesem Menü konfigurieren Sie die Übermittlung der Abrechnungsinformationen vom Gerät an Ihr PMS.

SNMP-ID:

2.64.10

Pfad Telnet:

Setup > **PMS-Interface**

Accounting-Tabelle-Reinigungsintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü von abgelaufenen Sitzungen befreit.

SNMP-ID:

2.64.10.3

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

60

Besondere Werte:

0

Der Wert `0` deaktiviert die automatische Bereinigung.

Flashrom-Speicherintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät die gesammelten Accounting-Informationen in seinem internen Flash-ROM sichert.

Wichtig: Beachten Sie, dass ein häufiges Beschreiben dieses Speichers die Lebensdauer Ihres Gerätes reduziert!

SNMP-ID:

2.64.10.2

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:

15

Besondere Werte:

0

Der Wert `0` deaktiviert die Funktion.

Accounting-Tabelle-Updateintervall

Über diesen Eintrag konfigurieren Sie, in welchem Intervall das Gerät seine interne Accounting-Tabelle im Status-Menü aktualisiert.

SNMP-ID:

2.64.10.4

Pfad Telnet:

Setup > **PMS-Interface** > **Accounting**

Mögliche Werte:

0 … 4294967295 Sekunden

Default-Wert:
15

Besondere Werte:

0
Wenn der Wert 0 ist, ist die Aktualisierung deaktiviert und die Status-Tabelle zeigt keine Werte an.

Login-Formular

In diesem Menü nehmen Sie die PMS-spezifischen Einstellungen zur Login-/Portalseite, die Ihren Gäste beim unauthentifizierten Zugriff auf den Hotspot erscheint.

SNMP-ID:
2.64.11

Pfad Telnet:
Setup > **PMS-Interface**

Kostenlos-VIP-Status

In dieser Tabelle verwalten Sie lokal die VIP-Kategorien aus Ihrem PMS.

SNMP-ID:
2.64.11.6

Pfad Telnet:
Setup > **PMS-Interface** > **Login-Formular**

Status

Tragen Sie hier die VIP-Kategorie aus Ihrem PMS ein, deren Mitgliedern Sie einen kostenlosen Internetzugang zur Verfügung stellen wollen.

Haben Sie auf Ihrem PMS-Server z. B. drei mögliche VIP-Stati eingerichtet (VIP1, VIP2, VIP3), wollen allerdings nur den Hotelgästen aus Kategorie VIP2 einen freien Internetzugang anbieten, tragen Sie deren entsprechende Kennung hier ein.

SNMP-ID:

2.64.11.6.1

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular** > **Kostenlos-VIP-Status**

Mögliche Werte:

max. 20 Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Fidelio-kostenlos-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.3

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Keiner

Fidelio-kostenlos-VIP-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich eine VIP – zusätzlich zu ihrem Benutzernamen und ihrer Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenlose Internetnutzung für VIPs anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.5

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Keiner

Fidelio-kostenpflichtig-Sicherheits-Check

Wählen Sie aus, mit welcher weiteren Kennung sich ein Hotelgast – zusätzlich zu seinem Benutzernamen und seiner Zimmernummer – am Public Spot authentisiert, sofern Sie eine kostenpflichtige Internetnutzung anbieten. Wenn Sie `Keiner` wählen, verzichtet das Gerät auf die Abfrage einer weiteren Kennung.

SNMP-ID:

2.64.11.4

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

Keiner
Reservierungsnummer
Ankunftsdatum
Abreisedatum
Vorname
Profilnummer

Default-Wert:

Reservierungsnummer

PMS-Login-Formular

Wählen Sie aus, welche Anmeldemaske die Portalseite für Ihre PMS-Schnittstelle anzeigt.

SNMP-ID:

2.64.11.2

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

kostenlos

Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenlosen Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dennoch dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren, um eine Internetnutzung durch Unbefugte zu erschweren.

kostenpflichtig

Wählen Sie diese Einstellung, wenn Sie Ihren Hotelgästen einen kostenpflichtig Internetzugang anbieten. Ihre Hotelgäste werden auf der Portalseite dazu aufgefordert, sich mit ihrem Benutzernamen, ihrer Zimmernummer und ggf. einer weiteren Kennung am Hotspot zu authentisieren und einen Tarif auszuwählen.

kostenlos-VIP

Wählen Sie diese Einstellung, wenn Sie einen eigentlich kostenpflichtigen Internetzugang für VIPs kostenlos anbieten wollen. Ihre VIPs erhalten dann zwar die Anmeldemaske für den kostenpflichtigen Zugang, es werden ihnen jedoch keine Gebühren in Rechnung gestellt.

Default-Wert:

kostenlos

PublicSpot-Login-Formular

Aktivieren bzw. deaktivieren Sie, ob die Portalseite die Public-Spot-eigenen Anmeldemaske anzeigt. Wenn Sie diese Einstellung deaktivieren, können sich Public-Spot-Nutzer, die eine Kombination aus Benutzername und Passwort als Zugangsdaten verwenden (z. B. fest eingetragene oder über Voucher eingerichtete Nutzer), nicht mehr am Gerät anmelden.

SNMP-ID:

2.64.11.1

Pfad Telnet:

Setup > **PMS-Interface** > **Login-Formular**

Mögliche Werte:

nein
ja

Default-Wert:

nein

Gastname-Case-Sensitiv

Aktivieren oder deaktivieren Sie, ob das Gerät beim Abgleich des beim Login angegebenen Nachnamens mit dem Gastnamen in der PMS-Datenbank auf Groß- und Kleinschreibung achtet. Ist diese Einstellung aktiviert, wird einem Gast der Public-Spot-Zugang verweigert, wenn die Schreibweise seines Namens nicht der dem Hotel mitgeteilten Schreibweise entspricht.

SNMP-ID:

2.64.12

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

nein
ja

Default-Wert:

ja

Trennzeichen

Über diesen Eintrag konfigurieren Sie das Trennzeichen, das Ihr PMS benutzt, um Datensätze an eine API weiterzureichen. Die Micros-Fidelio-Spezifikation z. B. verwendet standardmäßig den senkrechten Trennstrich (|, Hex 7C).

Wichtig: Sie sollten diesen Wert nach Möglichkeit nicht verändern. Ein falsches Trennzeichen führt dazu, dass das Gerät die von Ihrem PMS übermittelten Datensätze nicht mehr lesen kann und die PMS-Schnittstelle nicht funktioniert!

SNMP-ID:

2.64.6

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

max. 1 Zeichen aus

`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

|

Zeichensatz

Wählen Sie den Zeichensatz aus, in dem Ihr PMS die Nachnamen Ihrer Gäste an das Gerät übermittelt.

SNMP-ID:

2.64.7

Pfad Telnet:

Setup > **PMS-Interface**

Mögliche Werte:

CP850
W1252

Default-Wert:

CP850

15 Weitere Dienste

Ein Gerät bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzen mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Zeit-Server

15.1 Automatische IP-Adressverwaltung mit DHCP

15.1.1 Einleitung

DHCP-Server

Für einen reibungslosen Betrieb in einem TCP/IP-Netzwerk benötigen alle Geräte in einem lokalen Netzwerk eindeutige IP-Adressen. Zusätzlich brauchen sie noch die Adressen von DNS- und NBNS-Servern sowie eines Standard-Gateways, über das Datenpakete von lokal nicht erreichbaren Adressen geroutet werden sollen.

Bei einem kleinen Netzwerk ist es durchaus noch denkbar, diese Adressen bei allen Rechnern im Netz manuell einzutragen. Bei einem großen Netz mit vielen Arbeitsplatzrechnern wird das jedoch leicht zu einer unüberschaubaren Aufgabe. In solchen Fällen bietet sich die Verwendung des DHCP (Dynamic Host Configuration Protocol) an. Über dieses Protokoll kann ein DHCP-Server in einem TCP/IP-basierten LAN den einzelnen Stationen die benötigten Adressen dynamisch zuweisen.

Die Geräte verfügen über einen eingebauten DHCP-Server, der die Zuweisung der IP-Adressen im LAN übernehmen kann. Dabei teilt er den Arbeitsplatzrechnern u. a. die folgenden Parameter mit:

- IP-Adresse
- Netzmaske
- Broadcast-Adresse
- Standard-Gateway
- DNS-Server
- NBNS-Server
- Gültigkeitsdauer der zugewiesenen Parameter

Damit der DHCP-Server den Rechnern im Netz IP-Adressen zuweisen kann, muss er zunächst einmal wissen, welche Adressen er für diese Zuweisung verwenden darf. Für die Auswahl der möglichen Adressen gibt es drei verschiedene Optionen:

- Die IP-Adresse kann aus dem eingestellten Adress-Pool genommen werden (Start-Adress-Pool bis End-Adress-Pool). Hier können beliebige im jeweiligen IP-Netzwerk gültige Adressen eingegeben werden.
- Wird stattdessen “0.0.0.0” eingegeben, so ermittelt der DHCP-Server selbstständig die jeweiligen Adressen (Start bzw. Ende) aus den Einstellungen für das IP-Netzwerk (Netzadresse und Netzmaske).
- Wenn in dem Gerät noch keine IP-Netzwerke definiert sind, befindet es sich in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse “172.23.56.254” und den Adress-Pool “172.23.56.x” für die Zuweisung der IP-Adressen im Netz.

Wenn nun ein Rechner im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Server die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

Im einfachsten Fall müssen Sie nur das neue Gerät im Auslieferungszustand in einem Netz ohne andere DHCP-Server anschließen und einschalten. Der DHCP-Server regelt im Zusammenspiel mit LANconfig über einen Assistenten dann alle weiteren Adresszuweisungen im lokalen Netz selbst.

Hinweis: Die DHCP-Einstellungen können für jedes Netzwerk unterschiedlich sein. Im Zusammenhang mit dem Advanced Routing and Forwarding (ARF) können in HiLCOS mehrere IP-Netzwerke definiert werden. Die DHCP-Einstellungen beziehen sich daher – bis auf einige allgemeine Einstellungen – auf ein bestimmtes IP-Netzwerk.

DHCP-Relay

Wenn im lokalen Netz schon ein anderer DHCP-Server vorhanden ist, kann ein Gerät alternativ im DHCP-Client-Modus selbst die benötigten Adress-Informationen von dem anderen DHCP-Server beziehen.

Darüber hinaus kann ein Gerät sowohl als DHCP-Relay-Agent als auch als DHCP-Relay-Server arbeiten.

DHCP-Relay-Agent

Als DHCP-Relay-Agent leitet das Gerät DHCP-Anfragen an einen weiteren DHCP-Server weiter.

DHCP-Relay-Server

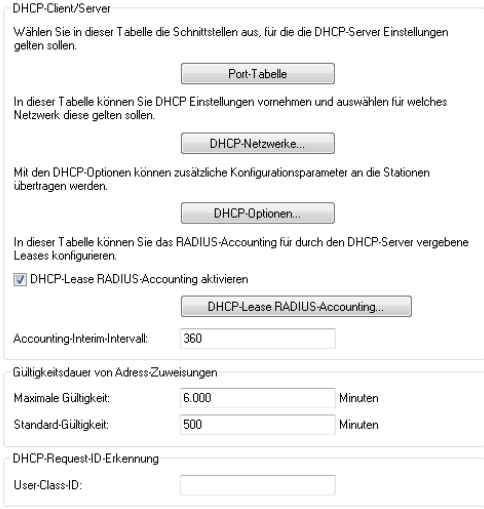
Als DHCP-Relay-Server kann das Gerät von DHCP-Relay-Agents weitergeleitete DHCP-Anfragen bearbeiten.

BOOTP

Über das Bootstrap-Protokoll (BOOTP) können einer Station beim Starten eine bestimmte IP-Adresse und weitere Parameter übermittelt werden. Stationen ohne Festplatten können über BOOTP ein Boot-Image und damit ein komplettes Betriebssystem von einem Bootserver laden (ARF).

15.1.2 Konfiguration der DHCPv4-Parameter mit LANconfig

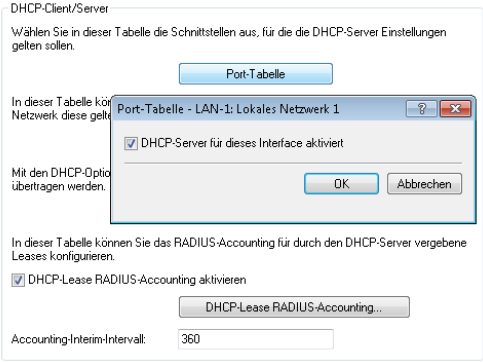
Die DHCPv4-Einstellungen konfigurieren Sie in LANconfig unter **IPv4** > **DHCPv4**.



Hinweis: Informationen zur Konfiguration der DHCPv6-Einstellungen finden Sie im Kapitel *IPv6*.

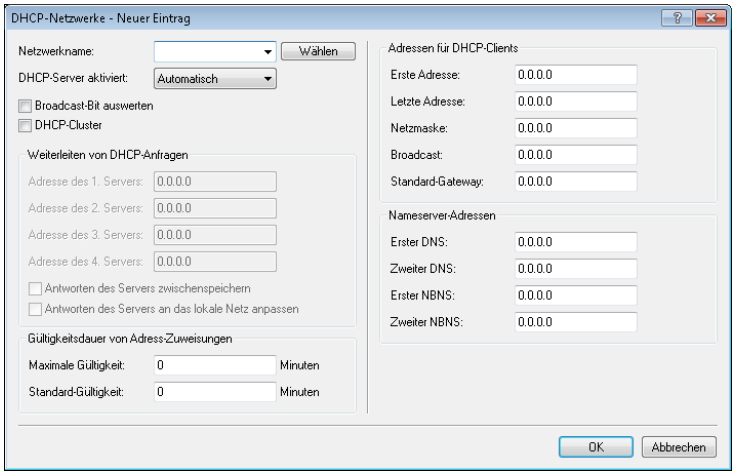
Port-Tabelle

Die Aktivierung bzw. Deaktivierung des DHCP-Servers ist für jedes logische Interface (z. B. LAN-1, WLAN-1, P2P-1-1 etc.) separat möglich. Wählen Sie dazu im Konfigurationsmenü unter **IPv4** > **DHCPv4** > **Port-Tabelle** das entsprechende logische Interface aus und schalten Sie den DHCP-Server für dieses Interface ein oder aus.



DHCP-Netzwerke

Für jedes im Gerät definierte IP-Netzwerk lassen sich die zugehörigen DHCP-Einstellungen separat festlegen. Die Parameter zur Definition der DHCP-Netzwerke finden Sie mit einem Klick auf **DHCP-Netzwerke**.



Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das die Einstellungen gelten sollen.

Die Konfiguration IP-Netzwerke finden Sie in LANconfig im Konfigurationsmenü unter **IPv4** > **Allgemein** > **IP-Netzwerke**.

DHCP-Server aktiviert

Der DHCP-Server kann die folgenden verschiedenen Zustände annehmen:

Ein

Der DHCP-Server ist dauerhaft eingeschaltet. Bei der Eingabe dieses Wertes wird die Konfiguration des Servers (Gültigkeit des Adress-Pools) überprüft.

- Bei einer korrekten Konfiguration bietet das Gerät sich als DHCP-Server im Netz an.
- Bei einer fehlerhaften Konfiguration (z. B. ungültige Pool-Grenzen) wird der DHCP-Server wieder abgeschaltet und wechselt in den Zustand “Aus”.

Hinweis: Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.

Aus

Der DHCP-Server ist dauerhaft abgeschaltet.

Automatisch (Default)

In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LED “LAN-Rx/Tx” am Gerät.

- Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den Router noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Das verhindert u. a., dass ein nicht konfiguriertes Gerät nach dem Einschalten im Netz unerwünscht Adressen vergibt.
- Werden keine anderen DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server ein. Wird zu einem späteren Zeitpunkt ein anderer DHCP-Server im LAN eingeschaltet, wird der DHCP-Server im Router deaktiviert.

Client-Modus

Der DHCP-Server ist ausgeschaltet, das Gerät verhält sich als DHCP-Client und bezieht seine Adress-Informationen von einem anderen DHCP-Server im LAN.

Hinweis: Verwenden Sie diese Einstellung nur dann, wenn sichergestellt ist, dass ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

Anfragen weiterleiten

Der DHCP-Server ist eingeschaltet und das Gerät nimmt die Anfragen der DHCP-Clients im lokalen Netz entgegen. Das Gerät beantwortet diese Anfragen jedoch nicht selbst, sondern leitet sie an einen zentralen DHCP-Server in einem anderen Netzwerkabschnitt weiter.

Der Zustand des DHCP-Servers ist den DHCP-Statistiken zu entnehmen.

Broadcast-Bit auswerten

Wählen Sie hier, ob der DHCP-Server das vom Client gemeldete Broadcast-Bit auswerten soll oder nicht.

Wenn das Bit nicht ausgewertet wird, dann werden alle DHCP-Antworten als Broadcast gesendet.

DHCP-Cluster

Aktivieren bzw. deaktivieren Sie hier den Betrieb eines DHCP-Servers im Cluster.

Aktiviert

Wenn der Cluster-Betrieb aktiviert ist, verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern in Cluster angemeldet haben. Diese Stationen werden in der DHCP-Tabelle mit dem Flag “cache” gekennzeichnet.

Deaktiviert (Default)

Der DHCP-Server verwaltet nur Informationen über die bei ihm selbst angeschlossenen Stationen.

Hinweis: Wenn die Lease-Time der über DHCP zugewiesenen Informationen abläuft, schickt eine Station eine Anfrage zur Erneuerung an den DHCP-Server, von dem sie die Informationen erhalten hat (Renew-Request). Falls der ursprüngliche DHCP-Server auf diesen Request nicht antwortet, versendet die Station eine Anfrage nach einer neuen DHCP-Anbindung (Rebinding Request) als Broadcast an alle erreichbaren DHCP-Server. Renew-Requests werden von den DHCP-Servern im Cluster ignoriert – so wird ein Rebinding erzwungen, damit alle im Cluster vorhandenen DHCP-Server über den Broadcast ihren Eintrag für die Station erneuern können. Auf den Rebind-Request antwortet zunächst nur der DHCP-Server, bei dem die Station ursprünglich registriert war. Wird der Rebind-Request von einer Station wiederholt, dann gehen alle DHCP-Server im Cluster davon aus, das der ursprünglich zuständige DHCP-Server im Cluster nicht mehr aktiv ist und beantworten die Anfrage. Diese Antwort enthält zwar die gleiche IP-Adresse für die Station, kann aber unterschiedliche Gateway- und DNS-Serveradressen enthalten. Die Station sucht sich nun aus den Antworten einen neuen DHCP-Server aus, an den sie von nun an gebunden ist und übernimmt von ihm Gateway und DNS-Server (sowie alle anderen zugewiesenen Parameter).

Weiterleiten von DHCP-Anfragen

Adresse des 1., 2. 3. und 4. Servers

Konfigurieren Sie die IP-Adressen von bis zu vier übergeordneten DHCP-Servern, an die das Gerät DHCP-Anfragen weiterleitet, wenn für das Netzwerk die DHCP-Betriebsart “Anfragen weiterleiten” aktiv ist.

Antworten des Servers zwischenspeichern

Wenn Sie diese Option aktivieren, dann speichert das Gerät die Antworten des übergeordneten DHCP-Servers zwischen, damit es spätere Anfragen direkt beantworten kann.

So vermeiden Sie unnötige Verbindungen, wenn sich der übergeordnete Server in einem entfernten Netz befindet.

Antworten des Servers an das lokale Netz anpassen

Wenn Sie diese Option aktivieren, dann modifiziert das Gerät die Antworten des übergeordneten DHCP-Servers, um sie dem lokalen Netz anzupassen.

Dabei ersetzt es die Werte für “Standard-Gateway”, “DNS-Server” und “NBNS-Server”.

Gültigkeitsdauer von Adress-Zuweisungen

Neben der global konfigurierten Gültigkeitsdauer unter **IPv4** > **DHCPv4** ist hier die Konfiguration einer Gültigkeitsdauer nur für dieses DHCP-Netzwerk möglich.

Maximale Gültigkeit

Geben Sie hier die maximale Gültigkeitsdauer an, die ein Client anfordern darf.

Standard-Gültigkeit

Wenn ein Client IP-Adressdaten anfordert, ohne eine Gültigkeitsdauer für diese Daten zu fordern, erhält er als Gültigkeitsdauer den hier eingestellten Wert vom DHCP-Client zugewiesen.

Adressen für DHCP-Clients

Erste Adresse

Geben Sie hier die erste IP-Adresse des Adressbereiches ein, den Sie den DHCP-Clients zur Verfügung stellen wollen.

Wenn Sie keinen Bereich angeben, verwendet der DHCP-Server automatisch alle freien Adressen in seinem eigenen Netz.

Letzte Adresse

Geben Sie hier die letzte IP-Adresse des Adressbereiches ein, den Sie den DHCP-Clients zur Verfügung stellen wollen.

Netzmaske

Geben Sie hier die zu dem ausgewählten Adressbereich zugehörige Netzmaske ein.

Wenn Sie keine Netzmaske eingeben, wird ermittelt das Gerät die Netzmaske nach Möglichkeit aus der eigenen Adresse und Netzmaske.

Broadcast

In der Regel wird im lokalen Netz für Broadcast-Pakete eine Adresse verwendet, die sich aus den gültigen IP-Adressen und der Netzmaske ergibt. Nur in Sonderfällen (z. B. bei Verwendung von Sub-Netzen für einen Teil der Arbeitsplatzrechner) kann es nötig sein, eine andere Broadcast-Adresse zu verwenden. In diesem Fall tragen Sie die zu verwendende Broadcast-Adresse an dieser Stelle ein.

Achtung: Die Änderung der Voreinstellung für die Broadcast-Adresse ist nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu einem unerwünschten, ggf. kostenpflichtigen Verbindungsaufbau führen.

Standard-Gateway

Das Gerät weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse in diesem Netzwerk als Gateway-Adresse zu. Falls erforderlich, können Sie durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway konfigurieren.

Nameserver-Adressen

Erster/zweiter DNS

Geben Sie hier die Adressen eines Nameservers und eines alternativen Nameservers ein, an die DNS-Anfragen weitergeleitet werden sollen.

Nutzen Sie einen Internetprovider oder eine andere Gegenstelle, die dem Router beim Einloggen automatisch einen Nameserver zuweist, dann können Sie diese Felder leer lassen.

Erster/zweiter NBNS

Geben Sie hier die Adressen eines Netbios-Nameservers und eines alternativen Netbios-Nameservers ein, an die NBNS-Anfragen weitergeleitet werden sollen.

Nutzen Sie einen Internetprovider oder eine andere Gegenstelle, die dem Router beim Einloggen automatisch einen Netbios-Nameserver zuweist, dann können Sie diese Felder leer lassen.

Bei der Konfiguration der DHCP-Netzwerke werden die Adressen definiert, die den DHCP-Clients zugewiesen werden (IP-Adress-Pool). Wenn ein Client im Netz gestartet wird, der mit seinen Netzwerk-Einstellungen über DHCP eine IP-Adresse anfordert, wird ihm ein Gerät mit aktiviertem DHCP-Server die Zuweisung einer Adresse anbieten. Als IP-Adresse wird dabei eine gültige Adresse aus dem Pool genommen. Wurde dem Rechner in der Vergangenheit schon mal eine IP-Adresse zugewiesen, so fordert er eben diese Adresse wieder an, und der DHCP-Server versucht ihm diese Adresse wieder zuzuweisen, wenn sie nicht bereits einem anderen Rechner zugewiesen wurde.

Der DHCP-Server prüft zusätzlich, ob die ausgesuchte Adresse im lokalen Netz noch frei ist. Sobald die Eindeutigkeit einer Adresse festgestellt wurde, wird dem anfragenden Rechner die gefundene Adresse zugewiesen.

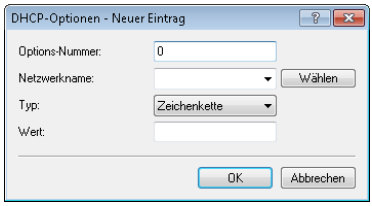
Hinweis: Im Auslieferungs-Zustand sind in den Geräten die IP-Netzwerke 'Intranet' und 'DMZ' angelegt, sind aber noch nicht mit IP-Adresse und Netzmaske ausgestattet – das Gerät befindet sich in einem besonderen Betriebszustand. Es verwendet dann selbst die IP-Adresse '172.23.56.254' und den Adress-Pool '172.23.56.x' für die Zuweisung der IP-Adressen im Netz.

Hinweis: Mehrere Netzwerke auf einem Interface: Mit der Konfiguration der IP- und DHCP-Netzwerke können auf einem logischen Interface mehrere Netzwerke mit unterschiedlichen DHCP-Einstellungen aktiv sein. In diesem Fall werden die DHCP-Einstellungen aus dem ersten passenden Netzwerk verwendet. Hierfür ist ggf. eine Priorisierung der Netzwerke notwendig.

DHCP-Optionen

Mit den DHCP-Optionen überträgt der DHCP-Server zusätzliche Konfigurationsparameter an die DHCP-Clients. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt z. B. den Gerätetyp an.

Sie finden die Konfiguration der DHCP-Optionen in LANconfig im Konfigurationsmenü unter **IPv4** > **DHCPv4** > **DHCP-Optionen**. Klicken Sie auf **Hinzufügen**, um einen neuen Eintrag anzulegen.



Options-Nummer

Nummer der Option, die an die DHCP-Clients übermittelt werden soll. Die Options-Nummer beschreibt die übermittelte Information, z. B. “17” (Root Path) für den Pfad zu einem Boot-Image für einen PC ohne eigene Festplatte, der über BOOTP sein Betriebssystem bezieht.

Hinweis: Eine Liste aller DHCP-Optionen finden Sie im “RFC 2132 – DHCP Options and BOOTP Vendor Extensions” der Internet Engineering Task Force (IETF).

Netzwerkname

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Typ

Typ des Eintrags. Dieser Wert ist abhängig von der jeweiligen Option. RFC 2132 definiert z. B. die Option “35” (ARP Cache Timeout) wie folgt:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

Aus dieser Beschreibung können Sie ablesen, dass für diese Option der Typ “32-Bit-Integer” verwendet wird.

Hinweis: Den Typ der Option entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

Wert

In diesem Feld definieren Sie den Inhalt der DHCP-Option.

IP-Adressen werden in der üblichen Schreibweise von IPv4-Adressen angegeben, also z. B. als “123.123.123.100”, Integer-Typen werden als normale Dezimalzahlen eingetragen, Strings als einfacher Text.

Mehrere Werte in einem Feld werden mit Kommas separiert, also z. B. “123.123.123.100, 123.123.123.200”.

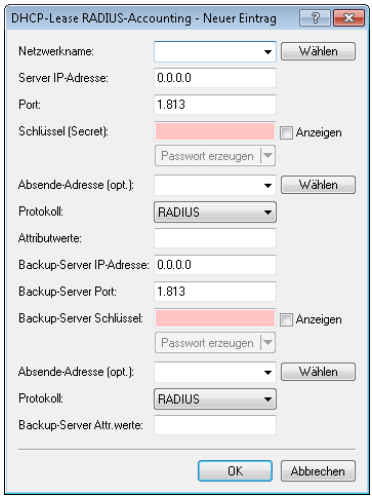
Hinweis: Die mögliche Länge des Optionswertes entnehmen Sie bitte dem entsprechenden RFC bzw. bei herstellerspezifischen DCHP-Optionen der jeweiligen Herstellerdokumentation.

DHCP-Lease RADIUS-Accounting

Weist der DHCP-Server einem DHCP-Client eine IP-Adresse zu, sendet er bei aktiviertem RADIUS-Accounting dem entsprechend zugewiesenen Accounting-Server (bzw. dem Backup-RADIUS-Server) ein `RADIUS Accounting Start`. Läuft die Gültigkeit der Adresszuweisung (DHCP-Lease) mangels Verlängerung ab, sendet der DHCP-Server ein `RADIUS Accounting Stop`. Zwischen diesen beiden Ereignissen sendet der DHCP-Server dem RADIUS-Server regelmäßig in einem konfigurierbaren Intervall ein `RADIUS Accounting Interim Update`.

Das RADIUS-Accounting für den DHCP-Server aktivieren oder deaktivieren Sie unter **IPv4** > **DHCPv4** mit einem Klick auf die Option **DHCP-Lease RADIUS-Accounting aktivieren**.

Das Intervall für die RADIUS-Interim-Updates konfigurieren Sie im Eingabefeld **Accounting-Interim-Intervall**. Den RADIUS-Accounting-Server und den entsprechenden Backup-Server konfigurieren Sie mit einem Klick auf **DHCP-Lease RADIUS-Accounting**.



Netzwerkname

Wählen Sie hier den Netzwerknamen des Netzes aus, für das RADIUS-Accounting-Nachrichten gesendet werden sollen.

Server IP-Adresse

Geben Sie hier die IP-Adresse oder den DNS-Namen des RADIUS-Servers an (IPv4 oder IPv6).

Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port “1813”.

Schlüssel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum RADIUS-Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

Absende-Adresse (opt.)

Standardmäßig schickt der RADIUS-Server seine Antworten zurück an die IP-Adresse Ihres Gerätes, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen alternativen Absende-Adresse verändern Sie die Quelladresse bzw. Route, mit der das Gerät den RADIUS-Server anspricht. Dies kann z. B. dann sinnvoll sein, wenn der Server über ver-

schiedene Wege erreichbar ist und dieser einen bestimmten Weg für seine Antwort-Nachrichten wählen soll.

Protokoll

Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für die Kommunikation mit dem RADIUS-Accounting-Server verwendet.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Backup-Server IP-Adresse

Geben Sie hier die IP-Adresse oder den DNS-Namen des Backup-RADIUS-Servers an.

Backup-Server Port

Geben Sie hier den TCP-Port an, über den der Backup-RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port “1813”.

Backup-Server Schlüssel

Geben Sie hier den Schlüssel (Shared Secret) für den Zugang zum Backup-RADIUS-Accounting-Server an. Stellen Sie sicher, dass dieser Schlüssel im entsprechenden Accounting-Server übereinstimmend konfiguriert ist.

Absende-Adresse (opt.)

Geben Sie hier optional eine alternative Absende-Adresse an, die der DHCP-Server an den Backup-RADIUS-Server überträgt.

Protokoll

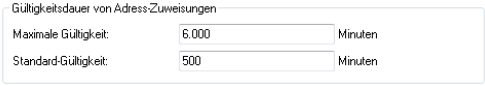
Über diesen Eintrag geben Sie das Protokoll an, dass der DHCP-Server für den Backup-RADIUS-Server verwendet.

Backup-Server Attr.werte

Geben Sie hier die zusätzlichen Attributwerte für die RADIUS-Kommunikation mit dem Backup-Server an.

Gültigkeitsdauer von Adress-Zuweisungen

Wenn ein DHCP-Client eine IP-Adresse bei einem DHCP-Server anfragt, kann er eine Gültigkeitsdauer für diese Adresse anfordern. In diesem Abschnitt konfigurieren Sie, wie der DHCP-Server diese Anfragen behandelt.



Maximale Gültigkeit

Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

Standard-Gültigkeit

Wenn ein Client eine IP-Adresse anfragt, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, weist der DHCP-Server dieser Adresse als Gültigkeitsdauer den hier eingestellten Wert zu.

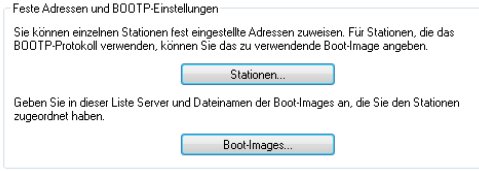
Vendor-Class- und User-Class-Identifier im DHCP-Client

Der DHCP-Client im Gerät kann in den versendeten DHCP-Requests zusätzliche Angaben einfügen, die eine Erkennung der Requests im Netzwerk erleichtern.

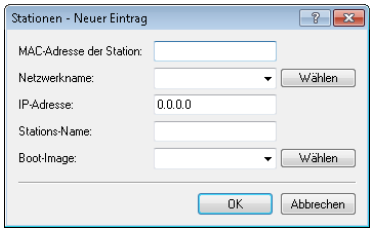
- Der Vendor-Class-Identifier (DHCP-Option 60) zeigt den Gerätetyp an. Die Vendor-Class-ID wird immer übertragen.
- Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an, der unter `Setup/DHCP` oder im LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'DHCP' im Feld 'User-Class-ID' eingetragen werden kann (Default: leer). Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

BOOTP: Zuweisung von festen IP-Adressen an bestimmte Stationen konfigurieren

Die Parameter zur Konfiguration von BOOTP finden Sie in LANconfig im Konfigurationsmenü unter **IPv4** > **BOOTP**.



Definieren Sie in der Liste der **Stationen** die MAC-Adresse einer Station, der Sie eine bestimmte IP-Adresse zuweisen möchten.



MAC-Adresse der Station

Geben Sie hier die Node-ID des Clients ein.

Die Node-ID ist die physikalische Kennung des Client-Netzwerkadapters und entspricht der MAC-Adresse.

Netzwerkname

Wählen Sie hier den Netzwerknamen des ARF-Netzes aus, für das die Einstellungen gelten sollen.

Wenn Sie diesen Eintrag leer lassen, weist das Gerät die konfigurierte Adresse aus dem ARF-Netz zu, aus dem die DHCP-Anfrage erfolgte. Erfolgt die Anfrage aus einem ARF-Netz, für das Sie keine spezielle Adresse konfiguriert haben, so weist das Gerät eine Adresse dynamisch aus dem Adress-Pool zu.

Hinweis: Wenn eine zugewiesene IP-Adresse nicht im Adressbereich des konfigurierten ARF-Netzes liegt, so wird die Zuweisung verworfen und anstelle dessen eine IP-Adresse aus dem Adress-Pool des ARF-Netzes verwendet, aus dem die Anfrage erfolgte.

IP-Adresse

Geben Sie hier die IP-Adresse ein, die das Gerät dem Client zuweist.

Stations-Name

Geben Sie hier einen Namen ein, mit dem das Gerät den Client identifiziert.

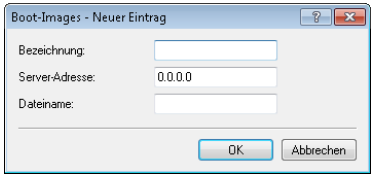
Wenn ein Client seinen Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

Boot-Image

Wenn der Client das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das der Client sein Betriebssystem laden soll.

Den Server, der das Boot-Image zur Verfügung stellt, sowie den Namen der Datei auf dem Server müssen Sie in der Boot-Image-Tabelle eingeben.

Definieren Sie in der Liste der **Boot-Images** ein Boot-Image, dass Sie optional einer Station zuweisen möchten.



Bezeichnung

Geben Sie eine Bezeichnung an, die diesen Eintrag eindeutig kennzeichnet.

Server-Adresse

Bestimmen Sie die IP-Adresse des Servers, der das Boot-Image zur Verfügugn stellt.

Dateiname

Geben Sie den Namen der Datei an, die das Boot-Image enthält.

15.1.3 Konfiguration der DHCP-Clients

Standardmäßig sind fast alle Einstellungen in der Netzwerkumgebung von Windows so eingestellt, dass die benötigten Parameter über DHCP angefragt werden. Überprüfen Sie die Windows-Einstellungen mit einem Klick auf **Start** / **Einstellungen** / **Systemsteuerung** / **Netzwerk**. Wählen Sie den Eintrag für **TCP/IP** Ihres Netzwerkadapters, und öffnen Sie die **Eigenschaften**. Auf den verschiedenen Registerkarten können Sie nun nachsehen, ob spezielle Einträge z. B. für die IP-Adresse oder das Standard-Gateway vorhanden sind. Wenn Sie alle Werte vom DHCP-Server zuweisen lassen wollen, löschen Sie nur die entsprechenden Einträge.

Sollte ein Rechner andere Parameter verwenden als die ihm zugewiesenen (z. B. ein anderes Standard-Gateway), so müssen diese Parameter direkt am Arbeitsplatzrechner eingestellt werden. Der Rechner ignoriert dann die entsprechenden Parameter in der Zuweisung durch den DHCP-Server. Unter Windows geschieht das z. B. über die Eigenschaften der Netzwerkumgebung. Klicken Sie auf **Start** / **Einstellungen** / **Systemsteuerung** / **Netzwerk**. Wählen Sie den Eintrag für 'TCP/IP' an Ihrem Netzwerkadapter und öffnen die **Eigenschaften**. Auf den verschiedenen Registerkarten können Sie nun die gewünschten Werte eintragen.

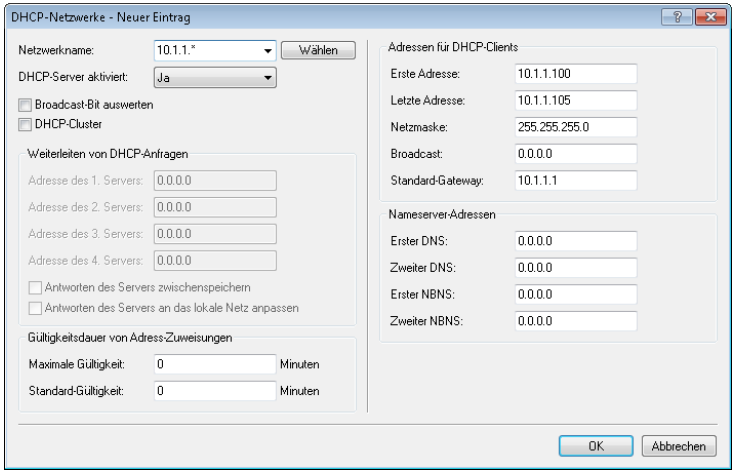
15.1.4 DHCP-Relay-Server

Ein Gerät kann nicht nur DHCP-Anfragen an einen übergeordneten DHCP-Server weiterleiten, es kann auch selbst als zentraler DHCP-Server fungieren (DHCP-Relay-Server).

Um ein Gerät als DHCP-Relay-Server für andere Netzwerke anzubieten, wird die Relay-Agent-IP-Adresse (GI-Adresse) als Netzwerkname in die Tabelle der IP-Netzwerke eingetragen.

Wenn das gleiche Netz von mehreren Relay-Agents verwendet wird (z. B. mehrere Accesspoints leiten die Anfragen auf einen zentralen DHCP-Server weiter), dann kann die GI-Adresse auch mit einem “*” abgekürzt werden. Wenn z. B. Clients im entfernten Netz `10.1.1.0/255.255.255.0` Adressen zugewiesen werden sollen und in diesem Netz mehrere Relay-Agents stehen, die alle das Gerät als übergeordneten DHCP-Server verwenden, dann kann

die Zuweisung von IP-Adressen und Standard-Gateway an die Clients so erfolgen:



Hinweis: Für die Betriebsart als DHCP-Relay-Server ist die Angabe des Adress-Pools und der Netzmaske zwingend erforderlich.

DNS-Auflösung von über DHCP gelernten Namen

Der DNS-Server berücksichtigt bei der Auflösung von über DHCP gelernten Namen die Interface-Tags, d. h. es werden nur Namen aufgelöst, die aus einem Netz mit dem gleichen Interface-Tag gelernt wurden wie das Netz des Anfragenden. Kommt die Anfrage aus einem ungetaggten Netz, so werden alle Namen – also auch die, die von getaggten Netzen gelernt wurden – aufgelöst. Ebenso sind für getaggte Netze alle Namen sichtbar, die von ungetaggten Netzen gelernt wurden.

Namen, die von Relay-Agents gelernt wurden, werden immer so behandelt, als wären sie von einem ungetaggten Netz gelernt worden, d. h. diese Namen sind für alle Netze sichtbar.

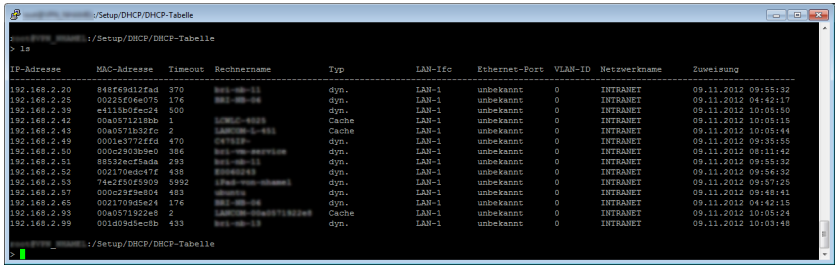
15.1.5 Anzeige von Statusinformationen des DHCP-Servers

Eine Übersicht über die IP-Adressen im LAN gibt die Status-Tabelle des DHCP-Servers. Sie zeigt folgende Informationen über die Geräte an, denen der DHCP-Server eine IP-Adresse zugewiesen hat:

- IP-Adresse, welche der DHCP-Server dem Netzwerkgerät zugewiesen hat
- MAC-Adresse des Netzwerkgerätes
- Timeout, verbleibende Gültigkeitsdauer in Minuten
- Rechnername
- Typ der Adresszuweisung, dynamisch oder aus dem Cache
- LAN-Ifc, logische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- Ethernet-Port, physikalische Schnittstelle über welche der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat
- VLAN-ID des Netzwerks
- Netzwerkname
- Zuweisung, Zeitpunkt zu dem der DHCP-Server dem Netzwerkgerät die IP-Adresse zugewiesen hat

Sie finden die Statusinformationen des DHCP-Servers an folgenden Stellen:

- Telnet: /Setup/DHCP/DHCP-Tabelle



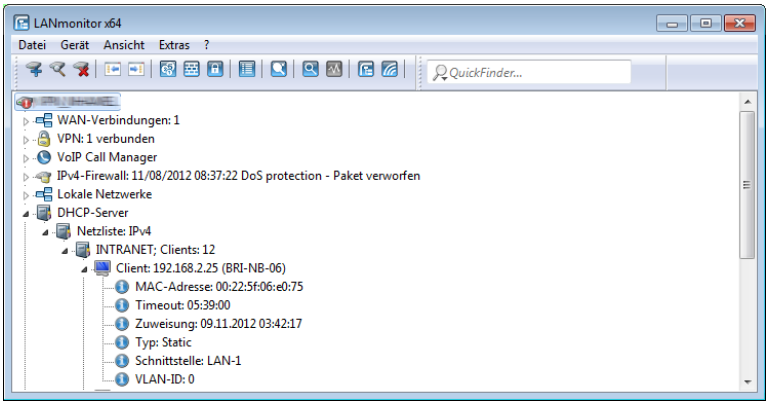
- Webconfig: /Setup/DHCP/DHCP-Tabelle

LCOS-Menübaum
Setup
DHCP

DHCP-Tabelle

IP-Adresse	MAC-Adresse	Timeout	Rechnername	Typ	LAN-Ifc	Ethernet-Port	VLAN-ID	Netzwerkname	Zuweisung
192.168.2.25	00225f06e075	346	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:17
192.168.2.39	e4115b0fec24	321		dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:17:13
192.168.2.42	00a0571218bb	2	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:45
192.168.2.43	00a0571b32fc	1	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:15:17
192.168.2.49	0001e3772ffd	389	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 05:24:59
192.168.2.50	000c2903b9e0	306	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:01:46
192.168.2.51	88532ecf5ada	463	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:44:20
192.168.2.52	002170edc47f	358	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:53:53
192.168.2.53	74e2f50f5909	5968	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:43:35
192.168.2.57	000c29f9e804	431	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 06:07:08
192.168.2.65	0021709d5e24	346	[redacted]	dyn.	LAN-1	unbekannt	0	INTRANET	09.11.2012 04:42:15
192.168.2.93	00a0571922e8	2	[redacted]	Cache	LAN-1	unbekannt	0	INTRANET	09.11.2012 07:16:00

- LANmonitor: Aufgeteilt nach Netzwerkname unter DHCP-Server > Netzliste



15.1.6 DHCP-Cluster

Wenn mehrere DHCP-Server in einem Netz aktiv sind, dann "verteilen" sich die Stationen im Netz gleichmäßig auf diese Server. Der DNS-Server der Geräte löst allerdings nur die Namen der Stationen richtig auf, denen der eigene DHCP-Server die Adressinformationen zugewiesen hat. Damit der DNS-Server auch die Namen anderer DHCP-Server auflösen kann, können die DHCP-Server im Cluster betrieben werden. In dieser Betriebsart verfolgt der DHCP-Server alle im Netz laufenden DHCP-Verhandlungen mit und trägt

auch Stationen in seine Tabelle ein, die sich nicht bei ihm, sondern bei anderen DHCP-Servern im Cluster angemeldet haben.

Die Einstellung zu DHCP-Cluster aktivieren Sie unter **IPv4** > **DHCPv4** in den Einstellungen der **DHCP-Netzwerke**.

15.1.7 Alternative DHCP-Server zur Weiterleitung

Der DHCP-Server erlaubt verschiedene Betriebsarten. Im Weiterleitungs-Modus agiert das Gerät im lokalen Netz als DHCP-Relay und leitet Anfragen an einen oder mehrere konfigurierte DHCP-Server weiter. Diese Einstellung erlaubt den Betrieb von zentralen DHCP-Servern in einem anderen Netz.

Alle DHCP-Nachrichten, welche die DHCP-Clients als Broadcast senden, werden an alle konfigurierten DHCP-Server weitergeleitet. Der Client wählt dann den ersten Server der antwortet und sendet alle weiteren Nachrichten als Unicast, die gezielt an den zuständigen Server weitergeleitet werden. Falls der gewählte Server nicht erreichbar ist, versendet der Client erneut Broadcast-Nachrichten und wählt einen anderen DHCP-Server.

Die DHCP-Weiterleitungsserver konfigurieren Sie unter **IPv4** > **DHCPv4** in den Einstellungen der **DHCP-Netzwerke**.

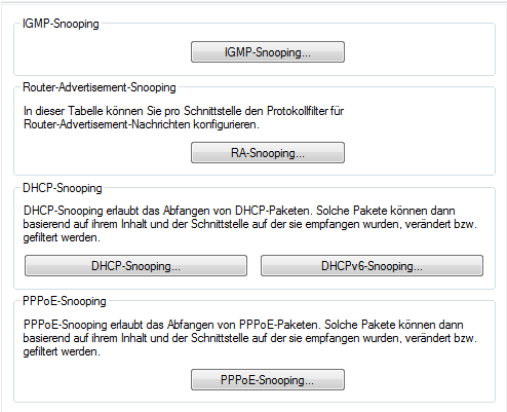
15.1.8 DHCP-Snooping und DHCP-Option 82

DHCP verfügt ursprünglich über keine Sicherheitsmechanismen zum Schutz von Angriffen auf die Zuweisung der Netzkonfiguration. Sendet z. B. ein Client ein DHCP-Discover-Paket ins Netz, um von einem DHCP-Server eine gültige Netzkonfiguration zu erhalten, kann ein Angreifer gefälschte DHCP-Offer-Pakete an diesen Client senden und ihm so z. B. ein präpariertes Default-Gateway vorsetzen (DHCP-Spoofing).

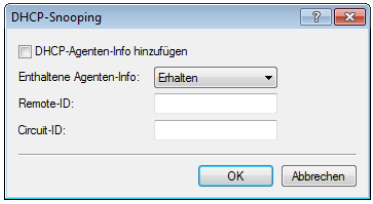
Das DHCP-Snooping ermöglicht Geräten, die DHCP-Pakete empfangen und weiterleiten, diese Datenpakete zu analysieren, zu verändern und anhand bestimmter Kriterien zu filtern. Die zusätzlich eingefügten Informationen über die Herkunft von DHCP-Paketen ermöglichen es einem DHCP-Server einerseits, umfangreiche Netzen besser zu verwalten. Anderseits kann ein Angreifer, in dessen DHCP-Paketen diese Zusatzinformationen fehlen, nicht mehr einfach in DHCP-Verhandlungen zwischen DHCP-Server, DHCP-Relay-Agent und DHCP-Client stören.

Der Access Point unterstützt DHCP-Snooping auf Layer-2. Damit ist es ihm z. B. möglich, Informationen (z. B. die SSID) in die empfangenen DHCP-Pakete des Clients auf dem WLAN einzufügen, bevor er sie anschließend in das LAN weiterleitet. Der Access Point fügt dazu die DHCP Relay Agent Information Option (Option 82) nach RFC 3046 ein.

Im LANconfig können Sie das DHCP-Snooping unter **Schnittstellen** > **Snooping** mit einem Klick auf **DHCP-Snooping** für jede Schnittstelle separat festlegen.



Nach Auswahl der entsprechenden Schnittstelle können Sie die folgenden Einstellungen festlegen:



DHCP-Agenten-Info hinzufügen

Bestimmen Sie hier, ob der DHCP-Relay-Agent den ankommenden DHCP-Paketen die DHCP-Option "Relay Agent Info" (Option 82) anfügen bzw. eine vorhandene "Relay Agent Info" bearbeiten soll, bevor er die Anfrage an einen DHCP-Server weiterleitet.

Die "Relay Agent Info" setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Erhaltene Agenten-Info

Bestimmen Sie hier, wie der DHCP-Relay-Agent mit der "Relay Agent Info" in ankommenden DHCP-Datenpaketen umgehen soll. Folgende Einstellungen sind möglich:

- erhalten: In dieser Einstellung leitet der DHCP-Relay-Agent ein DHCP-Paket mit vorhandener "Relay Agent Info" ohne Veränderung an den DHCP-Server weiter.
- ersetzen: In dieser Einstellung ersetzt der DHCP-Relay-Agent eine vorhandene "Relay Agent Info" durch die in den Feldern **Remote-Id** und **Circuit-Id** vorgegebenen Werte.
- Paket verwerfen: In dieser Einstellung löscht der DHCP-Relay-Agent ein DHCP-Paket, das eine "Relay Agent Info" enthält.

Remote-Id

Die Remote-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig den Client, der einen DHCP-Request stellt.

Circuit-Id

Die Circuit-ID ist eine Unteroption der "Relay Agent Info"-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen DHCP-Request stellt.

Sie können die folgenden Variablen für **Remote-Id** und **Circuit-Id** verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der Relay-Agent den DHCP-Request erhalten hat.
- %n: fügt den Namen des DHCP-Relay-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- %v: fügt die VLAN-ID des DHCP-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des DHCP-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das DHCP-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physi-

kalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.

- %r: fügt die schnittstellenunabhängige und systemweit gültige MAC-Adresse des Gerätes ein, welches den DHCP-Request erhalten hat.
- %s: fügt die WLAN-SSID ein, wenn das DHCP-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des Relay-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

15.2 Domain-Name-Service (DNS)

Der Domain-Name-Service (DNS) stellt in TCP/IP-Netzen die Verknüpfung zwischen Rechnernamen bzw. Netzwerknamen (Domains) und IP-Adressen her. Dieser Service ist auf jeden Fall erforderlich für die Kommunikation im Internet. Aber auch innerhalb eines lokalen Netzes oder bei der LAN-Kopplung ist es sinnvoll, die IP-Adressen im LAN den Namen der Rechner eindeutig zuordnen zu können.

15.2.1 Was macht ein DNS-Server?

Die bei einem DNS-Server nachgefragten Namen bestehen aus mehreren Teilen: Ein Teil besteht aus dem eigentlichen Namen des Hosts oder Dienstes, der angesprochen werden soll, ein anderer Teil kennzeichnet die Domain. Innerhalb eines lokalen Netzes ist die Angabe der Domain optional. Diese Namen können also z. B. 'www.domain.com' oder 'ftp.domain.com' heißen.

Ohne DNS-Server im lokalen Netz wird jeder lokal unbekannte Name über die Default-Route gesucht. Durch die Verwendung eines DNS-Servers können alle Namen, die mit ihrer IP-Adresse bekannt sind, direkt bei der richtigen Gegenstelle gesucht werden. Der DNS-Server kann dabei im Prinzip ein separater Rechner im Netz sein. Folgende Gründe sprechen jedoch dafür, die Funktionen des DNS-Servers direkt im Gerät anzusiedeln:

- Das Gerät kann in der Betriebsart als DHCP-Server die IP-Adressen für die Rechner im lokalen Netz selbstständig verteilen. Der DHCP-Server kennt also schon alle Rechner im eigenen Netz, die ihre IP-Adresse per DHCP beziehen, mit Rechnername und IP-Adresse. Ein externer DNS-

Server hätte bei der dynamischen Adressvergabe des DHCP-Servers möglicherweise Schwierigkeiten, die Zuordnung zwischen IP-Adresse und Namen aktuell zu halten.

- Beim Routing von Windows-Netzen über NetBIOS kennt das Gerät außerdem die Rechnernamen und IP-Adressen in den anderen angeschlossenen NetBIOS-Netzen. Außerdem melden sich auch die Rechner mit fest eingestellter IP-Adresse ggf. in der NetBIOS-Tabelle an und sind damit mit Namen und Adressen bekannt.
- Der DNS-Server im Gerät kann gleichzeitig als sehr komfortabler Filtermechanismus eingesetzt werden. Anfragen nach bestimmten Domains, die nicht besucht werden dürfen, können durch die einfache Angabe des Domain-Namens für das ganze LAN, nur für Teilnetze (Subnetze) oder sogar für einzelne Rechner gesperrt werden.

Wie reagiert der DNS-Server auf eine Anfrage?

Der DNS-Server bezieht bei Anfragen nach bestimmten Namen alle Informationen in die Suche mit ein, die ihm zur Verfügung stehen:

- Zuerst prüft der DNS-Server, ob der Zugriff auf diesen Namen nicht durch die Filterliste verboten ist. Wenn das der Fall ist, wird der anfragende Rechner mit einer Fehlermeldung darüber informiert, dass er auf diesen Namen nicht zugreifen darf.
- Dann sucht er in der eigenen statischen DNS-Tabelle nach Einträgen für den entsprechenden Namen.
- Steht in der DNS-Tabelle kein Eintrag für diesen Namen, wird die dynamische DHCP-Tabelle durchsucht. Die Verwendung der DHCP-Informationen kann bei Bedarf ausgeschaltet werden.
- Findet der DNS-Server in den vorausgegangenen Tabellen keine Informationen über den Namen, werden die Listen des NetBIOS-Moduls durchsucht. Auch die Verwendung der NetBIOS-Informationen kann bei Bedarf ausgeschaltet werden.
- Schließlich prüft der DNS-Server, ob die Anfrage über ein WAN-Interface an einen anderen DNS-Server weitergeleitet werden soll (Spezielles DNS-Forwarding über die DNS-Destinationstabelle).

Sollte der gesuchte Name in allen verfügbaren Informationen nicht gefunden werden, leitet der DNS-Server die Anfrage über den generellen DNS-Forwar-

ding-Mechanismus an einen anderen DNS-Server (z. B. beim Internet-Provider) weiter oder schickt dem anfragenden Rechner eine Fehlermeldung.

15.2.2 DNS-Forwarding

Wenn eine Anfrage nicht aus den eigenen DNS-Tabellen bedient werden kann, leitet der DNS-Server die Anfrage an andere DNS-Server weiter. Dieser Vorgang heißt DNS-Forwarding (DNS-Weiterleitung).

Dabei unterscheidet man zwischen

- speziellem DNS-Forwarding

  Anfragen nach bestimmten Namensbereichen werden an bestimmte DNS-Server weitergeleitet.

- generellem DNS-Forwarding

  Alle anderen nicht näher spezifizierten Namen werden an den „übergeordneten“ DNS-Server weitergeleitet.

Spezielles DNS-Forwarding

Beim speziellen DNS-Forwarding können Namensbereiche definiert werden, für deren Auflösung festgelegte DNS-Server angesprochen werden.

Ein typischer Anwendungsfall für spezielles DNS-Forwarding ergibt sich beim Heimarbeitsplatz: Der Benutzer möchte gleichzeitig sowohl auf das firmeneigene Intranet als auch direkt auf das Internet zugreifen können. Die Anfragen ins Intranet müssen an den DNS-Server der Firma, alle anderen Anfragen an den DNS-Server des Internet-Providers geleitet werden.

Generelles DNS-Forwarding

Alle DNS-Anfragen, die nicht auf sonstige Weise aufgelöst werden können, werden an einen DNS-Server weitergeleitet. Dieser DNS-Server bestimmt sich nach folgenden Regeln:

- Der Router sucht zunächst in seinen eigenen Einstellungen, ob ein DNS-Server eingetragen ist. Wird er dort fündig, holt er die gewünschte Information von diesem Server. Bis zu zwei übergeordnete DNS-Server können angegeben werden.

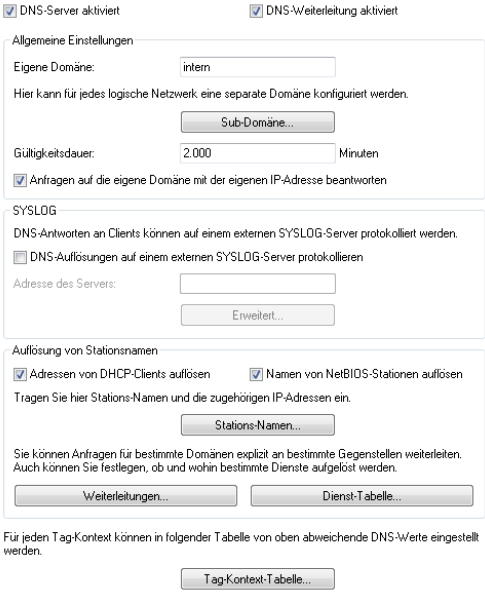
LANconfig	TCP/IP / Adressen / Erster DNS-Server / Zweiter DNS-Server
WEBconfig	HiLCOS-Menübaum / Setup / TCP/IP /E DNS-Default / DNS-Backup
Terminal/Telnet	`/Setup/TCP-IP/DNS-Default /Setup/TCP-IP/DNS-Backup`

- Gibt es keinen eingetragenen DNS-Server im Router, versucht er auf einer evtl. bestehenden PPP-Verbindung (z. B. zum Internet-Provider) einen DNS-Server zu erreichen, und holt die Zuordnung der IP-Adresse zum Namen von dort. Das gelingt natürlich nur dann, wenn während der PPP-Verhandlung die Adresse eines DNS-Servers an den Router übermittelt worden ist.
- Besteht keine Verbindung, wird die Default-Route aufgebaut und dort nach dem DNS-Server gesucht.

Durch dieses Verfahren benötigen Sie keine Kenntnisse über die Adressen eines DNS-Servers. Der Eintrag der Intranet-Adresse Ihres Routers als DNS-Server bei den Arbeitsplatzrechnern reicht aus, um die Namenszuordnung zu ermöglichen. Außerdem wird damit die Adresse des DNS-Servers automatisch aktualisiert. Sollte z. B. der Provider, der diese Adresse mitteilt, seinen DNS-Server umbenennen, oder sollten Sie zu einem anderen Provider wechseln, erhält Ihr lokales Netz stets die aktuellen Informationen.

15.2.3 So stellen Sie den DNS-Server ein

Die Einstellungen für den DNS-Server finden Sie in LANconfig unter **IPv4** > **DNS**.



1. Aktivieren Sie den DNS-Server, indem Sie die Option **DNS-Server aktiviert** markieren.

   Soll der DNS-Server die DNS-Anfrage an einen anderen DNS-Server weiterleiten (DNS-Forwarding), markieren Sie zusätzlich die Option **DNS-Weiterleitung aktiviert**.

2. Geben Sie die eigene Domain ein, in der sich der DNS-Server befindet.

   Mit Hilfe dieser Domain erkennt der DNS-Server bei DNS-Anfragen, ob sich der gesuchte Name im eigenen LAN befindet oder nicht. Die Angabe der Domain ist optional.

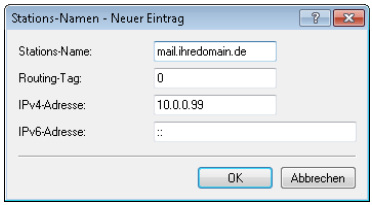
3. Geben Sie an, ob der DNS-Server die Client-Informationen aus dem DHCP-Server und dem NetBIOS-Modul verwenden soll.
4. Tragen Sie bekannte Gegenstellen und deren IP-Adressen in die Tabelle **Stations-Namen** ein.

   Der DNS-Server dient hauptsächlich dazu, Anfragen nach öffentlichen Adressen im Internet von den Anfragen nach Adressen bei anderen

Gegenstellen zu trennen. Tragen Sie daher alle Rechner in die Tabelle ein,

- deren Name und IP-Adresse Sie kennen,
- die nicht im eigenen LAN liegen,
- die nicht im Internet liegen und
- die über den Router erreichbar sind.

Wenn Sie z. B. in einem externen Büro oder in einer Filiale arbeiten und die Mitarbeiter über den Router den Mailserver in der Zentrale (Name: “mail.ihredomain.de”, IP: “10.0.0.99”) erreichen wollen, tragen Sie ein:



Hinweis:

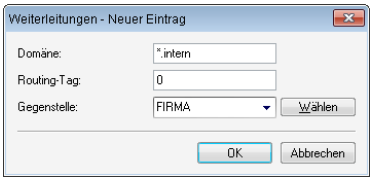
Die Angabe der Domain ist dabei optional, aber zu empfehlen.

Wenn ein Mitarbeiter nun sein Mailprogramm startet, sucht es automatisch den Server “mail.ihredomain.de” . Der DNS-Server gibt daraufhin die IP-Adresse “10.0.0.99” zurück. Das Mailprogramm startet dann eine Verbindung zu dieser IP-Adresse. Mit entsprechenden Einträgen in der IP-Routing-Tabelle und Gegenstellenliste des Routers baut das Mailprogramm die Verbindung zum Mailserver im Netz der Zentrale auf.

5. Um ganze Namensbereiche von einem anderen DNS-Server auflösen zu lassen, fügen Sie einen Weiterleitungseintrag bestehend aus Namensbereich und Gegenstelle hinzu.

Bei der Angabe der Namensbereiche dürfen Sie die Wildcards “?” für einzelne Zeichen und “*” für mehrere Zeichen verwenden.

Um alle Domains mit der Endung “.intern” auf einen DNS-Server im LAN der Gegenstelle “FIRMA” umzuleiten, erstellen Sie folgenden Eintrag:



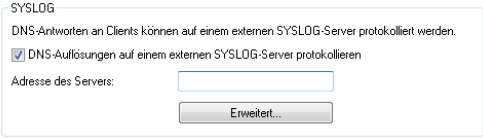
Hinweis: Der DNS-Server kann entweder über den Name der Gegenstelle (für automatische Konfiguration über PPP) oder die explizite IP-Adresse des zuständigen Nameservers angegeben werden.

15.2.4 Protokollierung von DNS-Anfragen über SYSLOG

Um Anfragen von Clients an den DNS-Server zu dokumentieren, besteht die Möglichkeit, dass der DNS-Server im Gerät die Antworten an den Client auch laufend in Form einer SYSLOG-Meldung an einen SYSLOG-Server sendet.

Hinweis: Bitte beachten Sie, dass eine Aufzeichnung der DNS-Anfragen nur gemäß der in ihrem Land gültigen Datenschutzbestimmungen erfolgen darf.

In LANconfig konfigurieren Sie die Dokumentation von DNS-Anfragen unter **IPv4** > **DNS** im Abschnitt **SYSLOG**.



DNS-Auflösungen auf einem externen SYSLOG-Server protokollieren

Diese Option aktiviert oder deaktiviert (Default-Einstellung) den Versand von SYSLOG-Meldungen bei DNS-Anfragen.

Hinweis: Dieser Schalter ist unabhängig vom globalen Schalter im Syslog-Modul unter **Meldungen** > **Allgemein** > **SYSLOG**. D. h., wenn Sie hier die Option zur Aufzeichnung der DNS-Anfragen aktivieren, sendet der DNS-Server auch bei global deaktiviertem SYSLOG-Modul die entsprechenden SYSLOG-Meldungen an einen SYSLOG-Server.

Jede DNS-Auflösung (ANSWER-Record oder ADDITIONAL-Record) erzeugt jeweils eine SYSLOG-Meldung mit dem Aufbau `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Ressource-Record`.

Dabei haben die Parameter die folgenden Bedeutungen:

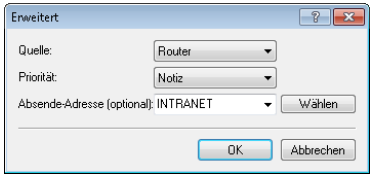
- Die `TID` (Transaction-ID) enthält einen 4-stelligen Hexadezimal-Code.
- Der `{Hostname}` ist nur dann Bestandteil der Meldung, wenn der DNS-Server ihn ohne DNS-Anfrage auflösen kann (wie auch im Firewall-Log).
- Die `Ressource-Record` besteht aus drei Teilen: Der Anfrage, dem Typ bzw. der Klasse und der IP-Auflösung (z. B. `www.mydomain.com STD A resolved to 193.99.144.32`)

Adresse des Servers

Geben Sie hier die Adresse des SYSLOG-Servers ein. Die Eingabe als IPv4-/IPv6-Adresse oder als DNS-Name ist möglich.

Hinweis: Die Angabe der IP-Adressen `127.0.0.1` und `::1` ist generell nicht erlaubt, um so die Nutzung eines externen Servers zu erzwingen.

Um die SYSLOG-Meldung zu konfigurieren, klicken Sie auf **Erweitert**.



Quelle

Wählen Sie hier aus, welche Quelle in den SYSLOG-Meldungen eingetragen ist.

Priorität

Wählen Sie hier aus, welche Priorität in den SYSLOG-Meldungen eingetragen ist.

Absende-Adresse (optional)

Geben Sie hier optional eine andere Adresse (Name oder IP) an, mit der Ihr Gerät gegenüber dem SYSLOG-Server als Absender auftritt. Standard-

mäßig verwendet Ihr Gerät seine Adresse aus dem jeweiligen ARF-Kontext, ohne dass Sie diese hier angeben müssen. Durch Angabe einer optionalen Loopback-Adresse verändern Sie die Quelladresse bzw. Route, mit der Ihr Gerät die Gegenstelle anspricht. Dies kann z. B. dann sinnvoll sein, falls Ihr Gerät über verschiedene Wege erreichbar ist und die Gegenstelle einen bestimmten Weg für ihre Antwort-Nachrichten wählen soll.

Hinweis: Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen **unmaskiert** verwendet.

Hinweis: Mehr Informationen über SYSLOG und die zur Verfügung stehenden Einstellungen finden Sie im Abschnitt *Das SYSLOG-Modul*.

15.2.5 URL-Blocking

1. Mit der Filterliste können Sie schließlich den Zugriff auf bestimmte Namen oder Domains sperren.

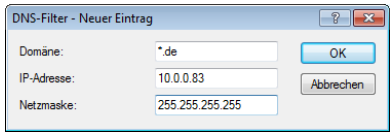
   Um die Domain (in diesem Fall den Web-Server) 'www.gesperrt.de' für alle Rechner im LAN zu sperren, sind die folgenden Befehle und Eingaben notwendig:

LANconfig	TCP/IP / DNS-Filter /E DNS-Filter / Hinzufügen
WEBconfig	… E/ Filter-Liste / Hinzufügen
Terminal/Telnet	`cd Setup/DNS/Filter-Liste set 001 www.gesperrt.de 0.0.0.0 0.0.0.0`

   Der Index '001' kann bei der Konfiguration über Telnet oder WEBconfig frei gewählt werden und dient nur der eindeutigen Bezeichnung des Eintrags.

Hinweis: Bei der Eingabe der Domäne sind auch die Wildcards '?' (steht für genau ein Zeichen) und '*' (für beliebig viele Zeichen) erlaubt.

Um nur einem bestimmten Rechner (z. B. mit IP 10.0.0.123) den Zugriff auf DE-Domains zu sperren, tragen Sie folgende Werte ein:



Im Konsolenmodus lautet der Befehl:

```
set 002 *.de 10.0.0.123 255.255.255.255
```

Hinweis: Die Hitliste in der DNS-Statistik zeigt Ihnen die 64 Namen, die am häufigsten nachgefragt werden, und bietet Ihnen damit eine gute Basis für die Einstellung der Filter-Liste.

Durch die geeignete Wahl von IP-Adressen und Netzmasken können bei der Verwendung von Subnetting in Ihrem LAN auch einzelne Abteilungen gefiltert werden. Dabei steht die IP-Adresse '0.0.0.0' jeweils für alle Rechner in einem Netz, die Netzmaske '0.0.0.0' für alle Netze.

15.2.6 Dynamic DNS

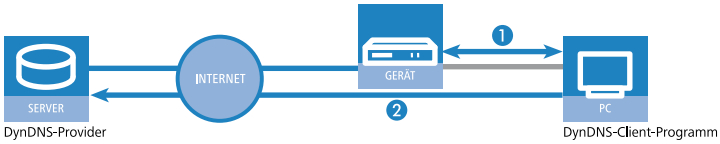
Damit auch Systeme mit dynamischen IP-Adressen über das WAN - also beispielsweise über das Internet - erreichbar sind, existieren eine Reihe von sog. Dynamic DNS-Server-Anbietern (z. B. www.dynDNS.org).

Damit wird ein Gerät immer unter einem bestimmten Namen (FQDN - ’fully qualified domain name’) erreichbar (z. B. “http://MyDevice.dynDNS.org”).

Der Vorteil liegt auf der Hand: Wenn Sie z. B. eine Fernwartung an einem Anschluss ohne ISDN durchführen wollen (z. B. über WEBconfig / HTTPS), oder über den VPN-Client auf eine Außenstelle mit dynamischer IP-Adresse zugreifen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen.

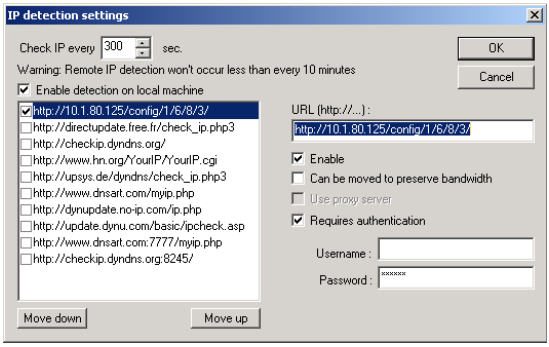
Wie gelangt die aktuelle IP-Adresse zum Dynamic-DNS-Server?

Dynamic-DNS-Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines Geräts ermitteln können **1**, und im Falle einer Änderung an den jeweiligen Dynamic-DNS-Server übertragen **2**.



Die aktuelle WAN-seitige IP-Adresse eines Geräts kann unter folgender Adresse ausgelesen werden:

```
http://<Adresse des Geräts>/config/1/6/8/3/
```



Alternativ kann das Gerät die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:

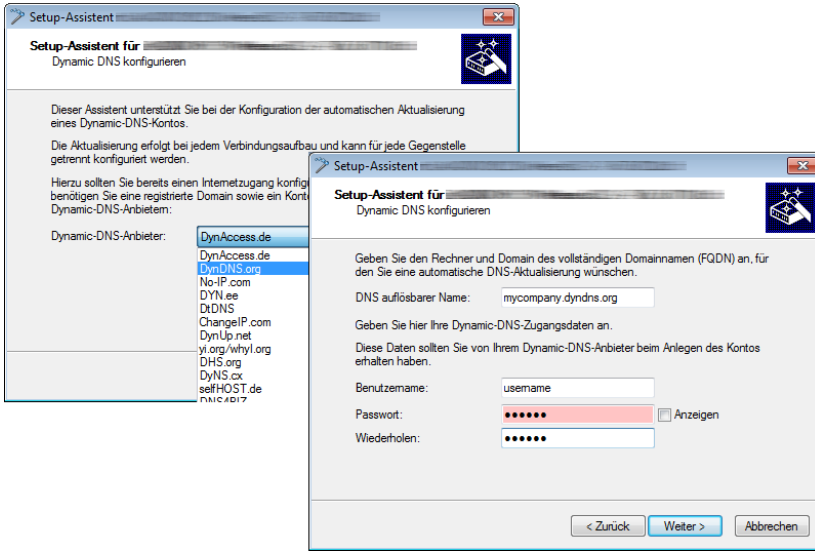
Dazu wird eine Aktion definiert, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein

Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org sieht z. B. so aus:

- http://Username:Password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a

Damit werden der Hostname der Aktion und die aktuelle IP-Adresse des Geräts an das durch Username und Password spezifizierte Konto bei DynDNS.org übermittelt, der entsprechende Eintrag wird aktualisiert.

Die dazu notwendigen Einstellungen können komfortabel mit dem Setup-Assistenten von LANconfig vorgenommen werden:



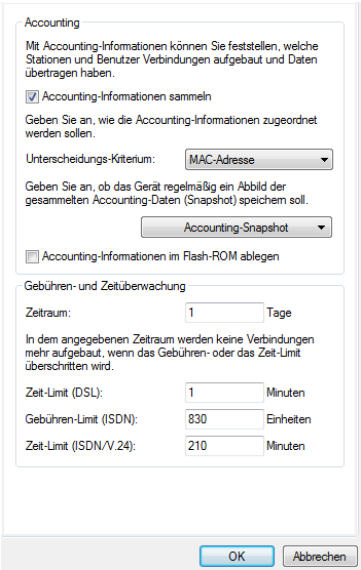
Der Setup-Assistent ergänzt die beschriebene Basis-Aktion um weitere anbieterspezifische Parameter, die hier nicht näher beschrieben werden. Außerdem legt der Setup-Assistent weitere Aktionen an, mit denen das Verhalten des Geräts gesteuert wird für den Fall, dass die Aktualisierung nicht im ersten Durchlauf erfolgreich durchgeführt werden konnte.

15.3 Accounting

In der Accounting-Tabelle werden Informationen über die Verbindungen der Clients im eigenen Netzwerk zu verschiedenen Gegenstellen mit Angabe der Verbindungszeit und der übertragenen Datenvolumen gespeichert. Mit Hilfe von Accounting-Snapshots können die Accounting-Daten zu bestimmten Zeitpunkten regelmäßig für eine weitere Auswertung festgehalten werden.

15.3.1 Konfiguration des Accounting

Bei der Konfiguration des Accounting werden die allgemeinen Parameter festgelegt:



Konfigurationstool	*Aufruf*
LANconfig	Management / Kosten
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Accounting

- Accounting-Informationen sammeln
  - Accounting ein- oder ausschalten.

- Accounting-Informationen im Flash-ROM ablegen
  - Accounting-Daten im Flashspeicher ein- oder ausschalten. Wenn die Accounting-Daten im Flash gespeichert werden, gehen sie auch bei Stromausfall nicht verloren.
- Sortierkriterium

  Auswahl des Merkmals, nach dem die Accounting-Daten kumuliert werden:
  - MAC-Adresse: Die Daten werden anhand der MAC-Adresse der Clients gesammelt.
  - IP-Adresse: Die Daten werden anhand der IP-Adresse der Clients gesammelt.

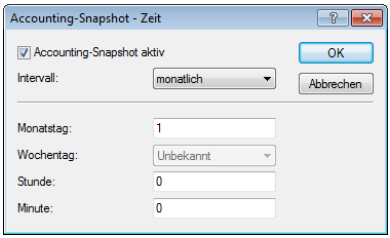
  Hinweis: Die Option 'IP-Adresse' kann bei wechselnden IP-Adressen, z. B. bei Verwendung eines DHCP-Servers, zu ungenauen Accounting-Daten führen. Eine Zuordnung der Daten zu Benutzern ist dann ggf. nicht exakt möglich. Auf der anderen Seite können mit dieser Einstellung die Daten von Clients separiert werden, die sich hinter einem weiteren Router befinden und daher mit der gleichen MAC-Adresse des Routers in der Accounting-Liste auftauchen.

- Sortieren nach

  Wählen Sie hier aus, ob die Daten in der Accounting-Tabelle nach Verbindungszeiten oder Datenvolumen sortiert werden sollen.

Konfiguration des Snapshots

Bei der Konfiguration des Snapshots wird das Interval festgelegt, in dem die Accounting-Daten in einem Snapshot zwischengespeichert werden:



Konfigurationstool	*Aufruf*
LANconfig	Management / Kosten / Accounting-Snapshot
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Accounting > Zeit-Schnappschuss

Hinweis: Die Snapshot-Funktion kann nur dann genutzt werden, wenn das Gerät über eine gültige Systemzeit verfügt.

- Accounting-Snapshot aktiv
  - Zwischenspeichern der Accounting-Daten ein- oder ausschalten.
- Interval
  - täglich, wöchentlich oder monatlich
- Monatstag

  Der Tag im Monat, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'monatlich' von Bedeutung.
- Wochentag

  Der Wochentag, an dem die Zwischenspeicherung vorgenommen wird. Nur beim Interval 'wöchentlich' von Bedeutung.
- Stunde

  Die Stunde, zu der die Zwischenspeicherung vorgenommen wird:
  - '0' bis '23'
- Minute

  Die Minute, zu der die Zwischenspeicherung vorgenommen wird:
  - '0' bis '59'

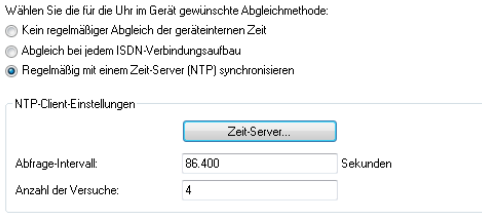
15.4 Zeit-Server für das lokale Netz

Router können hochgenaue Zeitinformationen entweder über ISDN oder über öffentlich zugängliche Zeit-Server im Internet (NTP-Server mit “Open

Access”-Policy, z. B. von der Physikalisch-Technischen Bundesanstalt) beziehen. Die so ermittelte Zeit stellt das Gerät allen Stationen im lokalen Netz zur Verfügung.

15.4.1 Konfiguration des Zeit-Servers unter LANconfig

Damit ein Gerät die aktuelle Zeit im Netzwerk bekannt machen kann, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** den regelmäßigen Abgleich mit einem Zeitserver.



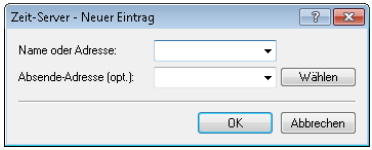
Abfrage-Intervall

Geben Sie hier das Zeitintervall in Sekunden an, nach dem eine Überprüfung und gegebenenfalls Neusynchronisierung der internen Uhr des Gerätes mit einem der angegebenen Zeit-Server (NTP) erfolgen soll.

Anzahl der Versuche

Geben Sie hier an, wie oft das Gerät eine Synchronisation mit dem Zeit-Server versuchen soll. Bei Angabe einer Null versucht das Gerät solange eine Verbindung, bis es eine gültige Synchronisation erreicht hat.

Im Abschnitt **NTP-Einstellungen** konfigurieren Sie anschließend unter **Zeit-Server** die Einstellungen für den Zeitabgleich mit dem entsprechenden Server.



Name oder Adresse

Geben Sie hier einen Zeit-Server (NTP) an, den das Gerät abfragen soll. Der Zeit-Server sollte über eines der vorhandenen Interfaces erreichbar sein.

Die Angabe einer Adresse ist möglich als FQDN, IPv4- oder IPv6-Adresse. Liefert die DNS-Namensauflösung für den Zeit-Server eine IPv6-Adresse zurück, bevorzugt das Gerät diese IPv6-Adresse.

Hinweis: Die Reihenfolge, in der das Gerät mehrere angegebene Zeit-Server abfragt, bestimmen Sie in der Übersicht der Einträge

Absende-Adresse (opt.)

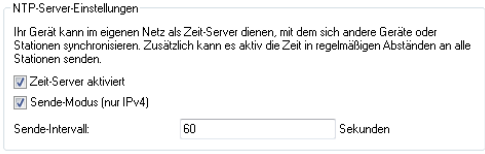
Konfigurieren Sie hier optional eine Absendeadresse, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Falls Sie z. B. Loopback-Adressen konfiguriert haben, geben Sie diese hier als Absendeadresse an.

Hinweis: Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerkes (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IPv4- oder IPv6-Adresse

Mit diesen Einstellungen bezieht zunächst nur das Gerät selbst die Zeit von den öffentlichen Zeitservern. Um die aktuelle Zeit auch im LAN den anderen Geräte bekannt zu machen, aktivieren Sie unter **Datum/Zeit** > **Synchronisierung** im Abschnitt **NTP-Server-Einstellungen** den Zeit-Server im Gerät.



Zeit-Server aktiviert

Aktivieren Sie diese Option, wenn das Gerät als Zeit-Server im Netz funktionieren soll.

Sende-Modus (nur IPv4)

Soll das Gerät regelmäßig als Zeit-Server an alle Stationen im Netz die aktuelle Zeit senden, aktivieren Sie den “Sende-Modus”.

Hinweis: Der Sende-Modus des Gerätes unterstützt nur IPv4-Adressen.

Sende-Intervall

Geben Sie den zeitlichen Abstand in Sekunden an, in welchem der Zeit-Server des Gerätes die aktuelle Zeit an die erreichbaren Stationen im Netz senden soll.

Loopback-Adressen für Zeit-Server

Router können Zeitinformationen u. a. von öffentlich zugänglichen Zeit-Server im Internet (NTP-Server) beziehen. Die so ermittelte Zeit kann das Gerät allen Stationen im lokalen Netz zur Verfügung stellen. Bei der Definition der Zeit-Server können neben den Namen oder IP-Adressen der NTP-Server, von denen der Router die Uhrzeit abfragt, auch Loopback-Adressen angegeben werden.

LANconfig: Datum/Zeit / Synchronisierung / Zeit-Server

WEBconfig: HiLCOS-Menübaum / Setup / NTP / RQ-Adresse

- **Name oder Adresse**

  Name oder IP-Adresse des NTP-Servers. Der Router versucht die Server in der Reihenfolge der Einträge zu erreichen.

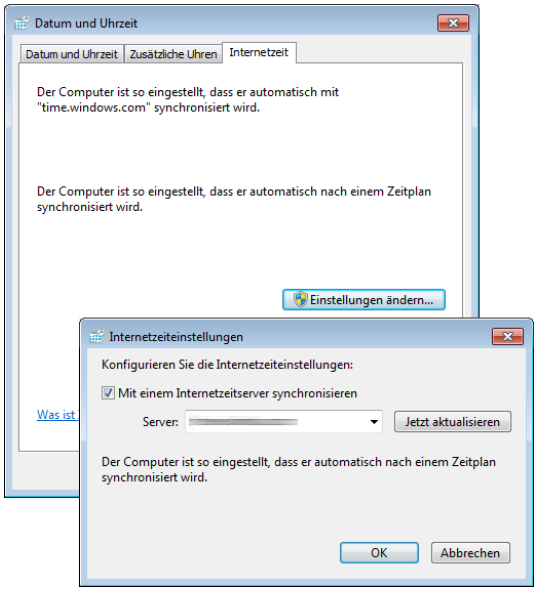
- **Loopback-Adresse**

  Absenderadresse, in der die NTP-Anfrage eingetragen wird und auf der auch die NTP-Antwort erwartet wird.

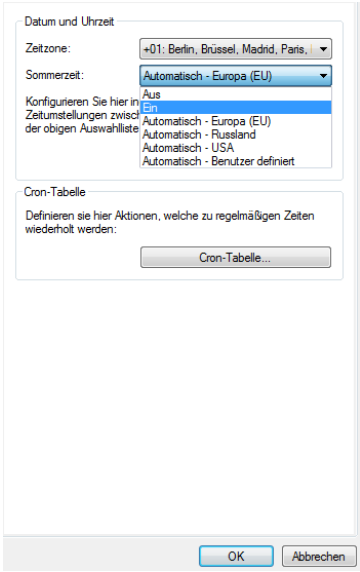
15.4.2 Konfiguration der NTP-Clients

Die NTP-Clients müssen so konfiguriert sein, dass sie die Zeitinformationen des Geräts verwenden. Nicht alle Betriebssysteme verfügen über einen integrierten NTP-Client: Windows XP verfügt über einen solchen, für andere Windows-Betriebssysteme ist ein separater NTP-Client notwendig, bei Linux-Distributionen muss NTP entsprechend mitinstalliert sein.

Die 'Eigenschaften von Datum und Zeit' in einem XP-System werden mit einem Doppelklick auf die Uhrzeit unten rechts im Bildschirm geöffnet. Auf der Registerkarte 'Internetzeit' kann dort der Server zur Synchronisation der Zeit ausgewählt werden.



Das Gerät arbeitet intern mit der koordinierten Weltzeit (UTC). Für Protokollausgaben und zeitbezogene Einstellungen (z. B. cron-Jobs) wird die lokale Uhrzeit verwendet, die über die eingestellte Zeitzone berechnet wird. Zur Berücksichtigung der lokalen Sommerzeit-Einstellungen können die benötigten Anpassungen konfiguriert werden.



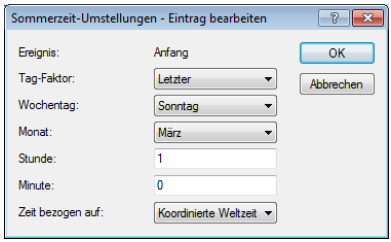
LANconfig: **Datum/Zeit** > **Allgemein**

WEBconfig, Telnet: **HiLCOS-Menübaum** > **Setup** > **Zeit** > **Sommerzeit**

- Sommerzeit
  - Aus: Es wird keine Korrektur der Systemzeit bzgl. der Sommerzeit vorgenommen.
  - Ein: Solange diese Option aktiviert ist, wird statisch eine Stunde zur aktuellen Systemzeit (Gebildet aus UTC und Zeitzone) hinzuaddiert.
  - Automatisch (EU, USA, Russland): In dieser Einstellung wird die Sommerzeit automatisch in Anpassung an die verwendete Zeitzone am Gerätestandort vorgenommen.
  - Automatisch (Benutzerdefiniert): Falls sich das Gerät an einem nicht aufgeführten Standort befindet, können die Optionen für die Sommerzeitumstellung benutzerdefiniert vorgenommen werden.

Benutzerdefinierte Sommerzeitumstellung

Für den Beginn und das Ende der automatischen Sommerzeitumstellung können benutzerdefinierte Werte festgelegt werden.



LANconfig: **Datum/Zeit** > **Allgemein** > **Sommerzeit-Umstellungen**

WEBconfig, Telnet: **HiLCOS-Menübaum** > **Setup** > **Zeit** > **Umstellung-Sommerzeit**

- Tag-Faktor
  - Erster, Zweiter, Dritter, Vierter, Letzter, Zweitletzter, Drittletzter, Viertletzter: An diesem wiederkehrenden Tag des Monats wird die Umstellung ausgeführt.
- Wochentag
  - Montag bis Sonntag: Tag, an dem die Umstellung ausgeführt wird.
- Monat
  - Januar bis Dezember: Monat, an dem die Umstellung ausgeführt wird.
- Stunde
  - 0 bis 23: Stunde, zu der die Umstellung ausgeführt wird.
- Minute
  - 0 bis 59: Minute, zu der die Umstellung ausgeführt wird.
- Zeit bezogen auf
  - Lokale Normalzeit oder UTC: Definiert die Zeitzone, auf die sich die Angaben beziehen.

Hinweis: In der letzten Stunde der Sommerzeit bzw. der darauffolgenden ersten Stunde der Normalzeit besteht eine Mehrdeutigkeit der Uhrzeit. Wird in dieser Zeit die Uhrzeit per ISDN geholt oder manuell gesetzt, wird immer angenommen, dass es sich um eine Zeitangabe gemäß Sommerzeit handelt.

15.5 Scheduled Events

15.5.1 Zeitautomatik für HiLCOS-Befehle

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei **jede** beliebige Kommandozeilenfunktion. Es können damit also alle Features mit einer zeitlichen Steuerung versehen werden.

Anwendungsbeispiele:

- Verbindungsauf- und -abbauten zu bestimmten Zeiten:

  Bei vielen Flatrate-Tarifen für die Internetnutzung wird die Verbindung durch den Provider automatisch nach 24 Stunden “Dauerbetrieb” getrennt. Diese Zwangstrennung kann zu unerwünschten Störungen führen, wenn diese tagsüber zu nicht festgelegten Zeitpunkten stattfindet und dabei VPN-Tunnel abgebaut und die IP-Adresse des Geräts geändert werden. Um die Zwangstrennung zeitlich zu steuern, kann z. B. jede Nacht um 24 Uhr ein manueller Abbau der Internetverbindung angestoßen werden. Die Zwangstrennung erfolgt dann nicht mehr tagsüber zu ungeeigneten Zeitpunkten.

  Als zweites Beispiel können die Geräte in einer verteilten Netzwerkstruktur, die nur über dynamische IP-Adressen verfügen, zu bestimmten Zeitpunkten eine Verbindung zum VPN-Gateway in der Zentrale aufbauen, damit über diese Verbindung Daten sicher aus den Netzen der Filialen ausgelesen werden können. Auf diese Weise ist ein geschützter Zugriff z. B. auf die Kassendaten der Filialen auch ohne ISDN-Verbindungen möglich.

- Ein- und Ausschalten von Firewall-Regeln oder QoS-Regeln

  Die Regeln für Firewall und QoS sind zunächst einmal zeitlich konstant. Je nach Tageszeit oder Wochentag kann es aber sein, dass unterschiedliche Einstellungen in diesem Bereich Sinn machen. Außerhalb der Bürozeiten oder am Wochenende können z. B. andere Prioritäten für die garantierten Bandbreiten gelten als zwischen 9:00 und 17:00 Uhr.

- Durchführung regelmäßiger Firmware- oder Konfigurationsupdates

Die Zeitautomatik erlaubt nicht nur das Setzen einzelner Werte in der Konfiguration, auch das komplette Umschalten auf eine andere Konfiguration ist möglich. Mit dieser Möglichkeit können Sie eine ganze Reihe von Befehlen bündeln und mit einem Kommando ändern. Der Wechsel der Gerätekonfiguration mit vollständig anderen Werten für das Wochenende und wieder zurück in der Nacht zum Montag gelingt so mit einer einzigen Zeile in der Zeitautomatik.

Auch das regelmäßige Update auf die neueste Firmware von einer festen Quelle aus ist so über die Zeitsteuerung zu realisieren.

- E-Mail-Benachrichtigungen

  Mit der Zeitautomatik kann das Gerät nicht nur bei bestimmten Firewall-Ereignissen E-Mails an den Administrator versenden, sondern auch zu festgelegten Zeitpunkten. Die E-Mail kann so z. B. über den erfolgreichen Aufbau der Internetverbindung nach der Zwangstrennung informieren oder nach dem Booten des Gerätes über den Grund des Neustarts informieren.

- Ein- und Ausschalten von Interfaces

  Zu den Möglichkeiten für die Zeitautomatik gehört auch das Ein- und Ausschalten von einzelnen Schnittstellen in festen zeitlichen Intervallen. Damit kann z. B. ein WLAN-Interface nur zu bestimmten Zeiten den drahtlosen Zugang zum Netzwerk erlauben.

- Löschen von bestimmten Tabellen

  Bei manchen Tabellen im HiLCOS macht es Sinn, die Inhalte regelmäßig zu löschen. So können Sie z. B. mit dem monatlichen Löschen der Accounting-Tabelle den Überblick über das jeden Monat verbrauchte Datenvolumen behalten.

15.5.2 CRON-Jobs mit Zeitverzögerung

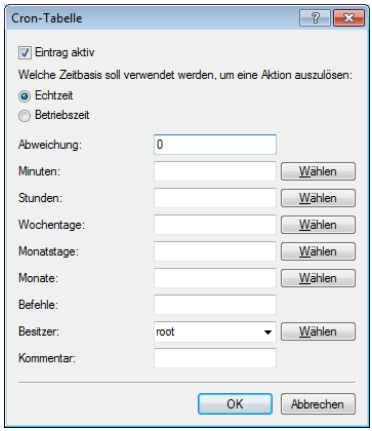
Mit Hilfe von CRON-Jobs lassen sich regelmäßige Aktionen zu bestimmten Zeiten automatisch auf einem Gerät ausführen. Sind in einer Installation sehr viele Geräte aktiv, die zu einem gemeinsamen Zeitpunkt über einen CRON-Job die gleiche Aktion ausführen (z. B. eine Konfiguration per Script aktualisieren), kann das zu unerwünschten Effekten führen, weil z. B. alle Geräte gleichzeitig die VPN-Verbindungen abbauen. Um diesen Effekt zu vermeiden,

können die CRON-Jobs mit einer zufälligen Verzögerungszeit von 0 bis 59 Minuten definiert werden.

15.5.3 Konfiguration der Zeitautomatik

Das folgende Tutorial zeigt Ihnen, wie Sie einen neuen CRON-Job anlegen und welche Parameter Ihnen dabei zur Verfügung stehen.

1. Öffnen Sie in LANconfig die manuelle Konfiguration für Ihr Gerät.
2. Öffnen Sie die **Cron-Tabelle** im Dialog **Datum/Zeit** > **Allgemein** und klicken Sie **Hinzufügen**, um einen neuen CRON-Job zu erstellen.



3. Geben Sie eine Zeitbasis an.
   Die Zeitbasis bestimmt, ob HiLCOS die zeitliche Steuerung der künftigen Aktion auf Grundlage der Echtzeit oder der Systemlaufzeit des Gerätes ausführt. In der Einstellung **Echtzeit** wertet das System sämtliche Zeit- und Datumsangaben aus. In der Einstellung **Betriebszeit** wertet das System nur die Minuten- und Stundenangaben seit dem letzten Gerätestart aus.
4. Geben Sie unter **Abweichung** eine Zeit in Minuten an, um welche die Ausführung eines CRON-Jobs gegenüber der festgelegten Startzeit maximal verzögert wird.
   Die tatsächliche Verzögerungszeit erkennt das Gerät zufällig; sie liegt zwischen Null und der hier eingetragenen Zeit. Bei einer Variation von Null wird der CRON-Job exakt zur festgelegten Zeit ausgeführt.

Hinweis: Echtzeit-basierte Regeln sind ausschließlich dann ausführbar, wenn Ihr Gerät über einen gültigen Zeitbezug verfügt, also z. B. via NTP.

5. Geben Sie den/die Minute(n), Stunde(n), Wochentag(e), Monatstag(e) und Monat(e), an denen Ihr Gerät das festgelegte Kommando ausführt.

   Wenn Sie keinen Wert eingeben, zieht Ihr Gerät den betreffenden Zeitwert auch nicht in die Steuerung mit ein. Für jeden Parameter haben Sie optional auch die Möglichkeit, eine kommaseparierte Liste von Werten oder einen Wertebereich (in Form von als `<Min.>-<Max.>`) anzugeben.

   Die Syntax des Feldes **Wochentage** entspricht dabei der üblichen CRON-Interpretation:

Sonntag	Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag
0	1	2	3	4	5	6

   Hinweis: Das Wochentagsfeld ist auch für Regeln bedeutend, die auf die Betriebszeit bezogen sind. Das ist sinnvoll für Aktionen, die Sie nur einmal beim Start des Gerätes (also bei Null Tagen Betriebszeit) ausführen. So gleichen Sie z. B. den Wochentag gegen die Tage der Betriebszeit ab.

6. Geben Sie unter **Befehle** das auszuführende Kommando oder eine kommaseparierte Liste von Kommandos ein.
   Ausgeführt werden kann **jede** beliebige Kommandozeilenfunktion.
7. Geben Sie den **Besitzer** des CRON-Jobs an.
   Als Besitzer lässt sich ein im Gerät definierter Administrator auswählen. Sofern ein Besitzer angegeben ist, werden die Befehle des Cron-Jobs mit den Rechten des Besitzers ausgeführt.
8. Geben Sie im Feld **Kommentar** eine kurze Beschreibung zu dem CRON-Job ein.
9. Klicken Sie **OK**, um den Eintrag zu speichern. Schreiben Sie anschließend die Konfiguration zurück auf das Gerät.

Weitere Konfigurationsbeispiele:

Zeitbasis	*Min.*	*Std.*	*W.-Tage*	*M.-Tage*	*Monate*	*Befehl*
Echtzeit	0	4	0-6	1-31	1-12	do /so/man/abbau internet
Echtzeit	59	3	0-6	1-31	1-12	mailto:admin@beispiel.de?subject=Zwangstrennung?body=Manuelles Trennen der Internetverbindung
Echtzeit	0	0		1		do /setup/accounting/loeschen
Echtzeit	0	18	1,2,3,4,5			do /so/man/aufbau ZENTRALE

- Der erste Eintrag trennt jeden Morgen um 4:00 Uhr die Verbindung zum Internetprovider (Zwangstrennung).
- Der zweite Eintrag sendet jeden Morgen um 3:59 Uhr, also kurz vor der Zwangstrennung, eine Info-Mail an den Admin.
- Der dritte Eintrag löscht an jedem 1. eines Monats die Accounting-Tabelle.
- Der vierte Eintrag baut an jedem Werktag um 18:00 Uhr eine Verbindung zur Zentrale auf.

Wichtig: Das Gerät führt zeitgesteuerte Regeln mit einer Genauigkeit von einer Minute aus. Bitte achten Sie darauf, dass die Sprache der eingetragenen Befehle zur eingestellten Konsolensprache passt, da das Gerät ansonsten die Kommandos der Zeitautomatik ignoriert.

15.6 PPPoE-Server

15.6.1 Einleitung

Im Zuge der DSL-Verbreitung sind mittlerweile in allen Betriebssystemen PPPoE-Clients integriert oder verfügbar. Diese können für eine „Anmeldung am Netzwerk“ sowie eine damit einhergehende Zugriffsrechteverwaltung auf Dienste wie Internet, E-Mail oder bestimmte Gegenstellen benutzt werden.

PPPoE ist nur auf einem Netzwerksegment einsetzbar

PPPoE ist als so genannte „Layer-2“-Technologie nur innerhalb eines Netzwerksegments einsetzbar, d.h. nicht über IP-Subnetze hinweg. Die PPPoE-

Verbindung kann nicht über die Grenzen des Netzwerksegments, also z. B. über einen Router, hinaus aufgebaut werden.

Nach dem Einloggen eines Benutzers im LAN (z. B. Username: 'Einkauf', Password: 'geheim') über eine vorgeschriebene PPPoE-Anmeldung können weitere Rechte über die Firewall geregelt werden. Dabei wird der PPPoE-Benutzername als 'Gegenstelle' in der Firewall eingetragen. Mit einer Deny-All-Regel und einer PPPoE-Regel der folgenden Form kann dem Benutzer Mustermann die Nutzung des Internets mit Web und FTP erlaubt werden:

- Quelle: Mustermann
- Ziel: alle Stationen
- Dienste: WWW, FTP

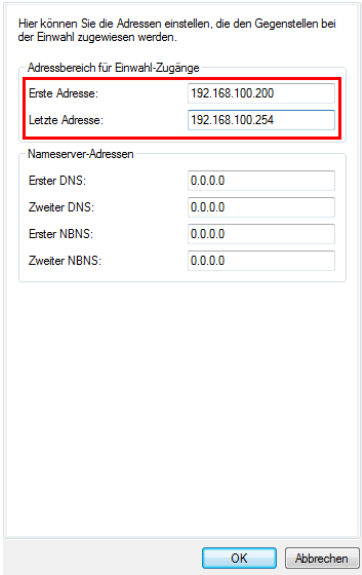
15.6.2 Anwendungsbeispiel

Alle Mitarbeiter der Abteilung 'Einkauf' müssen sich per PPPoE erst am Gerät authentisieren (IP-Routing, Prüfung mit PAP), damit sie auf das Internet zugreifen dürfen.

Randbedingung: Das Gerät ist als Router, Firewall und Gateway für die Benutzer im LAN direkt zu erreichen, d. h. es sind keine weiteren Router dazwischengeschaltet.

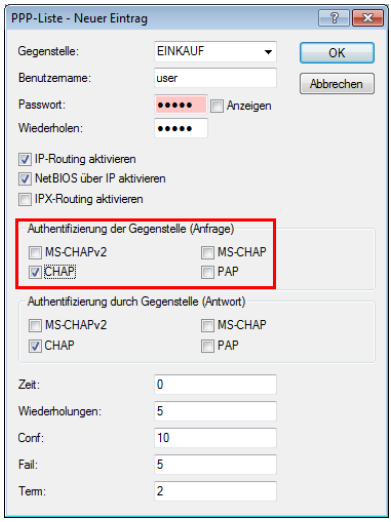
Die Rechner im Einkauf bekommen über die Liste der Adressen für Einwahlzugänge (LANconfig / TCP/IP / Adressen) eine IP-Adresse aus einem bestimmten Adressbereich zugewiesen (z. B. 192.168.100.200 bis 192.168.100.254).

Hinweis: Das Gerät selbst steht dabei in einem anderem IP-Adressbereich!

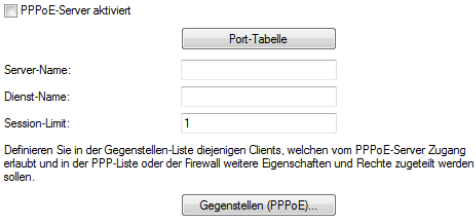


Damit die Anwender die Authentifizierung nicht umgehen können, wird in der Firewall eine DENY-ALL-Regel angelegt, die alle lokalen Verbindungen unterbindet.

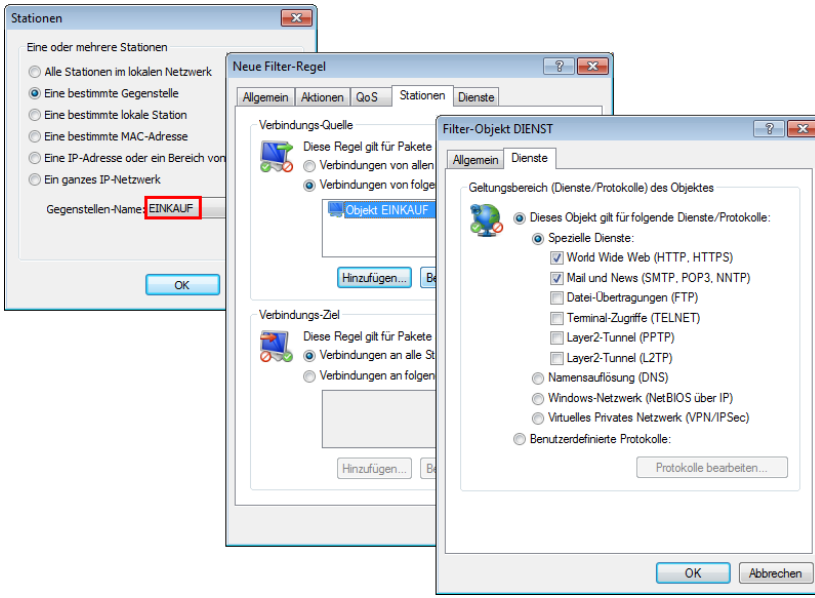
Dazu wird der Benutzer 'Einkauf' als Gegenstelle ohne Benutzername, aber mit einem gemeinsamen Kennwort für alle Mitarbeiter in der Abteilung in der PPP-Liste angelegt (LANconfig / Kommunikation / Protokolle) und die Authentifizierung (verschlüsselt) über CHAP vorgegeben. Für diesen PPP-Benutzer werden sowohl IP-Routing als auch NetBIOS (Windows Networking) aktiviert:



Neben der Aktivierung des PPPoE-Servers (LANconfig / Kommunikation / Allgemein) können weitere Einschränkungen (z. B. auf die erlaubten MAC-Adressen) ebenfalls im PPPoE-Server definiert werden. Dieses Beispiel nutzt aber den dort vorhandenen Eintrag 'DEFAULT' mit der MAC-Adresse '00.00.00.00.00.00', so dass alle MAC-Adressen erlaubt sind.

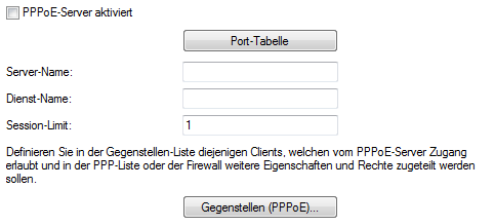


Mit Hilfe der Firewall (LANconfig / Firewall/QoS / Regeln) können die erlaubten Dienste für die Mitarbeiter des Einkaufs gesteuert werden (z. B. nur Freischalten von HTTP und EMAIL).



15.6.3 Konfiguration

Die Einstellungen für den PPPoE-Server nehmen Sie in LANconfig unter **Kommunikation** > **Allgemein** vor.



In dieser Ansicht haben Sie folgende Konfigurationsmöglichkeiten:

PPPoE-Server aktiviert

Über diese Einstellung schalten Sie den PPPoE-Server global ein- oder aus.

Port-Tabelle

Über diese Tabelle lässt sich der PPPoE-Server für jede physikalische sowie logische Schnittstelle getrennt aktivieren oder deaktivieren.

Server-Name

Über dieses Eingabefeld haben Sie optional die Möglichkeit, dem PPPoE-Server einen eigenen Namen unabhängig vom Gerätenamen zuzuweisen (AC-Name = Access Concentrator Name). Sofern Sie dieses Feld leer lassen, verwendet der PPPoE-Server den Gerätenamen als Server-Namen.

Dienst-Name

In diesem Eingabefeld tragen Sie den Namen des angebotenen Dienstes ein. Der Dienst-Name ermöglicht einem PPPoE-Client die Auswahl eines bestimmten PPPoE-Servers. Dazu konfigurierenn Sie den Dienst-Namen direkt auf dem Clients.

Session-Limit

Über diese Einstellung geben Sie an, wie oft ein Client mit der gleichen MAC-Adresse gleichzeitig angemeldet sein kann. Ist das Limit erreicht, antwortet der Server nicht mehr auf empfangene Anfragen des Clients. Ein Session-Limit von `0` steht für eine unbegrenzte Session-Anzahl.

Gegenstellen (PPPoE)

Über diese Tabelle definieren Sie die einzelnen Clients, denen der PPPoe-Server den Zugang zu den gewünschten Diensten (wie Internet, E-Mail) oder bestimmten Gegenstellen erlaubt.

Hinweis: Die **MAC-Adresse** `000000000000` erlaubt einer Gegenstelle, sich mit einer beliebigen MAC-Adresse am Gerät anzumelden. Ist eine spezifische MAC-Adresse eingetragen, so wird die PPP-Verhandlung abgebrochen, wenn sich der User von einer anderen MAC-Adresse anmeldet.

Hinweis: Nach der Anmeldung versucht das Gerät, die **Haltezeit** der Gegenstelle zu setzen. Existiert kein Eintrag, so verwendet das Gerät die Gegenstelle `DEFAULT`.

Zusätzlich zu dieser Tabelle müssen Sie für die Benutzer einen Eintrag in der PPP-Tabelle vornehmen, in welchem Sie das Passwort, die Rechte

(IP, IPX, NetBIOS) und sonstige PPP-Parameter (LCP-Polling etc.) hinterlegen. Alternativ haben Sie auch die Möglichkeit, die Benutzer über einen RADIUS-Server zu authentifizieren. Dazu konfigurieren Sie den Server unter **Kommunikation** > **RADIUS** > **Authentifizierung über RADIUS für PPP und CLIP** und setzen dessen Betriebsart auf **Exklusiv** (ausschließlich RADIUS) oder **Aktiv** (gemischte Datenhaltung RADIUS/PPP-Tabelle).

15.6.4 PPPoE-Snooping

Das PPPoE-Snooping ermöglicht Geräten, die PPPoE-Discovery-Pakete (PPPoED) empfangen und weiterleiten, diese Datenpakete zu analysieren und mit zusätzlichen Informationen zu versehen. Diese Informationen ermöglichen es einem PPPoE Access Concentrator (AC), die PPPoED-Datenpakete entsprechend zu verarbeiten. Diese Rolle wird als “PPPoE-Intermediate-Agent” bezeichnet.

PPPoE-Snooping im HiLCOS verarbeitet die folgenden PPPoED-Pakete:

- PADI (PPPoE Active Discovery Indication)
- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

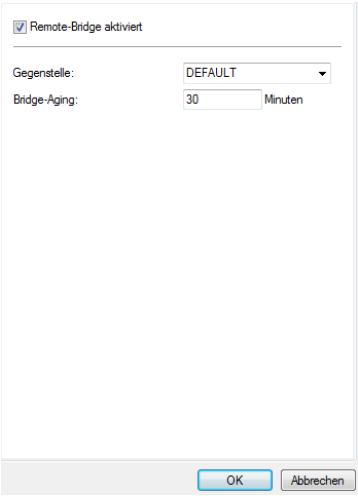
Der für das PPPoE-Snooping zuständige PPPoE Intermediate Agent erweitert das PPPoED-Paket um Hersteller spezifische Attribute (Circuit-ID und Remote-ID) oder ersetzt diese IDs durch eigene Werte, falls sie bereits im empfangenen Datenpaket enthalten sind.

- Remote-ID: kennzeichnet eindeutig den Client, der einen PPPoE-Request stellt.
- Circuit-ID: kennzeichnet eindeutig die Schnittstelle, über die ein Client einen PPPoE-Request stellt.

Die Konfiguration von PPPoE-Snooping erfolgt pro LAN/WLAN-Schnittstelle.

15.7 Remote-Bridge

Über die Remote-Bridge werden zwei entfernte Netzwerke so miteinander gekoppelt, als wären sie physikalisch verbunden. Sie sind völlig unabhängig von den eingesetzten Netzwerkprotokollen.



Konfigurationstool	*Aufruf*
LANconfig	Bridge / Allgemein
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Bridge

- Gegenstelle

  Name der Gegenstelle, an welche die Remote-Bridge gebunden ist

- Bridge-Aging

  Zeit nach der eine einmal gelernte MAC-Adresse wieder gelöscht wird

- Schnittstellen-Zuordnung

  Logisches Interface, dem die Remote-Bridge zugeordnet wird.

  Hinweis: Bei der Schnittstellenzuordnung sind WLANs nicht möglich, da die WAN-Bridge nur in Geräten ohne WLAN vorhanden ist. Daher ist auch die Schnittstellenzuordnung "beliebig" nicht möglich.

- VLAN-ID

  ID des VLANs, auf dem die Remote-Bridge aktiv sein soll.

15.8 L2-Firewall

Service-Techniker erledigen Wartungs- und Diagnosetätigkeiten vermehrt mit mobilen Geräten. Im folgenden Beispiel nutzt der Service-Techniker ein Tablet zur Wartung von Sensoren in einem Ethernet basierten Maschinennetz. Der WLAN-Zugriff auf das Maschinennetz erfolgt über einen als AP konfigurierten OpenBAT. Das Anschließen eines APs an das Maschinennetz eröffnet potentiellen Angreifern allerdings die Möglichkeit, unbefugte Aktionen im Maschinennetz durchzuführen. Hirschmann unterstützt Sie mit der L2-Firewall bei der Abwehr solcher Bedrohungen. Den verschiedenen Applikationen im Maschinennetz können unterschiedliche vom OpenBAT aufgespannte logische WLAN-Netzwerke zugeordnet werden. Über diese Zuordnung lässt sich der Zugriff einschränken. Die L2-Firewall bietet Ihnen die Möglichkeit, für beliebige logische WLAN- und LAN-Schnittstellen, die einer Bridge-Gruppe zugeordnet sind, eigene Firewall-Regeln festzulegen. Bezogen auf das obige Beispiel bedeutet das, dass der Administrator festlegt, auf welche Sensoren der Service-Techniker zugreifen darf und welche Firewall-Regeln diesen Zugriff einschränken.

15.8.1 L2-Firewall Funktionen

Die L2-Firewall ist auf Layer 2 an der Bridge zwischen den logischen Schnittstellen angesiedelt und auch in der Lage, auf Grundlage der Protokolle von Layer 3 und Layer 4 zu filtern. Sie ist als Stateful-Firewall ausgelegt und unterstützt folgende Protokolle:

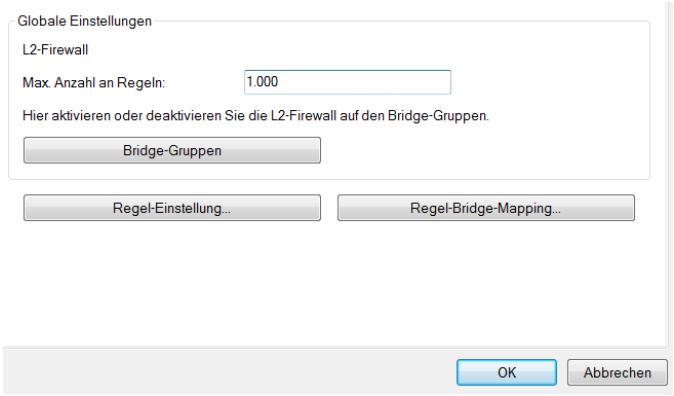
- IPv4
- ICMP
- TCP
- UDP

Die L2-Firewall bietet Ihnen die Möglichkeit, Regeln festzulegen. Anschließend können Sie die Regeln auf den Bridges mappen.

15.8.2 Tutorial: Konfiguration der L2-Firewall

Um die L2-Firewall zu aktivieren und zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie in die Ansicht **Firewall/QoS** > **L2-Firewall.**



2. Legen Sie die **Max. Anzahl an Regeln fest.**
3. Aktivieren Sie die L2-Firewall auf den gewünschten **Bridge-Gruppen**.
4. Legen Sie die **Regel-Einstellung fest**.
5. Legen Sie das **Regel-Bridge-Mapping fest**.
6. Klicken Sie **OK**.

Sie haben die L2-Firewall aktiviert und konfiguriert.

15.9 RADIUS

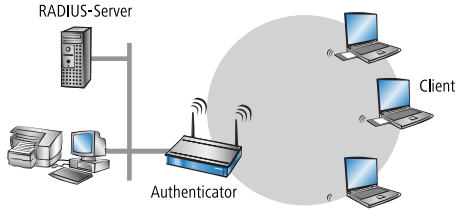
RADIUS steht für „Remote Authentication Dial-In User Service“ und wird als „Triple-A-Protokoll“ bezeichnet. Dabei stehen die drei „A“ für

- Authentication (Authentifizierung)
- Authorization (Autorisierung)
- Accounting (Abrechnung)

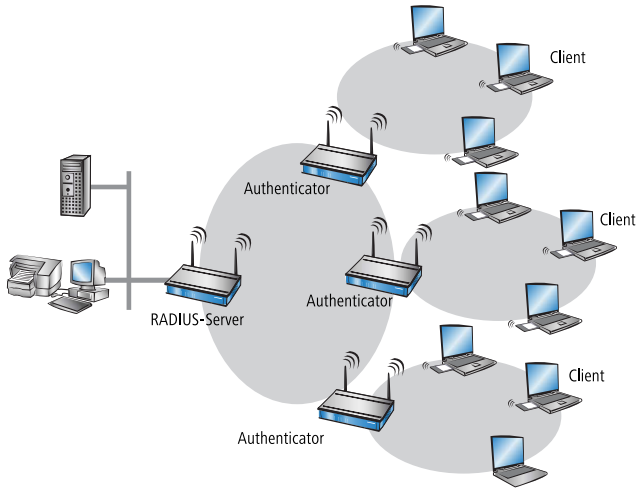
Sie können mit diesem Protokoll Benutzern Zugang zu einem Netz gewähren, ihnen bestimmte Rechte zuweisen und ihre Aktionen verfolgen. Gegebenenfalls können Sie auch die in Anspruch genommenen Leistungen gegenüber dem Benutzer mit Hilfe des RADIUS-Servers abrechnen (z. B. bei WLAN Hotspots). Für jede Aktion, die vom Benutzer durchgeführt wird, kann der RADIUS-Server eine Autorisierung durchführen, und so den Zugriff auf Netzwerkressourcen je nach Benutzer freigeben oder sperren.

Damit RADIUS funktioniert, sind 3 verschiedene Geräte nötig.

- Client: Das ist ein Gerät (PC, Notebook etc.) über das der Benutzer sich in das Netz einwählen möchte
- Authenticator: Eine Netzwerkkomponente, welche die Authentifizierung weiterleitet und zwischen dem Netz und dem Client liegt. Diese Aufgabe kann z. B. ein Access Point übernehmen. Der Authenticator wird auch als Network Access Server (NAS) bezeichnet.



- Authentication-Server: RADIUS-Server, auf dem die Daten für die Benutzer konfiguriert sind. Dieser steht gewöhnlich in dem Netz, für das er Zugangsberechtigungen erteilen soll. Er ist für den Client über den Authenticator erreichbar. Auch für diese Aufgabe kann in entsprechenden Szenarien ein Access Point eingesetzt werden.



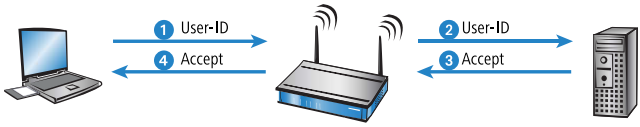
Der Authenticator hat zunächst keine Informationen über die Clients, die sich anmelden wollen. Diese sind alle in einer Datenbank des RADIUS-Servers gespeichert. Welche Anmeldeinformationen der RADIUS-Server für die Authentifizierung benötigt, ist dort in der Datenbank hinterlegt und kann von Netzwerk zu Netzwerk variieren. Der Authenticator hat nur die Aufgabe, die Informationen zwischen dem Client und dem RADIUS-Server zu übertragen.

Der Zugang zu einem RADIUS-Server kann über verschiedene Wege aufgebaut werden:

- Über PPP bei der Einwahl in ein Netzwerk
- Über WLAN
- Über einen Public Spot für Benutzer, die sich per Browser anmelden
- über das 802.1x-Protokoll

15.9.1 Funktionsweise von RADIUS

Die Authentifizierung eines Clients mit Hilfe eines Authenticators an einem RADIUS-Server kann je nach Implementation unterschiedlich detailliert ablaufen. In einem einfachen Anwendungsfall schickt der Client seine Anmeldedaten über den Authenticator an den RADIUS-Server und erhält von dort eine Bestätigung („Accept“) oder eine ablehnende Fehlernachricht („Reject“).



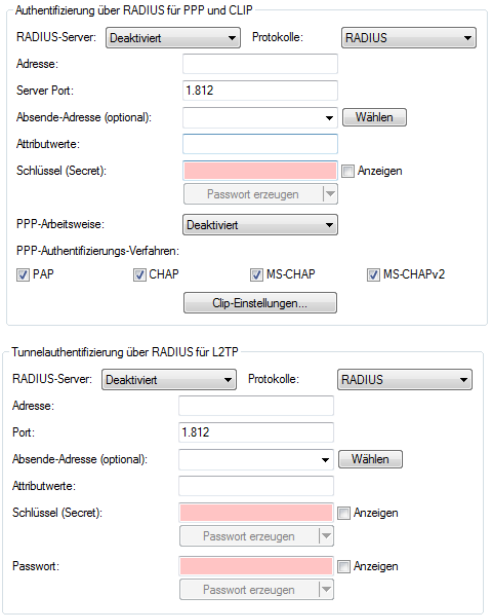
In erweiterten Anwendungen kann der RADIUS-Server mit Hilfe einer so genannten „Challenge“ weitere Anmeldeinformationen anfordern, die Verhandlungsphase sieht dann z. B. so aus:

15.9.2 Konfiguration von RADIUS als Authenticator bzw. NAS

Das RADIUS-Protokoll wird von den Geräten in unterschiedlichen Anwendungsfällen unterstützt. Für jeden dieser Fälle gibt es einen eigenen Satz von Parametern, der unabhängig von den anderen Anwendungen konfiguriert werden kann. Zusätzlich gibt es allgemeine Parameter, die für jede dieser Anwendungen konfiguriert werden müssen. Nicht alle Geräte unterstützen jede Anwendung.

Allgemeine Einstellungen

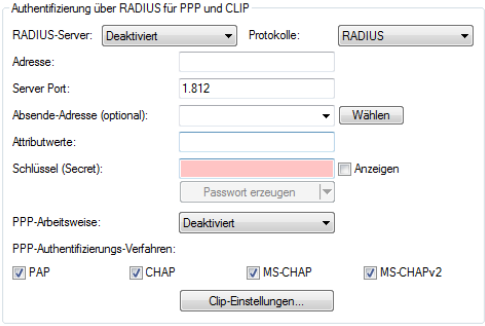
Die allgemeinen Einstellungen unter **Kommunikation** > **RADIUS** gelten für alle RADIUS-Anwendungen. Die Default-Werte sind so gewählt, dass sie im Normalfall nicht geändert werden müssen.



Hinweis: Die Angabe einer RADIUS-Serveradresse ist als IPv4- oder IPv6-Adresse sowie alternativ als DNS-Name möglich.

Einwahl über PPP und RADIUS

Bei der Einwahl über das PPP-Protokoll (Point-to-Point-Protocol) kann die Zugangsberechtigung der Clients mittels RADIUS geprüft werden. Ein Client kann sich dabei von einem beliebigen Ort in das Netz einwählen. Die anschließende Datenübertragung zwischen dem Client und dem Authenticator wird verschlüsselt



Die Konfiguration erfolgt im LANconfig unter **Kommunikation** > **RADIUS**.

Radius-Server

Bei der Authentifizierung via RADIUS wird die Benutzerverwaltung und Authentifizierung von einem RADIUS-Server übernommen.

- Deaktiviert: Die RADIUS-Funktion ist ausgeschaltet, es werden keine Anfragen an den RADIUS-Server weitergeleitet (Default).
- Aktiviert: Die RADIUS-Funktion ist eingeschaltet, es können Anfragen an den konfigurierten RADIUS-Server weitergeleitet werden. Je nach Einstellung können auch andere Quelle für die Authentifizierung verwendet werden (z. B. PPP-Liste).
- Exklusiv: Die RADIUS-Funktion ist eingeschaltet, die Authentifizierung wird ausschließlich über RADIUS durchgeführt.

Für die Nutzung der RADIUS-Funktion muss der entsprechende RADIUS-Server konfiguriert sein. Alle Benutzerangaben wie Benutzername und Passwort werden im RADIUS-Server eingetragen.

Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren (Default: 1.812).

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten

Schrägstrich vorangestellt (\"), der umgekehrte Schrägstrich ebenfalls (\\).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Shared-Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

PPP-Arbeitsweise

Bei der Einwahl über PPP kann ein RADIUS-Server zur Authentifizierung genutzt werden.

- Deaktiviert: PPP-Clients werden nicht über RADIUS authentifiziert, sie werden **ausschließlich** anhand der PPP-Liste geprüft (Default).
- Aktiviert: Die RADIUS-Authentifizierung für PPP-Clients ist eingeschaltet. Die von den Clients gelieferten Benutzerdaten werden **zuerst** über die PPP-Liste geprüft. Ist in der PPP-Liste kein passender Eintrag vorhanden, dann wird der Client über den RADIUS-Server geprüft. Verläuft die Prüfung in PPP-Liste **oder** RADIUS-Server positiv, ist die Authentifizierung erfolgreich.

- Exklusiv: Die RADIUS-Authentifizierung für PPP-Clients ist eingeschaltet. Die von den Clients gelieferten Benutzerdaten werden **ausschließlich** über den RADIUS-Server geprüft. In dieser Einstellung werden lediglich die erweiterten Einstellungen der PPP-Liste für den Benutzer ausgewertet (z. B. Prüfung nach PAP/CHAP bzw. die erlaubten Protokolle IP, IPX und/oder NetBIOS).

CLIP-Arbeitsweise

Bei der Einwahl über PPP kann zur Steuerung eines Rückrufs ein RADIUS-Server genutzt werden.

- Deaktiviert: Die Rückruf-Funktion wird nicht über RADIUS gesteuert, es werden **ausschließlich** die Einträge der Namenliste verwendet (Default).
- Aktiviert: Die RADIUS-Funktion für den Rückruf ist eingeschaltet. Die von den Clients gemeldete Rufnummer wird **zuerst** über die Namenliste geprüft. Ist in der Namenliste kein passender Eintrag vorhanden, dann wird die Rufnummer über den RADIUS-Server geprüft. Verläuft die Prüfung in Namenliste **oder** RADIUS-Server positiv, kann ein Rückruf aufgebaut werden.

  Hinweis: Wenn die übermittelte Rufnummer in der Namenliste enthalten ist, dort aber kein Rückruf aktiv ist, erfolgt keine weitere Prüfung über RADIUS.

- Exklusiv: Die RADIUS-Funktion für den Rückruf ist eingeschaltet. Die von den Clients gemeldete Rufnummer wird **ausschließlich** über den RADIUS-Server geprüft.

Zur Nutzung der Rückrufsteuerung über RADIUS muss im RADIUS-Server für jede zu authentifizierende Rufnummer ein Benutzer angelegt werden, dessen Name der Rufnummer entspricht, und der als Passwort das hier angegebene CLIP-Passwort hat.

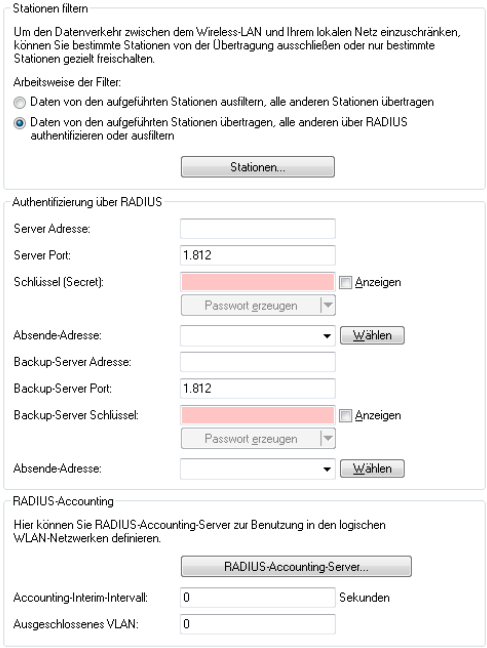
CLIP-Passwort

Passwort für die Rückrufsteuerung.

Hinweis: Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden. Sie sind bei PPP auf der gleichen Seite wie die PPP-Parameter zu finden.

Einwahl über WLAN und RADIUS

Bei der Verwendung eines RADIUS-Servers zur Authentifizierung von WLAN-Clients prüft der RADIUS-Server die Berechtigungen der Clients über die MAC-Adresse.



Hinweis: Zur Nutzung der RADIUS-Funktion für WLAN-Clients muss für den Parameter „Stationen filtern“ die Option „Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren“ ausgewählt sein.

Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **Stationen**.

Server-Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren (Default: 1.812).

Schlüssel (Shared-Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Backup-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des Backup-RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Backup-Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem Backup-RADIUS-Server kommunizieren (Default: 1.812).

Backup-Server Schlüssel

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im Backup-RADIUS-Server konfiguriert sein.

Hinweis: Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden .

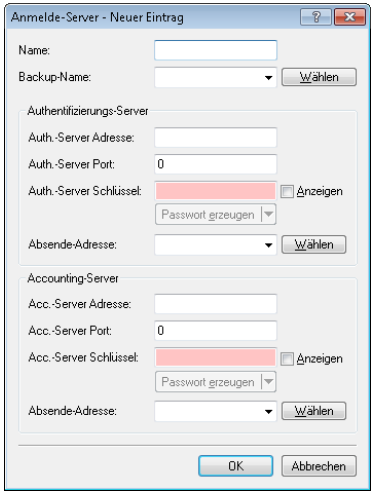
Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Einwahl über einen Public Spot und RADIUS

Bei der Konfiguration eines Public-Spot (Aktivierung über Software-Option für die Access Points) können die Benutzer-Anmeldedaten an einen oder mehrere

RADIUS-Server weitergeleitet werden. Diese werden in der Anbieter-Liste konfiguriert. Welche Anmeldedaten die einzelnen RADIUS-Server von den Clients benötigen, ist für den Access Point nicht wichtig, da diese Daten transparent an den RADIUS-Server weitergereicht werden.



Die Konfiguration erfolgt im LANconfig unter **Public-Spot** > **Benutzer** > **Anmelde-Server**.

Name

Name des Anbieters, für den der RADIUS-Server definiert werden soll.

Backup-Name

Als Backup kann der Name eines anderen Anbieters aus der aktuellen Tabelle ausgewählt werden. Durch solche Einträge können komfortabel Backup-Ketten von mehreren RADIUS-Servern konfiguriert werden.

Hinweis: Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden.

Auth.-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers für diesen Anbieter an.

Auth.-Server Port

Der Port, über den der Access Point mit dem RADIUS-Server für diesen Anbieter kommunizieren kann.

Auth. Server Schlüssel

Schlüssel (Shared Secret) für den Zugang zum RADIUS-Server des Anbieters. Der Schlüssel muss ebenfalls im entsprechenden RADIUS-Server konfiguriert sein.

Acc.-Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Accounting-Servers für die Zugänge zum Public-Spot an.

Acc.-Server Port

Der Port, über den der Access Point mit dem Accounting-Server kommunizieren kann.

Acc.-Server Schlüssel

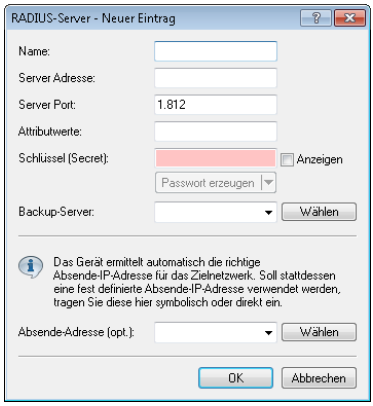
Schlüssel (Shared Secret) für den Zugang zum Accounting-Server. Der Schlüssel muss ebenfalls im Accounting-Server konfiguriert sein.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Einwahl über 802.1x und RADIUS

WLAN-Clients können sich über das 802.1x-Protokoll in ein Netzwerk anmelden. Der Access Point kann die Anmeldung über dieses Protokoll an den RADIUS-Server weiterleiten. Die MAC-Adresse wird zur Identifizierung der Benutzer verwendet.



Die Konfiguration erfolgt im LANconfig unter **Wireless-LAN** > **802.1X** > **RADIUS-Server**.

Name

Geben Sie jedem RADIUS-Server einen in dieser Tabelle eindeutigen Namen. Der Name 'DEFAULT' ist reserviert für alle WLAN-Netze, deren Authentifizierung nach IEEE 802.1x erfolgt, und die keinen eigenen RADIUS-Server angegeben haben.

Jedem WLAN-Netz, dessen Authentifizierung nach IEEE 802.1x erfolgt, kann im Feld 'Schlüssel 1/Passphrase' ein eigener RADIUS-Server zugewiesen werden, indem dort der hier definierte Name eingesetzt wird.

Server Adresse

Geben Sie hier die IP-Adresse (IPv4, IPv6) oder den Host-Namen des RADIUS-Servers an, mit dem Sie zentral die Benutzer verwalten.

Server Port

Geben Sie hier den Port an, über den Sie mit Ihrem RADIUS-Server kommunizieren.

Attributwerte

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Schlüssel (Shared-Secret)

Geben Sie hier den Schlüssel an, mit dem die Kodierung der Daten vorgenommen werden soll. Der Schlüssel muss ebenfalls im RADIUS-Server konfiguriert sein.

Backup-Server

Namen des Backup-Servers aus der Liste der bisher konfigurierten RADIUS-Server.

Hinweis: Die allgemeinen Werte für Wiederholung und Timeout müssen ebenfalls konfiguriert werden.

Im RADIUS-Server müssen die WLAN-Clients folgendermaßen eingetragen sein:

Der Benutzername ist die MAC-Adresse im Format AABBCC-DDEEFF. Das Passwort ist für alle Benutzer identisch mit dem Schlüssel (Shared-Secret) für den RADIUS-Server.

Absende-Adresse

Das Gerät ermittelt automatisch die richtige Absende-IP-Adresse für das Zielnetzwerk. Wollen Sie stattdessen eine fest definierte Absende-IP-Adresse verwenden, tragen Sie diese symbolisch oder direkt hier ein.

Zusätzliche Source-Ports für Access-Requests

Der RADIUS-Client nutzt einen Source-Port (UDP-Listener) zur Verhandlung von Access-Requests mit dem RADIUS-Server. Dieser Port ermöglicht die gleichzeitige Verhandlung von bis zu 256 IDs. Bei vielen Anfragen und gleichzeitig weit entferntem RADIUS-Server ist es möglich, dass alle 256 Access-Requests gleichzeitig offen sind und der RADIUS-Client entsprechend keine weitere Anfrage annehmen würde. Das kommt z. B. in umfangreichen Eduroam-Umgebungen vor.

In diesem Fall öffnet der RADIUS-Client den nächsthöheren Source-Port und ermöglicht die Access-Request-Verhandlung weiterer IDs. Das geschieht automatisch und ist nicht konfigurierbar.

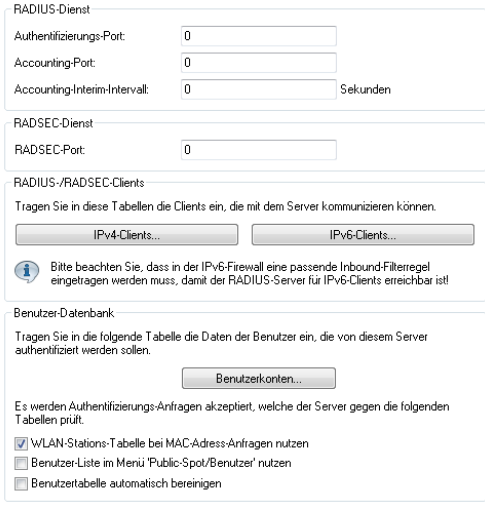
15.9.3 Konfiguration von RADIUS als Server

Neben der Funktion als RADIUS-Authenticator oder NAS kann ein Access Point auch als RADIUS-Server arbeiten. In dieser Betriebsart stellt das Gerät seine eigenen Informationen über die anmeldeberechtigten Benutzer den anderen Access Points im Authenticator-Modus zur Verfügung.

Parameter des RADIUS-Servers

Die Konfiguration des RADIUS-Servers beinhaltet, welcher Authenticator auf den RADIUS-Server zugreifen darf, welches Kennwort er für diesen Zugang benötigt und über welchen offenen Port er mit dem RADIUS-Server kommunizieren kann. Der Authentifizierungs-Port gilt dabei global für alle Authenticatoren.

Die Konfiguration des Servers erfolgt über **RADIUS-Server** > **Allgemein**



Authentifizierungs-Port

Geben Sie hier den TCP-Port an, über den die Authenticator mit dem RADIUS-Server im Access Point kommunizieren. Üblicherweise ist das der Port '1812'.

Der Port '0' deaktiviert den RADIUS-Server (Default-Einstellung).

Accounting-Port

Geben Sie hier den TCP-Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise ist das der Port '1813'.

Accounting-Interim-Intervall

Geben Sie hier an, welchen Wert der RADIUS-Server bei erfolgreicher Authentifizierung als Accounting-Interim-Intervall ausgeben soll. Sofern das anfragende Gerät dieses Attribut unterstützt, steuert dieser Wert, in welchem Intervall (in Sekunden) der Accounting-RADIUS-Server ein Update der Accounting-Daten erhält.

RADSEC-Port

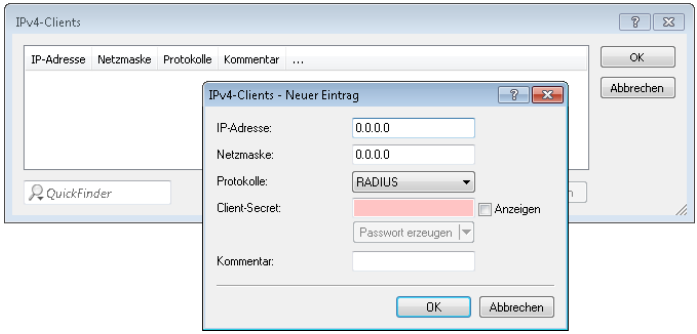
Geben Sie hier an, über welchen TCP-Port der Server über RADSEC verschlüsselte Accounting- oder Authentifizierungs-Anfragen annimmt. Üblicherweise ist das der Port '2083'.

Der Port '0' deaktiviert den RADSEC-Dienst im Gerät (Default-Einstellung).

RADIUS-/RADSEC-Clients

Tragen Sie in diese Tabellen die Clients ein, die mit dem Server kommunizieren können. Verwenden Sie je Netzwerkprotokoll die entsprechende Tabelle.

IPv4-Clients



Folgende Werte sind je Client einzutragen:

IP-Adresse

IP-Adresse (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Kennwort gilt.

Netzmaske

IP-Netzmaske der Clients.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

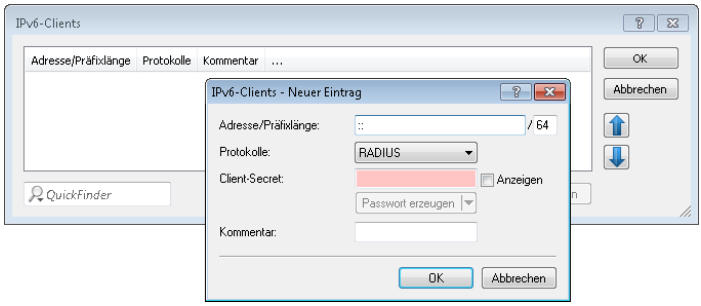
Client-Secret

Kennwort, das die Clients für den Zugang zum internen Server benötigen.

Kommentar

Kommentar zu diesem Eintrag.

IPv6-Clients



Folgende Werte sind je Client einzutragen:

Adresse/Präfixlänge

IP-Adresse (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Kennwort gilt.

Wichtig: Für die Verwendung einer Adresse muss die Präfix-Länge 128 Bit betragen. Der Eintrag "fd00::/64" z. B. erlaubt das gesamte Netzwerk, der Eintrag "fd00::1/128" erlaubt hingegen nur genau einen Client.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Kennwort, das die Clients für den Zugang zum internen Server benötigen.

Kommentar

Kommentar zu diesem Eintrag.

Hinweis: Damit der RADIUS-Server für IPv6-Clients erreichbar ist, muss ggf. in der IPv6-Firewall eine entsprechende Inbound-Regel eingetragen sein.

WLAN-Zugangsliste als Basis für RADIUS-Informationen

In der Zugangsliste können 512 WLAN-Clients eingetragen werden, die sich an einem Access Point anmelden dürfen. In der Betriebsart als RADIUS-Server kann diese Liste auch verwendet werden, um über RADIUS Clients zu prüfen, die sich an anderen Access Points anmelden wollen. In einer Installation mit mehreren Access Points kann so die Zugangsberechtigung der Clients an einer zentralen Stelle gepflegt werden.

Konfigurationstool	*Aufruf*
LANconfig	WLAN-Sicherheit E RADIUS
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > WLAN > RADIUS-Zugriffspruefung

- Server-Datenbank verwenden [Default: ja]

  Dieser Parameter gibt an, ob die WLAN-Zugangsliste als Informationsquelle für den RADIUS-Server im Access Point verwendet werden soll.

  Die WLAN-Zugriffsliste enthält den Benutzernamen in Form der MAC-Adresse und das Kennwort ('WPA-Passphrase'). Neben diesen Zugangsdaten liefert die Zugriffsliste Information wie Bandbreitenbeschränkung oder Zugehörigkeit zu einem bestimmten VLAN.

- Prüfzyklus [Default: 0]

  Ein einmal angemeldeter WLAN-Client bleibt nach der Authentifizierung über RADIUS solange aktiv, bis er sich selbst wieder abmeldet oder vom RADIUS-Server abgemeldet wird. Der RADIUS-Server kann mit der Vorgabe eines Prüfzyklus [Minuten] regelmäßig prüfen, ob die angemeldeten WLAN-Clients noch in der Zugangsliste enthalten sind. Wird ein WLAN-Client aus der Zugangsliste entfernt, bleibt er maximal bis zum nächsten Ablauf des Prüfzyklus im WLAN angemeldet.

Hinweis: Ein Prüfzyklus von '0' schaltet die regelmäßige Prüfung aus, die WLAN-Clients bleiben solange angemeldet, bis sie sich selbst abmelden.

15.9.4 RADIUS-Attribute

Der RADIUS-Client kann RADIUS-Attribute wie “Framed-IP-Address” etc. von einem externen RADIUS-Server anfragen und diese dann z. B. dem PPPoE-Server zur Verfügung stellen, um diese am PPPoE-, PPTP- oder L2TP-Server zu authentifizieren.

Hinweis: Mehr Informationen zu RADIUS-Attributen finden Sie in den folgenden technischen Dokumenten:

- *RFC 2865*
- *RFC 3162*
- *RFC 4679*
- *RFC 4818*
- *RFC 7268*

Die folgenden Attribute werden vom Gerät in Access-Request-Nachrichten übertragen:

ID	*Bezeichnung*	*Bedeutung*	*Mögliche Werte in HiLCOS*
1	User-Name	Der vom Benutzer eingegebene Name.	Verwendet bei 802.1x WLAN, PPPoE-Server, L2TP, PPTP, VPN
2	User-Password	Das vom Benutzer eingegebene Passwort.	Verwendet bei 802.1x WLAN, PPPoE-Server, L2TP, PPTP, VPN
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv4-Adresse des Gerätes>
6	Service-Type	Gibt den Service-Typ an, den das Gerät anfragt oder als Antwort erwartet.	▶ Authenticate-Only ▶ Framed
7	Framed-Protocol	Gibt an, welches Protokoll zu verwenden ist.	PPP
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>

ID	*Bezeichnung*	*Bedeutung*	*Mögliche Werte in HiLCOS*
26	Vendor 2356(LCS) Id 2	MAC-Adresse des Clients, sofern die Authentifizierung über MAC-Adresse stattfindet. Im Gegensatz zur Calling-Station-ID wird dieser Wert als ein 6-Byte Binär-String ausgegeben. Dieses Attribut existiert ausschließlich im Anmeldungsmodus **Anmeldung mit Name, Passwort und MAC-Adresse**.	<MAC-Adresse des Clients>
30	Called-Station-Id	Gibt die ID der gerufenen Station an (z. B. des VPN-Servers).	▶ Server-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) ▶ Dienst-Name (bei PPPoE) ▶ BSSID:SSID (bei WLAN) ▶ MAC-Adresse des Gerätes (bei Public Spot)
31	Calling-Station-Id	Gibt die ID der rufenden Station an (z. B. des VPN-Clients).	▶ Client-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) ▶ Client-MAC-Adresse (bei PPPoE, WLAN und Public Spot)
32	NAS-Identifier	Gibt den Namen des Gerätes an, für das der RADIUS-Server den Zugang verwaltet.	<Geräte-Name>
61	NAS-Port-Type	Gibt den physikalischen Port an, über den das Gerät den Benutzer authentifiziert.	▶ Virtual (bei VPN-Verbindungen über PPTP oder L2TP) ▶ Ethernet (bei PPPoE) ▶ Wireless-802.11 (bei WLAN)
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	▶ 13 (VLAN; bei Public Spot)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	▶ 6 (802; bei Public Spot)
81	Tunnel-Private-Group-Id	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	▶ 1-4096 (bei Public Spot)
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann	z. B. ▶ LAN-1

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
		sowohl eine physische als auch logische Schnittstelle sein.	▶ WLAN-1-5 ▶ WLC-TUNNEL-27
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv6-Adresse des Gerätes>
96	Framed-Interface-ID	Das Attribut definiert den IPv6-Interface-Identifier, der für den Benutzer im IPv6CP festgelegt werden soll.	
97	Framed-IPv6-Prefix	Präfix, welches dem Benutzer über Router Advertisements übermittelt wird.	
99	Framed-IPv6-Route	Dieses Attribut definiert die Route, die für diesen Benutzer festgelegt werden soll. Das Gerät legt in der IPv6-Routing-Tabelle diese Route mit Next-Hop zu diesem Benutzer an.	
100	Framed-IPv6-Pool	Angabe des IPv6-Pools, aus dem ein Präfix für den Benutzer bereitgestellt werden soll. Der IPv6-Pool wird per Name referenziert und muss unter **IPv6** > **Router Advertisement** > **Präfix-Pool** vorhanden sein.	
177	Mobility-Domain-ID	Kennzeichnet die Mobility-Domain, in der sich der Client befindet.	
181	WLAN-HESSID	Enthält die HESSID der 802.11u SSID.	
182	WLAN-Venue-Info	Enthält Informationen zur Kategorie des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
183	WLAN-Venue-Language	Enthält Informationen zur Sprache des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
184	WLAN-Venue-Name	Enthält die Bezeichnung des Standortes (Standort-Name).	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
186	WLAN-Pairwise-Cipher	Enthält Informationen über den paarweisen Schlüssel, den Client und AP verwenden.	
187	WLAN-Group-Cipher	Enthält Informationen über den Gruppenschlüssel, den Client und AP verwenden.	
188	WLAN-AKM-Suite	Enthält Informationen über die Zugriffsverwaltung (Authentication and Key Management) zwischen Client und AP.	
189	WLAN-Group-Mgmt-Cipher	Enthält Informationen über den Gruppenverwaltungsschlüssel, der eine	

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
		Verbindung über RSNA (Robust Security Network Association) zwischen AP und mobilem Client absichert.	
190	WLAN-RF-Band	Enthält Informationen über das Frequenzband, das der Client verwendet.	

Tabelle 37: Übersicht aller unterstützten RADIUS-Attribute

Ein Beispiel für einen PPP-Benutzer `test` mit IPv6 im FreeRADIUS lautet wie folgt:

```
test Cleartext-Password := "1234"
     Service-Type = Framed-User,
     Framed-Protocol = PPP,
     Framed-IPv6-Prefix = "fec0:1:2400:1::/64",
     Delegated-IPv6-Prefix = "fec0:1:2400:1100::/56",
     Framed-IP-Address = 172.16.3.33,
```

Der Benutzer `test` erhält in einer Dual Stack PPP-Session die IPv4-Adresse `172.16.3.33`, per Router Advertisement das Präfix `fec0:1:2400:1::/64` sowie per DHCPv6-Präfix Delegation das Präfix `fec0:1:2400:1100::/56`.

Für die folgenden herstellerspezifischen RADIUS-Attribute wird die IANA Private Enterprise Number “3561” des Broadband-Forums verwendet. Bei den übrigen Einträgen handelt es sich um LANCOM spezifische Attribute!

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
1	ADSL-Agent-Circuit-Id, Vendor 3561	Gibt die Schnittstelle des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen, wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	<Schnittstelle des Gerätes>
2	ADSL-Agent-Remote-Id, Vendor 3561	Gibt die Bezeichnung des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen, wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	<Bezeichnung des Gerätes>
16	LCS-Orig-NAS-Identifier, Vendor 2356	NAS-Identifier des ursprünglichen Access Points im WLC-Betrieb.	<Geräte-Name>
17	LCS-Orig-NAS-IP-Address, Vendor 2356	NAS-IP-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv4-Adresse des Gerätes>

ID	Bezeichnung	Bedeutung	Mögliche Werte in HiLCOS
18	LCS-Orig-NAS-IPv6-Address, Vendor 2356	NAS-IPv6-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv6-Adresse des Gerätes>

Tabelle 38: Übersicht aller unterstützten Hersteller spezifischen RADIUS-Attribute im Access-Request

RADIUS-Attribute konfigurierbar

HiLCOS ermöglicht es, die RADIUS-Attribute für die Kommunikation mit einem RADIUS-Server (sowohl Authentication als auch Accounting) zu konfigurieren.

Die Angabe der Attribute erfolgt als semikolon-separierte Liste von Attribut-Nummern oder -Namen (gem. *RFC 2865*, *RFC 3162*, *RFC 4679*, *RFC 4818*, *RFC 7268*) und einem entsprechenden Wert in der Form `<Attribut_1>=<Wert_1>;<Attribut_2>=<Wert_2>`.

Da die Anzahl der Zeichen begrenzt ist, lässt sich der Name abkürzen. Das Kürzel muss dabei eindeutig sein. Beispiele:

- `NAS-Port=1234` ist nicht erlaubt, da das Attribut nicht eindeutig ist (`NAS-Port`, `NAS-Port-Id` oder `NAS-Port-Type`).
- `NAS-Id=ABCD` ist erlaubt, da das Attribut eindeutig ist (`NAS-Identifier`).

Als Attribut-Wert ist die Angabe von Namen oder RFC-konformen Nummern möglich. Für das Gerät sind die Angaben `Service-Type=Framed` und `Service-Type=2` identisch.

Die Angabe eines Wertes in Anführungszeichen (`"<Wert>"`) ist möglich, um Sonderzeichen wie Leerzeichen, Semikolon oder Gleichheitszeichen mit angeben zu können. Das Anführungszeichen erhält einen umgekehrten Schrägstrich vorangestellt (`\"`), der umgekehrte Schrägstrich ebenfalls (`\\`).

Als Werte sind auch die folgenden Variablen erlaubt:

%n

Gerätename

%e

Seriennummer des Gerätes

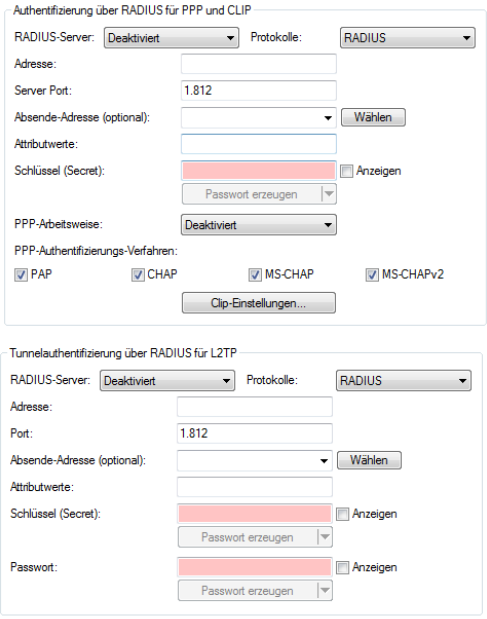
%%

Prozentzeichen

%{name}

Original-Name des Attributes, wie ihn die RADIUS-Anwendung überträgt. Damit lassen sich z. B. Attribute mit originalen RADIUS-Attributen belegen: `Called-Station-Id=%{NAS-Identifier}` setzt das Attribut `Called-Station-Id` auf den Wert, den das Attribut `NAS-Identifier` besitzt.

Unter LANconfig konfigurieren Sie die Attribute unter **Kommunikation** > **RADIUS** jeweils in den Abschnitten **Authentifizierung über RADIUS für PPP und Clip** und **Tunnelauthentifizierung über RADIUS für L2TP**.



15.9.5 Accounting-Statustypen "Accounting-On" und "Accounting-Off"

RADIUS-Server und AP tauschen Status-Informationen wie Start, Ende oder Update von Client-Sessions am AP aus. Diese Datenpakete orientieren sich am Verhalten des angemeldeten Clients.

Mit den Statustypen "Accounting-On" und "Accounting-Off" gibt der AP Informationen über seine generelle Eignung für das RADIUS-Accounting an den RADIUS-Server weiter:

Accounting-On

Wenn das Gerät in einen Betriebszustand wechselt, in dem es Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-On".

Accounting-Off

Wenn das Gerät in einen Betriebszustand wechselt, in dem es keine Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-Off".

Die folgenden Bedingungen lösen die Übertragung eines "Accounting-On" oder "Accounting-Off" aus:

- Das Gerät aktiviert oder deaktiviert eine physikalische WLAN-Schnittstelle mit der entsprechenden SSID.

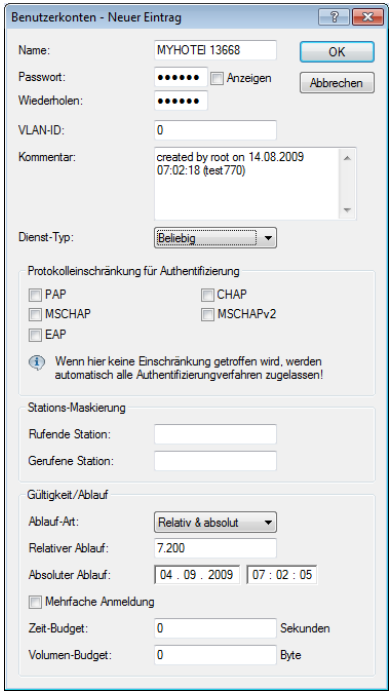
  Hinweis: Die Deaktivierung kann auch die Folge von Überhitzung, Verbindungsverlust oder fehlerhafter Link-Erkennung sein.

- Die WLAN-Schnittstelle wechselt in einen nicht-AP-Modus (also weder 'managed' noch Stand-alone-AP) oder zurück.
- Im P2P-Modus wechselt das Gerät in die Betriebsart "exklusiv", was alle SSIDs deaktiviert.
- Das Gerät aktiviert oder deaktiviert eine SSID.
- Das Gerät aktiviert oder deaktiviert das RADIUS-Accounting für eine SSID.

15.10 Erweiterungen im RADIUS-Server

15.10.1 Erweiterungen im RADIUS-Server

Für die Einrichtung von Public-Spot-Benutzern mit Zeit- und Volumen-Budgets sind zusätzliche Parameter in der Benutzertabelle des RADIUS-Servers erforderlich.



LANconfig: RADIUS / Allgemein / Benutzerkonten

WEBconfig: HiLCOS-Menübaum / Setup / RADIUS E Server / Benutzer

- Mehrfach-Logins

  Erlaubt die mehrfache Anmeldung mit einem Benutzer-Account zur gleichen Zeit.

  Mögliche Werte:

– Ja, Nein

Default:

– Ja

Hinweis: Die Option für die Mehrfach-Logins muss deaktiviert werden, wenn der RADIUS-Benutzer ein Zeit-Budget erhalten soll. Die Einhaltung des Zeit-Budgets kann nur überwacht werden, wenn für den Benutzer zu jeder Zeit nur eine Sitzung aktiv ist.

▶ Ablauf-Art

Diese Option legt fest, wie die Gültigkeitsdauer des Benutzer-Accounts bestimmt wird.

Mögliche Werte:

– Absolut: Die Gültigkeit des Benutzer-Accounts endet zu einem festen Zeitpunkt.
– Relativ: Die Gültigkeit des Benutzer-Accounts endet eine bestimmte Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Default:

– Leer: Die Gültigkeit des Benutzer-Accounts endet nie, es sei denn, ein definiertes Zeit- oder Volumen-Budget wird erreicht.

Hinweis: Die beiden Optionen können kombiniert werden. In diesem Fall endet die Gültigkeit des Benutzer-Accounts dann, wenn einer der beiden Grenzwerte erreicht wird.

Hinweis: Für die Nutzung der Zeit-Budgets bei Benutzer-Accounts muss das Gerät über eine gültige Zeit verfügen, da ansonsten der Ablauf der Gültigkeit nicht geprüft werden kann.

▶ Abs.-Ablauf

Wenn der Ablauf-Typ “Absolut” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts zu dem in diesem Wert angegebenen Zeitpunkt.

Mögliche Werte:

– Gültige Zeitinformation aus Datum und Uhrzeit. Maximal 20 Zeichen aus `0123456789/:.Pp`

Default:

– Leer

Besondere Werte:

– 0 schaltet die Überwachung der absoluten Ablaufzeit aus.

▶ Rel.-Ablauf

Wenn der Ablauf-Typ “Relativ” aktiviert ist, endet die Gültigkeit des Benutzer-Accounts nach der in diesem Wert angegebenen Zeitspanne nach dem ersten erfolgreichen Login des Benutzers.

Mögliche Werte:

– Zeitspanne in Sekunden. Maximal 10 Zeichen aus `0123456789`

Default:

– 0

Besondere Werte:

– 0 schaltet die Überwachung der relativen Ablaufzeit aus.

▶ Zeit-Budget

Maximale Nutzungsdauer für diesen Benutzer-Account. Diese Nutzungsdauer kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

– Zeitspanne in Sekunden. Maximal 10 Zeichen aus `0123456789`

Default:

– 0

Besondere Werte:

– 0 schaltet die Überwachung der Nutzungsdauer aus.

▶ Volumen-Budget

Maximales Datenvolumen für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Mögliche Werte:

- Volumen-Budget in Bytes. Maximal 10 Zeichen aus `0123456789`

Default:

- 0

Besondere Werte:

- 0 schaltet die Überwachung des Datenvolumens aus.

▶ Kommentar

Kommentar zu diesem Eintrag.

▶ Service-Typ

Der Service-Typ ist ein spezielles Attribut des RADIUS-Protokoll, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Service-Typ mit dem Service-Typ des Benutzer-Accounts übereinstimmt.

Mögliche Werte:

- Framed: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
- Login: Für Public-Spot-Anmeldungen.
- Nur-Auth.: Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.
- Beliebig

Default:

- Beliebig

Hinweis: Die Anzahl der Einträge mit dem Service-Typ “Beliebig” oder “Login” ist je nach Modell auf 64 oder 256 begrenzt. So wird die Tabelle nicht vollständig mit Einträgen von Public-Spot-Zugängen belegt (die den Service-Typ “Beliebig” verwenden) und ermöglicht eine parallele Nutzung für Anmeldungen über 802.1x.

15.10.2 Neue Authentifizierungs-Verfahren

Bis zu Version 6.30 unterstützt der HiLCOS-RADIUS-Server nur PAP als Authentifizierungsverfahren, d. h. der RADIUS-Client (im Weiteren als NAS bezeichnet – Network Access Server) übermittelt den Benutzernamen und das Passwort, der Server beantwortet diese Anfrage mit einem Access- Accept oder Access-Reject. Dieses Verfahren ist allerdings nur eine Möglichkeit aus einer Reihe von Authentifizierungsverfahren, die über RADIUS abgewickelt werden können. Der RADIUS-Server des HiLCOS unterstützt folgende Authentifizierungsverfahren

- PAP: Der NAS übermittelt den Benutzernamen und das Passwort. Der RADIUS-Server durchsucht seine Datensätze nach einem passenden Eintrag für den Benutzernamen, vergleicht dann das Passwort und antwortet mit einem RADIUS-Accept oder RADIUS-Reject.
- CHAP: Der NAS übermittelt den Benutzernamen, die CHAP-Aufforderung (Challenge) und die Passwort-Eigenschaften (nicht das Passwort selbst!). Der RADIUS-Server durchsucht seine Datensätze nach einem passenden Eintrag für den Benutzernamen und errechnet aus dem zugehörigen Passwort und der vom NAS übermittelten CHAP-Challenge die CHAP-Antwort. Wenn die berechnete Antwort mit der vom Client über den NAS gesendeten Antwort übereinstimmt sendet der RADIUS-Server einen RADIUS-Accept, ansonsten einen RADIUS-Reject.
- MS-CHAP: Der NAS übermittelt den Benutzernamen, die MS-CHAP-Challenge und die MS-CHAP-Passwort-Eigenschaften. Der weitere Vorgang ist der gleiche wie bei CHAP, die Antworten sind dabei allerdings nach dem MS-CHAP-Algorithmus berechnet (RFC 2433).
- MS-CHAPv2: Der NAS übermittelt den Benutzernamen, die MS-CHAP-Challenge und die MS-CHAP2-Antwort. Der weitere Vorgang ist der gleiche wie bei CHAP und MS-CHAP, die Antworten sind dabei allerdings nach dem MS-CHAPv2-Algorithmus berechnet (RFC 2759). Außerdem überträgt der RADIUS-Server eine MS-CHAP2-Bestätigung, wenn die Authentifizierung erfolgreich durchgeführt wurde. Diese Bestätigung enthält die Antwort des Servers auf die Aufforderung des Clients und ermöglicht so eine gegenseitige Authentifizierung.
- EAP: Der NAS übermittelt den Benutzernamen und eine EAP-Nachricht. Im Gegensatz zu allen vorherigen Methoden ist EAP nicht zustandslos, d. h. der RADIUS-Server kann mit einer eigenen Aufforderung (Challenge) statt nur mit einem Access-Accept oder Access-Reject antworten und so weitere Anforderungen vor dem Abschluss der Authentifizierung stellen.

EAP ist selbst ein modulares Authentifizierungsprotokoll, das unterschiedliche Authentifizierungsverfahren erlaubt.

15.10.3 EAP-Authentifizierung

EAP ist kein festes Authentifizierungsverfahren sondern es bietet einen Rahmen für beliebige Authentifizierungsverfahren. Der HiLCOS-RADIUS-Server unterstützt eine Reihe von EAP-Verfahren:

- EAP/MD5, definiert in RFC 2284. EAP/MD5 ist ein einfaches Challenge/Response-Protokoll. Es erlaubt weder eine gegenseitige Authentifizierung noch bietet es dynamische Schlüssel an, wie sie für die 802.1x-Authentifizierung in drahtlosen Netzwerken (WLANs) benötigt werden. Es wird daher nur für die Authentifizierung von nicht-wireless Clients benötigt oder als getunneltes Verfahren innerhalb von TTLS.
- EAP/MSCHAPv2, definiert in draft-kamath-pppext-eap-mschapv2-01.txt. Im Gegensatz zu EAP/MD5 erlaubt EAP/MSCHAPv2 zwar die gegenseitige Authentifizierung, unterstützt aber keine dynamischen Schlüssel und ist daher ähnlich anfällig für Dictionary Attacks (Wörterbuchattacken) wie EAP/MD5. Dieses Verfahren wird üblicherweise innerhalb von PEAP-Tunneln genutzt.
- EAP/TLS, definiert in RFC2716. Der Einsatz von EAP/TLS erfordert ein Root-Zertifikat, eine Geräte-Zertifikat und einen privaten schlüssel (Private Key) im Gerät. EAP/TLS bietet hervorragende Sicherheit und die für Wireless-Verbindungen benötigten dynamischen Schlüssel, ist allerdings aufwendig in der Einführung, weil für jeden Client ein Zertifikat und ein Private Key erstellt werden müssen.

  Hinweis: Bitte beachten Sie, dass die TLS-Implementation im HiLCOS weder Zertifikatsketten noch Zertifikats-Rückruflisten (Certificate Revocation Lists – CRL) unterstützt.

- EAP/TTLS, definiert in draft-ietf-pppext-eap-ttls-05.txt. TTLS basiert auf TLS, verzichtet aber auf Client-Zertifikate und verwendet den schon aufgebauten TLS-Tunnel zur Authentifizierung des Clients. Der HiLCOS-RADIUS-Server unterstützt die folgenden TTLS-Verfahren:
  - PAP
  - CHAP
  - MSCHAP

- MSCHAPv2
- EAP, vorzugsweise EAP/MD5

- EAP/PEAPv0, definiert in draft-kamath-pppext-peapv0-00.txt. Ähnlich wie TTLS setzt PEAP auf TLS auf und arbeitet mit einer EAP-Verhandlung im TLS-Tunnel.

Hinweis: Bitte beachten sie, dass PEAP zwar beliebige Authentifizierungsverfahren ermöglicht, der HiLCOS-RADIUS-Server aber nur MSCHAPv2 als Tunnelmethode unterstützt.

Aktuell kann kein Authentifizierungsverfahren unterdrückt werden – der EAP-Supplicant und der RADIUS-Server handeln die EAP-Methode über den Standard-EAP-Mechanismus aus. Sollte der Client eine nicht unterstützte EAP-Methode anfordern, wird er vom RADIUS-Server abgewiesen.

EAP-SIM-Modul im RADIUS-Server

Der RADIUS-Server enthält ein EAP-SIM-Modul, welches das Gerät um die Fähigkeit erweitert, das Home Location Register (HLR) eines Mobilfunkproviders zu simulieren. Ein HLR generiert in der Regel die nötigen Keys für die registrierten SIM-Karten, damit ein RADIUS-Server einen Client per EAP-SIM authentifizieren kann.

Die notwendigen Keys lassen sich im RADIUS-Server manuell festlegen und hinterlegen, sodass ein HLR nicht notwendig ist. EAP-SIM wird z. B. im Zusammenhang mit Hotspot 2.0 verwendet.

15.10.4 LCS-WPA-Passphrase

Ab HiLCOS-Version 8.80 enthält die Benutzertabelle des RADIUS-Servers auch die jeweilig zugeordnete WPA-Passphrase des registrierten Benutzers. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS (LANCOM Enhanced Passphrase Security) nutzen.

Bei der Konfiguration von LEPS wird lediglich jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dazu wird der MAC-Filter positiv eingestellt, d. h. die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Hinweis: Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Die client-spezifische Passphrase ist in der Benutzertabelle des RADIUS-Servers gespeichert. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS nutzen.

Konfiguration

Bei der Konfiguration von LEPS wird lediglich jeder MAC-Adresse eines im WLAN zugelassenen Clients eine eigene Passphrase zugeordnet. Dazu wird der MAC-Filter positiv eingestellt, d. h., die Daten von den hier eingetragenen WLAN-Clients werden übertragen.

Hinweis: Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 32 Zeichen Länge.

Die client-spezifische Passphrase ist in der Benutzertabelle des RADIUS-Servers gespeichert. Somit kann auch ein LAN-gebundenes Gerät als zentraler RADIUS-Server dienen und die Vorteile von LEPS nutzen.

15.10.5 RADIUS-Forwarding

Bei den „mehrschichtigen“ EAP-Protokollen wie TTLS oder PEAP kann die eigentliche „innere“ Authentifizierung auf einem separaten RADIUS-Server erfolgen. Das ermöglicht z. B. die Weiterverwendung eines existierenden RADIUS-Servers, der nur die Benutzertabellen bereitstellt, selbst aber nicht EAP(/TLS)-fähig ist. Der TLS/TTLS/PEAP-Tunnel wird in diesem Fall vom HiLCOS-RADIUS-Server verwaltet.

Die Konfiguration von solchen mehrschichtigen Protokollen ist Teil einer allgemeinen Methode zur Weiterleitung von RADIUS-Anfragen, mit der ein HiLCOS-RADIUS-Servers auch als RADIUS-Proxy verwendet werden kann. Die Weiterleitung von Anfragen bzw. die Proxy-Funktion basieren auf dem Konzept der „Realms“. Ein Realm ist eine Zeichenkette, welche die Gültigkeit einer Reihe von Benutzerkonten definiert. Sofern es definiert ist, wird der Realm über ein @-Zeichen getrennt an den Benutzernamen angehängt in

der Form: Das Gerät betrachtet die folgenden Bestandteile eines Benutzernamens als Realm:

`benutzer@realm`

`user@company.com`

`company.com` bildet den Realm und ist durch ein @-Zeichen vom Benutzernamen getrennt.

`company\user`

`company` bildet den Realm und ist durch einen Backslash ("\") vom Benutzernamen getrennt. Diese Authentifizierung ist z. B. bei einem Windows-Login gebräuchlich.

`host/user.company.com`

Beginnt der Benutzername mit dem String `host/` und enthält der restliche Name mindestens einen Punkt, dann betrachtet das Gerät alles hinter dem ersten Punkt als Realm (in diesem Fall also `company.com`).

Der Realm kann als Hinweis auf den RADIUS-Server verstanden werden, auf dem das Benutzerkonto verwaltet wird. Vor dem Durchsuchen der Benutzertabelle auf dem RADIUS-Server wird der Realm wieder entfernt. Mit der Nutzung von Realms können ganze Netzwerke, die untereinander als vertrauenswürdig gelten, die RADIUS-Server in den Partner-Netzen nutzen und so auch zwischen den Netzen wechselnde Benutzer authentifizieren. Der HiLCOS-RADIUS-Server speichert die verbundenen RADIUS-Server mit Angabe des zugehörigen Realms in einer Weiterleitungs-Tabelle. Diese Tabelle wird nach dem – in Verbindung mit dem Benutzernamen übermittelten – Realm durchsucht. Wenn keine Übereinstimmung gefunden wird, wird die Anfrage mit einem Access Reject beantwortet. Ein leerer Realm wird als lokale Anfrage gewertet, d. h. der HiLCOS-RADIUS-Server durchsucht seine eigenen Benutzer-Tabellen und erzeugt daraus die entsprechende Antwort.

Zur Unterstützung der Realm-Verarbeitung verwendet der HiLCOS-RADIUS-Server zwei spezielle Realms:

- Default-Realm: Dieser Realm wird verwendet, wenn ein Realm übermittelt wird, für den kein expliziter Forwarding-Server definiert ist. Für den Default-Realm selbst muss in der Weiterleitungs-Tabelle allerdings ein entsprechender Eintrag angelegt werden.

- Leer-Realm: Dieser Realm wird verwendet, wenn **kein** Realm, sondern nur der Benutzername übermittelt wird.

Im Default-Zustand enthält die Weiterleitungs-Tabelle keine Einträge, der Default- und der Leer-Realm sind leer. Das bedeutet das alle Anfragen als lokale Anfragen behandelt werden und ggf. übermittelte Realms werden ignoriert. Um den HiLCOS-RADIUS-Server als reinen Weiterleitungs-Server bzw. RADIUS-Proxy zu verwenden, müssen der Default- und der Leer-Realm auf einen Wert gesetzt werden, für den in der Weiterleitungs-Tabelle ein entsprechender Server definiert ist.

Bitte beachten Sie, dass die Weiterleitung von RADIUS-Anfragen den übermittelten Benutzernamen nicht verändert – es wird weder ein Realm hinzugefügt, noch verändert oder abgeschnitten. Der Server, an den die Anfrage weitergeleitet wird, muss nicht der letzte der Weiterleitungs-Kette sein, und er benötigt möglicherweise den Realm selbst für eine korrekte Weiterleitung. Nur der RADIUS-Server, der letztlich die Anfrage bearbeitet, löst den Realm aus dem Benutzernamen und durchsucht erst dann die Tabellen mit den Benutzerkonten. Dementsprechend löst der HiLCOS-RADIUS-Server den Realm vom Benutzernamen, wenn die Anfragen lokal verarbeitet werden.

Zur Verarbeitung von getunnelten EAP-Anfragen im Zusammenhang mit TTLS und PEAP wird ein spezieller EAP-Tunnel-Server verwendet – auch in Form eines Realms. Wählen Sie hier einen Realm, der nicht mit anderen verwendeten Realms in Konflikt steht. Wenn kein EAP-Tunnel-Server angegeben ist, leitet der HiLCOS-RADIUS-Server Anfragen an sich selbst weiter, was bedeutet, dass sowohl die innere als auch die äußere EAP-Authentifizierung vom HiLCOS-RADIUS-Server selbst bearbeitet werden.

15.10.6 Separate RADIUS-Server pro SSID

Wenn Sie RADIUS zur zentralen Verwaltung von Konto- und Zugangsinformationen in Ihren WLANs einsetzen, übernimmt standardmäßig der Access Point zentral das Weiterleiten der Anfragen für die Authorisierung und das Accounting an den RADIUS-Server. Sofern Sie für die Verwaltung der Access Points einen WLAN-Controller einsetzen, kann auch der WLAN-Controller die RADIUS-Anfragen von allen angeschlossenen Access Points an den entsprechenden RADIUS-Server weiterleiten.

In manchen Anwendungsfällen möchte der Betreiber von Access Points oder WLAN-Controllern jedoch unterschiedliche RADIUS-Server für einzelne logische WLANs (SSIDs) einsetzen. Das ist z. B. dann der Fall, wenn mehrere

Kunden die technische WLAN-Infrastruktur gemeinsam nutzen, dabei jedoch eigene Systeme zur Authentifizierung einsetzen (zum Beispiel bei Wireless as a Service - WaaS).

In diesen Fällen haben Sie die Möglichkeit, für jedes logische WLAN (also jede SSID) ein separates RADIUS-Profil zu wählen. Das RADIUS-Profil enthält alle notwendigen Angaben zur Nutzung der entsprechenden RADIUS-Server inklusive der optionalen Backup-Lösung.

15.10.7 Parameter des RADIUS-Servers

Zur Konfiguration des RADIUS-Servers wird definiert, welche Clients auf den RADIUS-Server zugreifen dürfen (inklusive Kennwort) und über welchen UDP-Port die Clients mit dem RADIUS-Server kommunizieren können. Der Authentifizierungs-Port gilt dabei global für alle Clients.

Konfigurationstool	*Aufruf*
WEBconfig, Telnet	HiLCOS-Menübaum > Setup > Radius > Server

Globale Einstellungen für den RADIUS-Server

- Authentifizierungs-Port [Default: 0]

  Geben Sie hier den Port an, über den die Authenticator mit dem RADIUS-Server im Access Point kommunizieren. Üblicherweise wird der Port '1812' verwendet.

  - Der Port '0' schaltet den RADIUS-Server aus.

- Default-Realm

  Dieser Realm wird verwendet, wenn der übermittelte Benutzername einen **unbekannten** Realm verwendet, der nicht in der Liste der Weiterleitungs-Server enthalten ist.

- Empty-Realm

  Dieser Realm wird verwendet, wenn der übermittelte Benutzername **keinen** Realm enthält.

RADIUS-Clients

IP-Adresse

IP-Adressen (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Kennwort gilt.

Netzmaske

IP-Netzmasken der Clients.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Kennwort, das die Clients für den Zugang zum internen Server benötigen.

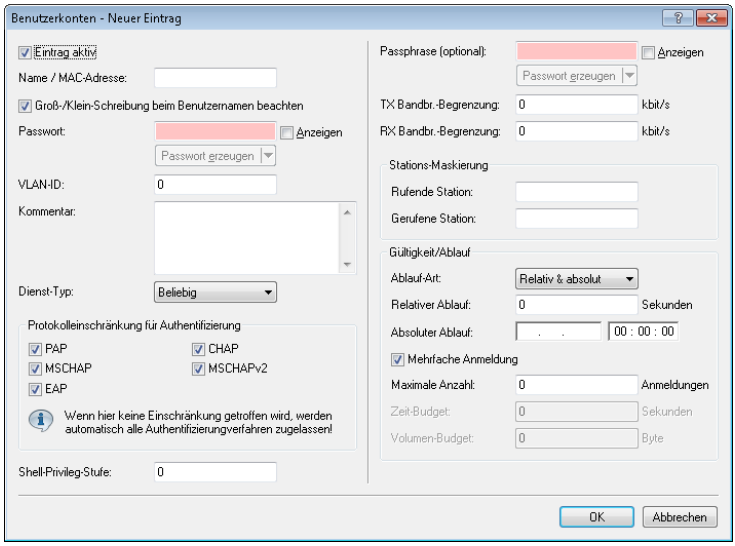
Kommentar

Kommentar zu diesem Eintrag.

RADIUS-Benutzer

In der RADIUS Benutzerdatenbank tragen die Benutzerkonten ein, die der RADIUS-Server ohne weitere Datenbanken authentifizieren kann. Diese Datenbank verwendet der RADIUS-Server für lokale Anfragen, also für Anfragen mit Benutzernamen ohne Realm.

Hinweis: Bitte beachten Sie, dass die Anzahl der Benutzer, die die Datenbank aufnehmen kann, modellabhängig ist. Die maximale mögliche Anzahl der Benutzerkonten entnehmen Sie der Produktbeschreibung Ihres Gerätes. Bei Geräten ohne Limitierung ist eine Obergrenze von max. 2.500 Benutzern empfehlenswert.



- **Eintrag aktiv**: Über diese Option aktivieren bzw. deaktivieren Sie gezielt ein RADIUS-Benutzerkonto. Auf diese Weise lassen sich z. B. einzelne Benutzerkonten temporär abschalten, ohne dafür das komplette Konto zu löschen.
- **Benutzername**: Geben Sie hier den Namen des Benutzers ein
- **Groß-/Kleinschreibung beim Benutzernamen beachten**: Bei aktivierter Option unterscheidet der RADIUS-Server nach Groß- und Kleinschreibung. "User12345" und "user12345" sind somit zwei unterschiedliche Benutzer.
- **Passwort**: Passwort des Benutzers
- **VLAN-ID**: ID des logischen Teilnetzes
- **Kommentar**: Zusätzliche Informationen zum Benutzer
- **Dienst-Typ**: Der Dienst-Typ ist ein spezielles Attribut des RADIUS-Protokolls, welches der NAS (Network Access Server) mit dem Authentication Request übermittelt. Der Request wird nur dann positiv beantwortet, wenn der angefragte Dienst-Typ mit dem Dienst-Typ des Benutzerkontos übereinstimmt. Mögliche Werte sind:
  - `Beliebig`: Der Dienst-Typ kann ein beliebiger Sein.
  - `Framed`: Für Prüfung von WLAN-MAC-Adressen über RADIUS bzw. bei IEEE 802.1x.
  - `Anmeldung`: Für Public-Spot-Anmeldungen.

- `Nur Authentifizierung` : Für Einwahl-Gegenstellen über PPP, die mit RADIUS authentifiziert werden.

Hinweis: Beachten Sie, dass in Abhängigkeit vom Gerät die Anzahl der Einträge mit dem Dienst-Typ `Beliebig` oder `Anmeldung` begrenzt sein kann. Ist Ihr Gerät z. B. dazu in der Lage, insgesamt 64 Public-Spot-Benutzer zu verwalten, dann verweigert LANconfig nach dem 64. Benutzerkonto mit dem Dienst-Typ `Beliebig`/`Anmeldung` die Anlage weiterer Benutzerkonten mit diesen Dienst-Typen.

- **Protokolleinschränkung**: Mit dieser Option können Sie die für den Benutzer erlaubten Authentifizierungsverfahren einschränken. Mögliche Werte sind:
  - PAP
  - CHAP
  - MSCHAP
  - MSCHAPv2
  - EAP
- **Shell-Privileg-Stufe**: Vendor spezifisches RADIUS-Attribut, um in einem RADIUS-Accept die Privilegstufe des Nutzers zu kommunizieren (Default: 0).
- **Passphrase**: zugeordnete WPA-Passphrase des registrierten Benutzers
- **TX-Bandbr.-Begrenzung**: Begrenzung der Bandbreite beim Senden von Daten
- **RX-Bandbr.-Begrenzung**: Begrenzung der Bandbreite beim Empfangen von Daten

Hinweis: Die Bandbreitenbegrenzung für Senden und Empfangen gilt unabhängig vom verwendeten Interface (LAN und WLAN).

- **Rufende Station**: Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die rufende Station (WLAN-Client) übermittelt. Bei der Authentifizierung über 802.1x wird die MAC-Adresse der rufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt (z. B. "00-10-A4-23-19-C0").

- **Gerufene Station**: Diese Maske schränkt die Gültigkeit des Eintrags auf bestimmte IDs ein, die die gerufende Station (BSSID und SSID des Access-Points) übermittelt. Bei der Authentifizierung über 802.1x werden die MAC-Adresse (BSSID) der gerufenden Station im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt. Die SSID wird nach einem Doppelpunkt als Trennzeichen angehängt (z. B. "00-10-A4-23-19-C0:AP1").
- **Ablauf-Art**: Diese Option legt die Art der Gültigkeitsdauer des Benutzer-Accounts fest. Mögliche Werte sind:
  - `Relativ & absolut`
  - `Relativ`
  - `Absolut`
  - `Niemals`
- **Relativer Ablauf**: Gültigkeit in Sekunden ab der ersten erfolgreichen Anmeldung
- **Absoluter Ablauf**: Gültigkeit in Stunden, Minuten und Sekunden ab einem bestimmten Datum
- **Mehrfache Anmeldung**: Aktiviert die Möglichkeit für den Client, sich mehrfach anmelden zu können.
- **Maximale Anzahl**: Maximale Anzahl der gleichzeitigen Anmeldungen des Clients.
- **Zeit-Budget**: Legt das Zeit-Budget in Sekunden fest, das dem Client zur Verfügung steht.
- **Volumen-Budget**: Legt das Datenvolumen fest, das dem Client zur Verfügung steht.

Weiterleitungs-Server

In der Tabelle der Weiterleitungs-Server werden bis zu 16 Realms mit den zugehörigen Weiterleitungs-Zielen eingetragen.

- Realm

  Zeichenkette, mit der das Weiterleitungs-Ziel identifiziert wird.

- IP-Adresse

  IP-Adresse des RADIUS-Servers, an den die Anfrage weitergeleitet werden soll.

- Port

  Offener Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.

- Secret

  Kennwort, das für den Zugang zum Weiterleitungs-Server benötigt wird.

- Backup

  Alternativer Weiterleitungs-Server, an den Anfragen weitergeleitet werden, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

EAP-Optionen für den RADIUS-Server

- EAP-Tunnel-Server

  Realm als Verweis auf den Eintrag in der Tabelle der Weiterleitungs-Server, der für getunnelte TTLS bzw. PEAP-Anfragen verwendet werden soll.

- TLS-Pruefe-Benutzernamen

  Bei TLS authentifiziert sich der Client alleine über sein Zertifikat. Ist diese Option aktiviert, so prüft der RADIUS-Server zusätzlich, ob der im Zertifikat hinterlegte Benutzername in der RADIUS-Benutzertabelle enthalten ist.

15.10.8 Über RADIUS in die HiLCOS-Verwaltungsoberfläche einloggen

Aktuell existieren drei Methoden, sich in die Verwaltungsoberfläche des Geräts einzuloggen:

- intern: Das Gerät übernimmt die komplette Benutzerverwaltung mit Anmeldename, Passwort sowie Zugriffs- und Funktionsrechte-Zuordnung.
- TACACS+: Die Benutzerverwaltung erfolgt über einen TACACS+-Server im Netzwerk.
- RADIUS: Die Benutzerverwaltung erfolgt über einen RADIUS-Server im Netzwerk.

Mit RADIUS kann sich der Benutzer über die folgenden Verbindungen einloggen:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Hinweis: Eine RADIUS-Authentifizierung über SNMP ist derzeit nicht unterstützt.

Hinweis: Eine RADIUS-Authentifizierung über LL2M (LANCOM Layer 2 Management Protokoll) ist nicht unterstützt, da LL2M Klartext-Zugriff auf das im Gerät gespeicherte Passwort benötigt.

Der RADIUS-Server übernimmt die Verwaltung der Benutzer in den Bereichen Authentifizierung, Authorisierung und Accounting (Triple-A-Protokoll), was bei umfangreichen Netzwerk-Installationen mit mehreren Routern die Verwaltung von Admin-Zugängen stark vereinfacht.

Die Anmeldung über einen RADIUS-Server läuft wie folgt ab:

1. Bei der Anmeldung sendet das Gerät die eingegebenen Anmeldedaten des Benutzers an den RADIUS-Server im Netz. Die Server-Daten sind dazu im Gerät gespeichert.
2. Der Server prüft die Anmeldedaten auf Gültigkeit.
3. Bei ungültigen Daten sendet er dem Gerät eine entsprechende Nachricht, und das Gerät bricht den Anmeldevorgang mit einer Fehlernachricht ab.
4. Bei gültigen Anmeldedaten sendet der Server dem Gerät mit der Zugangserlaubnis auch die Zugriffs- und Funktionsrechte, so dass der Anwender nur auf die entsprechend freigeschalteten Funktionen und Verzeichnisse zugreifen kann.
5. Falls die Sitzungen des Anwenders durch den RADIUS-Server budgetiert sind (Bereich Accounting), speichert das Gerät die Sitzungsdaten wie Start, Ende, Benutzername, Authentifizierungsmodus und, wenn vorhanden, den genutzen Port.

15.11 RADSEC

RADIUS hat sich als Standard für serverbasierte Authentifizierung, Autorisierung und Abrechnung etabliert. Mittlerweile wird RADIUS z. B. im Zusammenspiel mit EAP/802.1x in Anwendungen eingesetzt, für die es ursprünglich nicht entwickelt wurde, und weist daher einige Mängel auf:

- RADIUS läuft über UDP und bietet daher kein natives Verfahren zur Prüfung von Paketverlusten. Dieser Aspekt ist in einer LAN-Umgebung nicht problematisch, gewinnt aber bei Übertragungen über WAN-Strecken oder das Internet an Bedeutung.
- RADIUS verfügt nur über einfache Verfahren zur Authentifizierung über ein „Shared Secret“ und nur über geringe Vertraulichkeit.

Mit RADSEC steht ein alternatives Protokoll zur Verfügung, welches die RADIUS-Pakete durch einen TLS-verschlüsselten Tunnel überträgt. TLS setzt auf TCP auf und bringt somit einen erprobten Mechanismus zur Überwachung verlorener Pakete mit. Ausserdem verfügt TLS über hohe Vertraulichkeit und ein Verfahren zur gegenseitigen Authentifizierung über X.509-Zertifikate.

15.11.1 Konfiguration von RADSEC für den Client

Gerät als RADIUS-Client

In der Funktion als RADIUS-Client wird ein Gerät auf die Verwendung von RADIUS über UDP oder RADSEC über TCP mit TLS eingestellt. Zusätzlich wird der zu verwendende Port angegeben: 1812 für Authentifizierung über RADIUS, 1813 für die Abrechnung über RADIUS und 2083 für RADSEC.

Diese Einstellungen werden an allen Stellen vorgenommen, an denen ein Gerät als RADIUS-Client konfiguriert wird:

WEBconfig: **Setup** / **WAN** / **RADIUS**

WEBconfig: **Setup** / **WLAN** / **RADIUS-Zugriffspruefung**

WEBconfig: **Setup** / **WLAN** / **RADIUS-Accounting**

WEBconfig: **Setup** / **Public-Spot-Modul** / **Anbieter-Tabelle**

WEBconfig: **Setup** / **IEEE802.1x** / **RADIUS-Server**

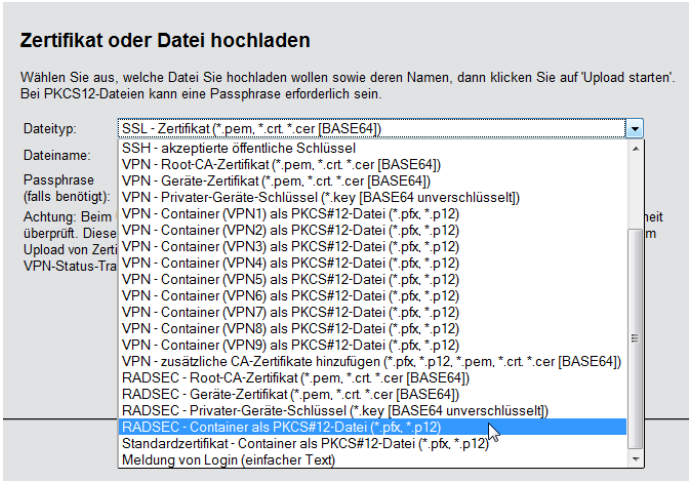
Gerät als RADIUS-Server

Arbeitet ein Gerät selbst als RADIUS-Server, kann der RADSEC-Port konfiguriert werden, auf dem der Server RADSEC-Anmeldungen erwartet. Darüber hinaus kann für alle RADIUS-Clients in der Client-Liste das zu verwendende Protokoll (RADIUS, RADSEC oder alle) eingestellt werden. Auf diese Weise kann z. B. RADIUS für die Clients im LAN, die zuverlässigere RADSEC-Variante über TCP für externe Anmeldungen über das Internet eingesetzt werden.

15.11.2 Zertifikate für RADSEC

Für die TLS-Verschlüsselung der RADSEC-Verbindung werden separate X.509-Zertifikate benötigt. Die einzelnen Zertifikate (Root-Zertifikat, Geräte-Zertifikat und privater Schlüssel) können entweder einzeln oder als PKCS#12-Container in das Gerät geladen werden.

WEBconfig: **Zertifikat oder Datei hochladen**



15.12 Betrieb von Druckern am USB-Anschluss des Gerätes

Über den bei verschiedenen Modellen vorhandenen USB-Port können Drucker an das Gerät angeschlossen und so im gesamten Netzwerk verfügbar gemacht werden. Das Gerät stellt dazu einen Printserver zur Verfügung, der die Druckaufträge aus dem Netzwerk verwaltet. Dabei werden die Protokolle RawIP und LPR/LPD unterstützt.

Hinweis: Parallele Druckaufträge von verschiedenen Stationen werden auf den jeweiligen Rechnern gespeichert. Der Printserver im Gerät arbeitet die anliegenden Aufträge nacheinander ab.

15.12.1 Konfiguration des Printservers im Gerät

Bei der Konfiguration des USB-Ports für den Anschluss eines Druckers werden in erster Linie die Ports festgelegt, auf denen Druckaufträge über die möglichen Protokolle angenommen werden.

Druckertabelle

Die Druckertabelle enthält die Einstellungen für die angeschlossenen Drucker.

Konfigurationstool	*Aufruf*
WEBconfig, Telnet	LCOS Menübaum > Setup > Drucker > Drucker

In der Regel müssen die Einstellungen für den Drucker nicht verändert werden. In der Voreinstellung arbeitet der Printserver sowohl mit RawIP als auch mit LPR/LDP und reagiert auf die Standard-Ports, die von Windows bei der Konfiguration des Druckeranschlusses vorgeschlagen werden. Falls diese Einstellungen keinen erfolgreichen Druckerbetrieb zulassen, können die Druckerparameter angepasst werden.

- **Drucker** [Default: *]

  Der Name des Druckers.

- RawIP-Port [Default: 9100]

  Über diesen Port können Druckaufträge über RawIP angenommen werden.

  Hinweis: RawIP wird von Windows als Standard verwendet und kann für den Betrieb von Druckern am USB-Port empfohlen werden.

- LDP-Port [Default: 515]

  Über diesen Port können Druckaufträge über LDP angenommen werden.

  Hinweis: Die hier eingetragenen Optionen zu Protokoll und Port müssen mit den Einstellungen des Druckeranschlusses im Betriebssystem der entsprechenden Rechner übereinstimmen.

- **Aktiv** [Default: Nein]
  - Ja: Der Printserver ist aktiv.
  - Nein: Der Printserver ist nicht aktiv.
- **Bidirektional** [Default: Nein]
  - Ja: Das Gerät versendet die Statusinformationen des Druckers in regelmäßigen Abständen an die angeschlossenen Rechner.
  - Nein: Das Gerät versendet keine Statusinformationen.

Zugangs-Liste

In der Zugangsliste werden bis zu 16 Netzwerke eingetragen, die Zugriff auf die konfigurierten Drucker haben.

Konfigurationstool	*Aufruf*
LANconfig	Drucker / Allgemein / Zugangsliste
WEBconfig, Telnet	LCOS Menübaum > Setup > Drucker > Zugangs-Liste

- **IP-Adresse**

  IP-Adresse des Netzwerks, dessen Clients Zugriff auf den Drucker haben dürfen.

- **Netzmaske**

  Netzmaske zu den erlaubten Netzwerken.

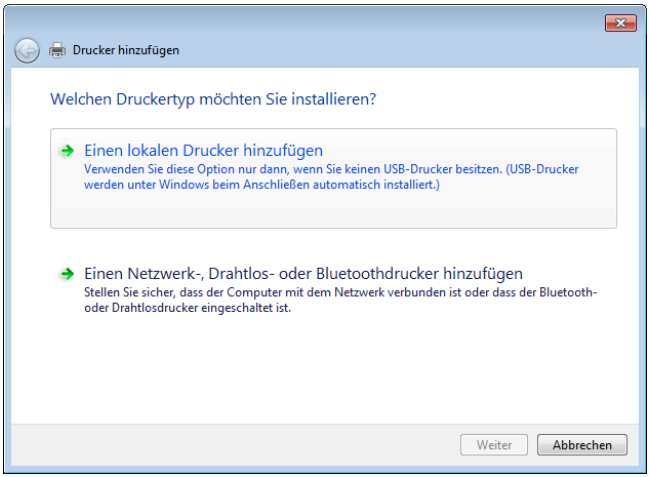
  Hinweis: Wenn die Zugangsliste keine Einträge enthält, können Rechner mit beliebigen IP-Adressen einen Drucker am USB-Port des Gerätes nutzen.

  Hinweis: Der Zugang zu einem Drucker am USB-Port des Gerätes über das WAN ist aus Sicherheitsgründen grundsätzlich nicht möglich.

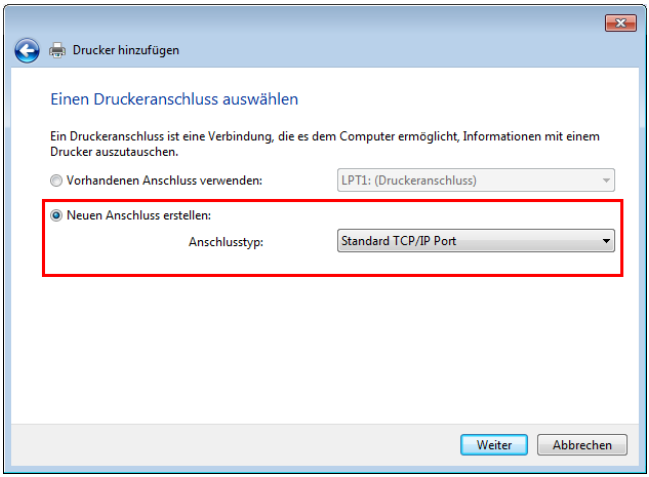
15.12.2 Konfiguration der Drucker auf dem Rechner

Zur Nutzung des Druckers am USB-Port über das Netzwerk muss auf den Rechnern der Druckertreiber mit einem entsprechenden Druckeranschluss verbunden werden. Die nachfolgende Beschreibung zeigt die Einrichtung unter Windows XP, die Konfiguration unter Windows 2000 verläuft sehr ähnlich. Ältere Windows-Versionen unterstützen die Druckeransteuerung über TCP/IP-Ports nur unzureichend.

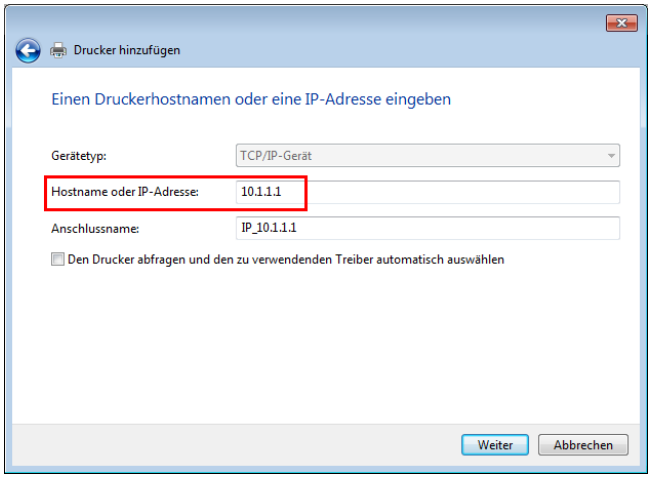
1. Öffnen Sie den Dialog zur Konfiguration eines neuen Druckers in der Systemsteuerung und starten Sie den Assistenten zum Hinzufügen eines neuen Druckers.
2. Wählen Sie die Option für einen lokalen Drucker und deaktivieren Sie den Plug and Play-Mechanismus.



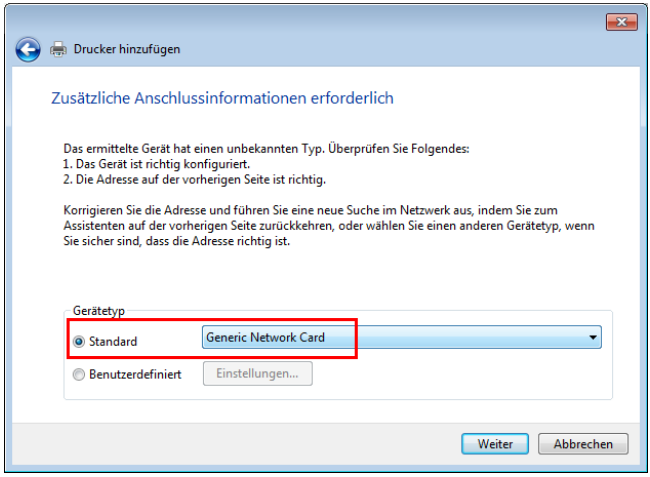
3. Wählen Sie die Option zum Erstellen eines neuen Druckeranschlusses.



4. Geben Sie die IP-Adresse des HiLCOS-Geräts als IP-Adresse für den Druckeranschluss ein. Der Name des Druckeranschlusses wird automatisch mit `IP_<IP-Address>` vorbelegt.

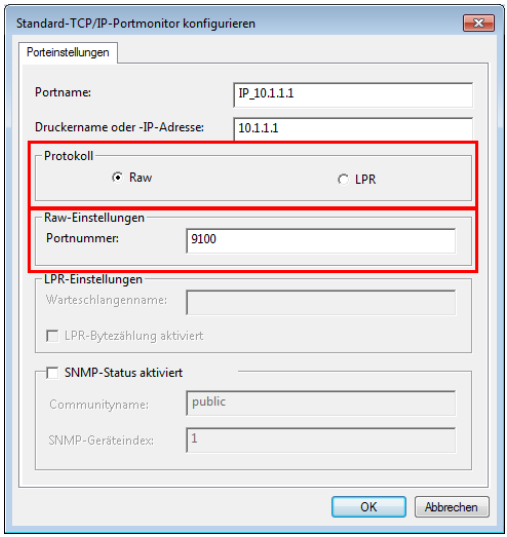


5. Wählen Sie als Gerätetyp die Option 'Standard' für eine 'Generic Network Card' aus. Wenn Sie die Standardeinstellungen beibehalten möchten (empfohlen), öffnen Sie mit der Schaltfläche **Weiter** den nächsten Dialog.



6. Alternativ können Sie mit der Auswahl 'Benutzerdefiniert' und der Schaltfläche **Einstellungen** einen zusätzlichen Dialog aufrufen. In diesem Dialog können Sie das Protokoll auswählen, das für die Übertragung der Druckaufträge zum Drucker am USB-Port des HiLCOS-Geräts verwendet werden soll ('Raw' – RawIP oder 'LPR'). Außerdem kann hier der zu verwendende

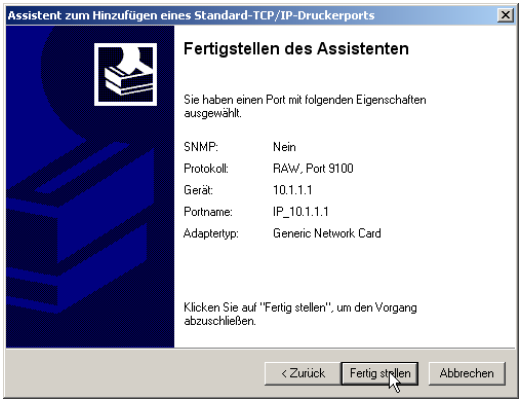
Port (nur bei RawIP) eingetragen werden. Bei LPR wird immer der Standard-Port '515' verwendet.



Hinweis: Die hier eingetragenen Optionen zu Protokoll und Port müssen mit den Einstellungen des Druckers in der HiLCOS-Konfiguration übereinstimmen.

Hinweis: Der Dialog zur Auswahl von Protokoll und Port kann auch später in der Systemsteuerung über die Eigenschaften eines Druckers auf der Registerkarte 'Anschlüsse' aufgerufen werden.

1. Mit diesen Einstellungen ist der Druckeranschluss fertig eingerichtet. Der Assistent fährt nun fort mit der Auswahl des Druckertreibers.



Hinweis: Weitere Informationen über die Installation des Druckertreibers entnehmen Sie bitte der Dokumentation des Drucker-Herstellers.

15.13 TACACS+

15.13.1 Einleitung

TACACS+ (Terminal Access Control Access Control Server) ist ein Protokoll für Authentifizierung, Authorisierung und Accounting (AAA), es stellt also den Zugang zu Netzwerkkomponenten nur für bestimmte Nutzer sicher, regelt die Berechtigungen der Benutzer und überträgt Daten für die Protokollierung der Netzwerknutzung. TACACS+ ist also eine Alternative zu anderen AAA-Protokollen wie RADIUS.

Hinweis: Der Einsatz von TACACS+ ist eine Voraussetzung für die Einhaltung der PCI-Compliance (Payment Card Industry).

Die Regelung der Zugriffsmöglichkeiten für die Anwender stellt in modernen Netzwerken mit zahlreichen Diensten und Netzwerkkomponenten eine große Herausforderung dar. Gerade in größeren Szenarien ist es kaum noch möglich, die Zugangsdaten der Benutzer auf jedem Gerät bzw. in jedem Dienst einzutragen und auf Dauer konsistent zu halten. Aus diesem Grund bietet sich die

zentrale Bereitstellung der Benutzerdaten auf einem entsprechenden Server an.

In einem einfachen Anwendungsbeispiel möchte sich ein Anwender auf einem Router anmelden und übermittelt dazu seine Zugangsdaten (User-ID) an den Router. Der Router fungiert in diesem Fall als Network Access Server (NAS): er überprüft die Zugangsdaten nicht selbst, sondern leitet diese an den zentralen AAA-Server weiter, der die Daten nach der Prüfung mit einen positiven Bestätigung (Accept) oder einer Ablehnung (Reject) beantwortet.

Zu den erweiterten Funktionen von TACACS+ gehört u.a. die Möglichkeit, den Benutzer zum Wechseln des Kennworts aufzufordern (z. B. beim ersten Login oder nach Ablauf einer bestimmten Frist). Die entsprechenden Meldungen werden vom NAS an den Benutzer weitergereicht.

Hinweis: Bitte beachten Sie, dass LANconfig nicht alle Meldungen des erweiterten Login-Dialogs auswerten kann. Falls LANconfig die Anmeldung an einem Gerät trotz korrekter Eingabe der Benutzerdaten ablehnt, melden Sie sich bitte über einen alternativen Konfigurationsweg an (WEBconfig oder Telnet).

Neben den weit verbreiteten RADIUS-Servern bietet sich als AAA-Server auch TACACS+ an. Die Tabelle zeigt einige wesentliche Unterschiede zwischen RADIUS und TACACS+:

TACACS+	*RADIUS*
Verbindungsorientierte Datenübertragung über TCP	Verbindungslose Datenübertragung über UDP
Gesamte Datenübertragung wird verschlüsselt	Nur Kennwort wird verschlüsselt, Inhalte bleiben unverschlüsselt
Vollständige Trennung von Authentifizierung, Authorisierung und Accounting möglich	Authentifizierung, Authorisierung sind kombiniert

- Die Übertragung über TCP macht TACACS+ zuverlässiger als RADIUS, da die Kommunikation zwischen NAS und AAA-Server bestätigt wird und der NAS somit informiert wird, wenn der AAA-Server nicht erreichbar ist.

- TACACS+ verschlüsselt neben dem Kennwort die gesamten Nutzdaten (bis auf den TACACS+-Header). Dadurch können auch Informationen wie der Benutzername oder die erlaubten Dienste nicht abgehört werden. TACACS+ benutzt zur Verschlüsselung ein One-Time-Pad, welches auf MD5-Hashes basiert.
- Die Trennung der drei AAA-Funktionen erlaubt unter TACACS+ schließlich die Nutzung anderer Server. Während bei RADIUS Authentifizierung und Authorisierung immer zusammen gehören, kann TACACS+ Authentifizierung und Authorisierung getrennt verwenden. So kann z. B. der TACACS+-Server nur für die Authentifizierung eingesetzt werden, dabei müssen auch nur die Benutzer, nicht aber die erlaubten Kommandos gepflegt werden.

Hinweis: Bitte beachten Sie: Auch wenn TACACS+ gezielt dazu genutzt wird, die Benutzerkonten nicht auf den einzelnen Geräten, sondern zentral auf einem AAA-Server abzulegen, sollten Sie auf jeden Fall für die Geräte ein sicheres Kennwort für den Root-Zugang definieren. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

15.13.2 Konfiguration der TACACS+-Parameter

Die Parameter für die Konfiguration von TACACS+ finden Sie auf folgenden Pfaden:

WEBconfig: HiLCOS-Menübaum / Setup / TACACS+

- Accounting

  Aktiviert das Accounting über einen TACACS+-Server. Wenn das TACACS+-Accounting aktiviert ist, werden alle Accounting-Daten über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

  Mögliche Werte:

  – aktiviert, deaktiviert

  Default

  – deaktiviert

Hinweis: Das TACACS+-Accounting wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist.

- Authentifizierung

  Aktiviert die Authentifizierung über einen TACACS+-Server. Wenn die TACACS+-Authentifizierung aktiviert ist, werden alle Authentifizierung-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

  Mögliche Werte:

  – aktiviert, deaktiviert

  Default

  – deaktiviert

  Hinweis: Die TACACS+-Authentifizierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Der Rückgriff auf lokale Benutzer kann dabei nur genutzt werden, wenn für das Gerät ein Root-Kennwort gesetzt ist. Bei Geräten ohne Root-Kennwort muss der Rückgriff auf lokale Benutzer deaktiviert werden, da sonst bei Ausfall der Netzwerkverbindung (TACACS+-Server nicht erreichbar) ein Zugriff ohne Kennwort auf das Gerät möglich wäre.

- Authorisierung

  Aktiviert die Authorisierung über einen TACACS+-Server. Wenn die TACACS+-Authorisierung aktiviert ist, werden alle Authorisierungs-Anfragen über das TACACS+-Protokoll an den konfigurierten TACACS+-Server übertragen.

  Mögliche Werte:

  – aktiviert, deaktiviert

  Default

  – deaktiviert

Hinweis: Die TACACS+-Authorisierung wird nur dann aktiviert, wenn ein erreichbarer TACACS+-Server definiert ist. Wenn die TACACS+-Authorisierung aktiviert ist, wird für jedes Kommando beim TACACS+-Server eine Anfrage gestellt, ob der Benutzer diese Aktion ausführen darf. Dementsprechend erhöht sich der Datenverkehr bei der Konfiguration, außerdem müssen die Rechte für die Benutzer im TACACS+-Server definiert sein.

- Rückgriff_auf_lokale_Benutzer

  Für den Fall, dass die definierten TACACS+-Server nicht erreichbar sind, kann ein Rückgriff auf die lokalen Benutzerkonten im Gerät erlaubt werden. So ist der Zugriff auf die Geräte auch bei Ausfall der TACACS+-Verbindung möglich, z. B. um die TACACS+-Nutzung zu deaktivieren oder die Konfiguration zu korrigieren.

  Mögliche Werte:

  - erlaubt, verboten

  Default

  - erlaubt

  Hinweis: Der Rückgriff auf lokale Benutzerkonten stellt ein Sicherheitsrisiko dar, wenn kein Root-Kennwort im Gerät gesetzt ist. Daher kann die TACACS+-Authentifizierung mit Rückgriff auf lokale Benutzerkonten nur aktiviert werden, wenn ein Root-Kennwort definiert ist. Wenn kein Root-Kennwort gesetzt ist, kann der Konfigurationszugang zu den Geräten aus Sicherheitsgründen gesperrt werden, wenn die Verbindung zu den TACACS+-Servern nicht verfügbar ist! In diesem Fall muss das Gerät möglicherweise in den Auslieferungszustand zurückgesetzt werden, um wieder Zugang zur Konfiguration zu erhalten.

- Shared-Secret

  Das Kennwort für die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

  Mögliche Werte:

  - 31 alphanumerische Zeichen

Default

– Leer

Hinweis: Das Kennwort muss im Gerät und im TACACS+-Server übereinstimmend eingetragen werden. Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen.

▶ SNMP-GET-Anfragen-Accounting

Zahlreiche Netzwerkmanagementtools nutzen SNMP, um Informationen aus den Netzwerkgeräten abzufragen. Auch der LANmonitor greift über SNMP auf die Geräte zu, um Informationen über aktuelle Verbindungen etc. darzustellen oder Aktionen wie das Trennen einer Verbindung auszuführen. Da über SNMP ein Gerät auch konfiguriert werden kann, wertet TACACS+ diese Zugriffe als Vorgänge, die eine Authorisierung voraussetzen. Da LANmonitor diese Werte regelmäßig abfragt, würde so eine große Zahl von eigentlich unnötigen TACACS+-Verbindungen aufgebaut. Wenn Authentifizierung, Authorisierung und Accounting für TACACS+ aktiviert sind, werden für jede Anfrage drei Sitzungen auf dem TACACS+-Server gestartet.

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für das Accounting zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Hinweis: Mit dem Eintrag einer Read-Only-Community unter HiLCOS-Menübaum / Setup / SNMP kann auch die Authentifizierung über TACACS+ für den LANmonitor deaktiviert werden. Die dort definierte Read-Only-Community wird dazu im LANmonitor als Benutzername eingetragen.

Mögliche Werte:

– nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von HiLCOS ein Accounting über den TACACS+-Server erforderlich.
– alle: In dieser Einstellung wird für alle SNMP-Zugriffe ein Accounting über den TACACS+-Server durchgeführt. Werden z. B. Status-Informa-

tionen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.

- keine: In dieser Einstellung ist für die SNMP-Zugriffe kein Accounting über den TACACS+-Server erforderlich.

Default:

- nur_für_SETUP_Baum

▶ SNMP-GET-Anfragen-Authorisierung

Mit diesem Parameter kann das Verhalten der Geräte bei SNMP-Zugriffen geregelt werden, um TACACS+-Sitzungen für die Authorisierung zu reduzieren. Eine Authentifizierung über den TACACS+-Server bleibt dennoch erforderlich, sofern die Authentifizierung für TACACS+ generell aktiviert ist.

Mögliche Werte:

- nur_für_SETUP_Baum: In dieser Einstellung ist nur bei SNMP-Zugriff auf den Setup-Zweig von HiLCOS eine Authorisierung über den TACACS+-Server erforderlich.
- alle: In dieser Einstellung wird für alle SNMP-Zugriffe eine Authorisierung über den TACACS+-Server durchgeführt. Werden z. B. Status-Informationen regelmäßig abgefragt, erhöht diese Einstellung deutlich die Last auf dem TACACS+-Server.
- keine: In dieser Einstellung ist für die SNMP-Zugriffe keine Authorisierung über den TACACS+-Server erforderlich.

Default:

- nur_für_SETUP_Baum

▶ Verschlüsselung

Aktiviert oder deaktiviert die Verschlüsselung der Kommunikation zwischen NAS und TACACS+-Server.

Mögliche Werte:

- aktiviert, deaktiviert

Default

- aktiviert

Hinweis: Eine Nutzung von TACACS+ ohne Verschlüsselung ist nicht zu empfehlen. Wenn die Verschlüsselung hier aktiviert wird, muss außerdem das Kennwort für die Verschlüsselung passend zum Kennwort auf dem TACACS+-Server eingetragen werden.

15.13.3 Konfiguration der TACACS+-Server

Zur Nutzung der TACACS+-Funktionen können zwei Server definiert werden. Dabei dient ein Server als Backup, falls der andere Server ausfällt. Beim Login über Telnet oder WEBconfig kann der Anwender den zu benutzenden Server auswählen.

Die Parameter für die Konfiguration der TACSACS-Server finden Sie auf folgenden Pfaden:

WEBconfig: HiLCOS-Menübaum / Setup / TACACS+ / Server

- Server-Adresse

  Adresse des TACACS+-Server, an den die Anfragen für Authentifizierung, Authorisierung und Accounting weitergeleitet werden sollen.

  Mögliche Werte:

  - Gültiger DNS-auflösbarer Name oder gültige IP-Adresse.

  Default

  - Leer

- Loopback-Adresse

  Hier können Sie optional eine Loopback-Adresse konfigurieren.

  Mögliche Werte:

  - Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
  - "INT" für die Adresse des ersten Intranets
  - "DMZ" für die Adresse der ersten DMZ
  - LB0 bis LBF für die 16 Loopback-Adressen
  - Beliebige gültige IP-Adresse

  Default

- Leer

▶ Kompatibilitätsmodus

TACACS+-Server werden in einer freien und in einer kommerziellen Version angeboten, die jeweils unterschiedliche Nachrichten verwenden. Der Kompatibilitätsmodus ermöglicht die Verarbeitung der Nachrichten von den freien TACACS+-Servern.

Mögliche Werte:

- aktiviert, deaktiviert

Default

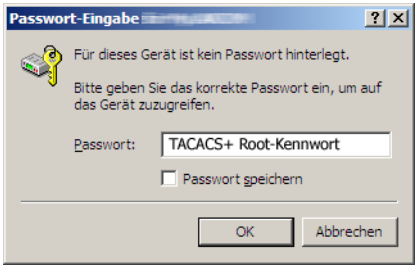
- deaktiviert

15.13.4 Anmelden am TACACS+-Server

Sobald die Verwendung von TACACS+ für die Authentifizierung und ggf. Authorisierung aktiviert ist, werden alle Logins auf dem Gerät an den TACACS+-Server weitergeleitet. Der weitere Ablauf des Logins unterscheidet sich je nach Zugangsart.

TACACS+-Anmeldung über LANconfig

Die Anmeldung über LANconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt ausschließlich über den Benutzer mit dem Namen “root”. Der Benutzer “root” muss entsprechend im TACACS+-Server konfiguriert sein. Geben Sie beim Login über LANconfig das Kennwort ein, dass im TACACS+-Server für den Benutzer “root” konfiguriert ist.

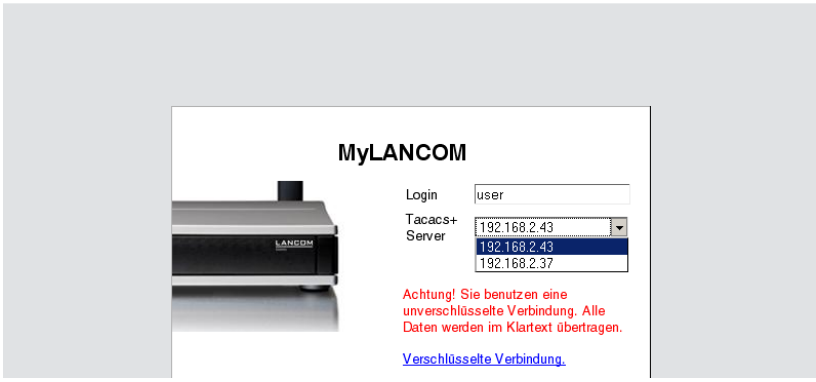


Hinweis: Der Benutzer “root” ist der einzige Benutzer, der nach Authentifizierung über TACACS+ automatisch die vollen Rechte eines Supervisors verfügt und somit die Konfiguration ohne Wechsel des Rechteniveaus bearbeiten darf. Wenn die Authorisierung benutzt wird entscheidet dies der TACACS+-Server.

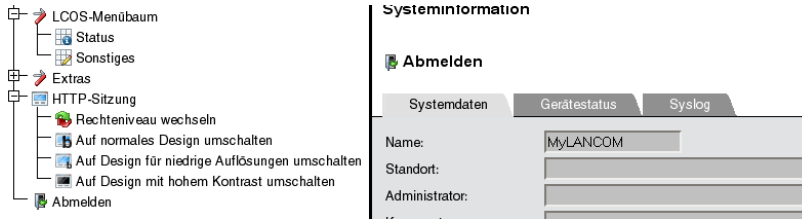
Hinweis: Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für den Benutzer “root” die Befehle “readconfig” und “writeconfig” erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät auslesen und nach Änderung wieder einspielen kann (*Rechtezuweisung unter TACACS+* auf Seite 1759).

TACACS+-Anmeldung über WEBconfig

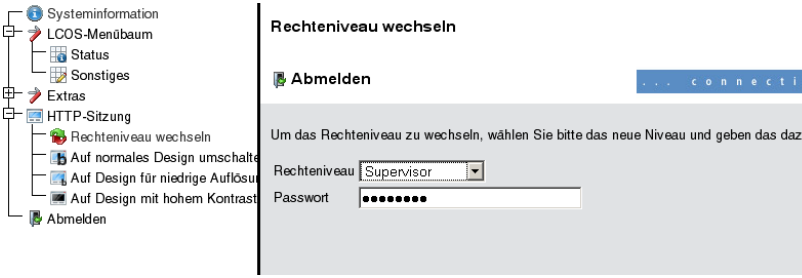
Die Anmeldung über WEBconfig an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind. Geben Sie beim Login über WEBconfig den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll.



Das zugehörige Kennwort wird im nächsten Dialog abgefragt. Nach dem Login sieht der Benutzer zunächst nur eine eingeschränkte WEBconfig-Oberfläche. Wenn die Autorisierung nicht genutzt wird, haben alle Benutzer (außer der Benutzer “root”) unter WEBconfig zunächst nur Leserechte.



Um weitere Rechte zu erhalten, klicken Sie im linken Bildschirmbereich den Link **Rechteniveau wechseln**.



In diesem Dialog wählen Sie gewünschten Benutzerrechte und geben das passende Kennwort ein.

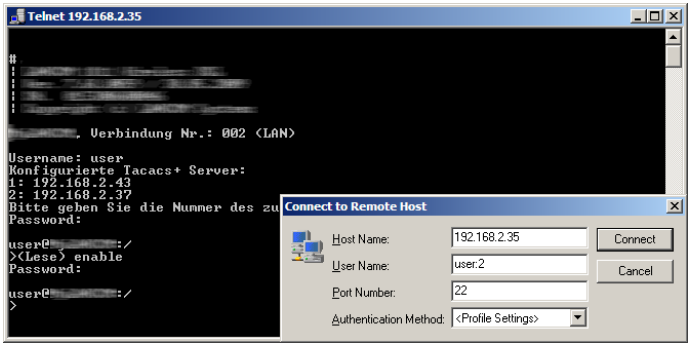
Hinweis: Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als “enable”-Kennwörter konfiguriert.

Hinweis: Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann (*Rechtezuweisung unter TACACS+* auf Seite 1759).

TACACS+-Anmeldung über Telnet oder SSH

Die Anmeldung über Telnet oder SSH an einem Gerät mit aktivierter TACACS+-Authentifizierung gelingt allen Benutzern, die im TACACS+-Server konfiguriert sind.

Geben Sie beim Login über Telnet den Benutzernamen ein, der im TACACS+-Server konfiguriert ist, und wählen Sie den Server aus, an dem die Authentifizierung vorgenommen werden soll. Beim Login über SSH geben Sie den gewünschten Server mit einem Doppelpunkt getrennt nach dem Benutzernamen ein, also entweder “user:1” oder “user:2”.



Nach dem Login haben alle Benutzer (außer dem Benutzer “root”) zunächst nur Leserechte.

Um weitere Rechte zu erhalten, geben Sie den Befehl `enable` ein und geben das Kennwort ein. Die Rechte werden dann entsprechend dem konfigurierten Kennwort zugewiesen. Das enable-Komando nimmt als Parameter die Zahlen 1-15. 1 ist das niedrigeste, 15 das höchste Niveau. Ohne Parameter wird automatisch 15 angenommen.

Hinweis: Die Kennwörter für die einzelnen Benutzerrechte werden dazu im TACACS+-Server als “enable”-Kennwörter konfiguriert.

Hinweis: Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen im TACACS+-Server für die jeweiligen Benutzer die gewünschten Befehle erlaubt werden, damit der Benutzer die Konfiguration aus dem Gerät einsehen und bearbeiten kann (*Rechtezuweisung unter TACACS+* auf Seite 1759).

15.13.5 Rechtezuweisung unter TACACS+

Die Rechte unter TACACS+ werden in bestimmten Leveln angegeben. Zur lokalen Authorisierung der Benutzer über das “enable”-Kommando unter Telnet/SSH bzw. das Rechteniveau unter WEBconfig werden die verschiedenen Admistratorenrechte von HiLCOS auf die TACACS+-Level abgebildet:

TACACS+-Level	*LCOS-Administratorenrechte*
0	No rights
1	Read-Only
3	Read-Write
5	Read-Only-Limited Admin
7	Read-Write-Limited Admin
9	Read-Only Admin
11	Read-Write Admin
15	Supervisor (Root)

15.13.6 Authorisierung von Funktionen

Wenn für das Gerät neben der Authentifizierung auch die Authorisierung aktiviert ist, müssen für die Konfiguration die entsprechenden Funktionen für den Benutzer im TACACS+-Server erlaubt sein. Tragen Sie die benötigten Werte in die Benutzerkonfiguration des TACACS+-Servers ein.

LANconfig

Befehl	*Argumente*	*Bemerkung*
readconfig	keine	Komplette Konfiguration auslesen
writeconfig	keine	Komplette Konfiguration schreiben

WEBconfig

Befehl	*Argumente*	*Bemerkung*
delRow	SNMP-ID der Tabelle	Zeile löschen
addRow	SNMP-ID der Tabelle	Zeile hinzufügen
editRow	SNMP-ID der Tabelle	Zeile bearbeiten

Befehl	*Argumente*	*Bemerkung*
modifyItem	SNMP-ID des Menüeintrags	Bearbeiten eines Menüeintrags
viewTable	SNMP-ID der Tabelle	Tabelle anzeigen
viewRow	SNMP-ID der Zeile	Zeile anzeigen
setValue	SNMP-ID des Menüeintrags	Wert eines Menüeintrags setzen
listmenu	SNMP-ID des Menüs	Untermenü anzeigen
action	SNMP-ID der Aktion	Ausführen einer Aktion
reboot	keine	Gerät neu starten
$URL	keine	Anzeige eines bestimmten URL

Hinweis: Für den Zugriff über WEBconfig müssen alle URLs freigeschaltet werden, die während der Konfiguration an den TACACS+-Server übertragen werden. Mit der URL "config2" erlauben Sie z. B. grundsätzlich den Zugriff auf den Konfigurationszweig von HiLCOS über WEBconfig. Zusätzlich müssen die einzelnen Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche URLs WEBconfig an den TACACS+-Server übermittelt, können Sie z. B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

Telnet/SSH

Befehl	*Argumente*	*Bemerkung*
dir	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
list	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
ls	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
llong	SNMP-ID des Verzeichnisses	Inhalt eines Verzeichnisses anzeigen
del	SNMP-ID der Tabelle	Zeile löschen
delete	SNMP-ID der Tabelle	Zeile löschen
rm	SNMP-ID der Tabelle	Zeile löschen
cd	SNMP-ID des Zielverzeichnisses	Verzeichnis wechseln

Befehl	*Argumente*	*Bemerkung*
add	SNMP-ID der Tabelle	Zeile hinzufügen
tab	SNMP-ID der Tabelle	Ändert die Reihenfolge der Spalten für das Hinzufügen von Werten
do	SNMP-ID der Aktion	Aktion ausführen
show	Name des Parameters	Information anzeigen
trace	Name des Parameters	Trace ausführen
time	Name des Parameters	Zeit einstellen
feature	Name des Parameters	Funktion hinzufügen
repeat	Name des Parameters	Befehl wiederholen
readmib	keine	SNMP-MIB auslesen (Hinweis beachten)
readconfig	keine	Komplette Konfiguration auslesen
readstatus	keine	Status-Menü auslesen
writefiash	keine	Firmware aktualisieren
activateimage	Name des Parameters	Anderes Firmware-Image aktivieren
ping	Name des Parameters	Starte Ping
wakeup	Name des Parameters	Sende Paket zum Aufwecken
linktest	Name des Parameters	WLAN-Linktest
writeconfig	keine	Komplette Konfiguration schreiben
ll2mdetect	keine	Starte LL2M-Erkennung
ll2mexec	Name des Parameters	LL2M-Befehl ausführen
scp	Name des Parameters	Sichere Kopie
rcp	Name des Parameters	Sichere Kopie
readscript	Name des Parameters	Skript auslesen
beginscript	keine	Start Skript
endscript	keine	Stop Skript
flash	Name des Parameters	Flash-Modus ein/ausschalten

Hinweis: Für den Zugriff über Telnet müssen alle Parameter freigeschaltet werden, die der Benutzer bearbeiten darf. Welche Werte Telnet an den TACACS+-Server übermittelt, können Sie z. B. mit dem entsprechenden Trace "trace+ tacacs" einsehen.

Hinweis: Der Befehl `readmib` ist nicht für aktuelle Geräte verfügbar. Die MIB aktueller Geräte können Sie über WEBconfig herunterladen (**Extras** > **SNMP-Geräte-MIB abrufen**).

SNMP

Befehl	*Argumente*	*Bemerkung*
get	SNMP-ID des Menüeintrags	Wert auslesen
set	SNMP-ID des Menüeintrags	Wert setzen

15.13.7 TACACS+-Umgehung

Einleitung

Mit der Nutzung von TACACS+ können alle Konfigurationsschritte auf einem Netzwerkgerät einer besonderen Prüfung (Autorisierung) unterzogen werden. Gleichzeitig können über das entsprechende TACACS+-Accounting die durchgeführten Konfigurationsschritte protokolliert und so nachvollziehbar gemacht werden. Die Verwendung von TACACS+ ist u. a. in Systemen für den elektronischen Zahlungsverkehr erforderlich (PCI-Compliance).

Die strikte Überwachung der ausgeführten Konfigurationsschritte führt allerdings zu einem zusätzlichen Austauschen von Anfragen und Nachrichten mit dem oder den verwendeten TACACS+-Servern. In großen Szenarien kann die TACACS+-Kommunikation bei der Verwendung von Scripten für zentrale Konfigurationsänderungen oder bei regelmäßigen Aktionen über CRON-Befehle zu einer Überlastung der TACSACS+-Server führen.

Konfiguration

Um eine mögliche Überlastung der TACACS+-Server durch automatisierte Konfigurationsschritte zu vermeiden, können die Verwendung von CRON, die Aktionstabelle und der Einsatz von Scripten von der Autorisierung und dem Accounting über TACACS+ ausgenommen werden.

WEBconfig: HiLCOS-Menübaum / Setup / TACACS+

- **Umgehe-Tacacs-fuer-CRON/Skripte/Aktions-Tabelle**

  Hier können Sie die Umgehung der TACACS-Autorisierung und des TACACS+-Accounting für verschiedene Aktionen aktivieren bzw. deaktivieren.

  Mögliche Werte:

  – Aktiviert, deaktiviert.

  Default:

  – Deaktiviert.

  Hinweis: Bitte beachten Sie, dass die Funktion von TACACS+ für das gesamte System über diese Optionen beeinflusst wird. Beschränken Sie die Nutzung von CRON, der Aktionstabelle und von Scripten auf jeden Fall auf einen absolut vertrauenswürdigen Kreis von Administratoren!

15.14 LLDP

Das Protokoll LLDP (Link Layer Discovery Protocol) bietet eine einfache und zuverlässige Möglichkeit für den Austausch von Informationen zwischen benachbarten Geräten im Netzwerk und für die Bestimmung der Topologie von Netzwerken. LLDP stellt durch das im Standard IEEE 802.1AB definierte Verfahren Funktionen zur Identifizierung einzelner Geräte und ganzer Netzwerkstrukturen zur Verfügung. Da das Protokoll auf Schicht 2 (Sicherungsschicht) des OSI-Schichtenmodells arbeitet und somit für die physikalische Adressierung von Geräten sorgt, ist seine Funktionalität nicht auf logische Netze wie IP-Netze begrenzt. LLDP deckt prinzipiell alle physikalisch erreichbaren Geräte eines Netzes ab.

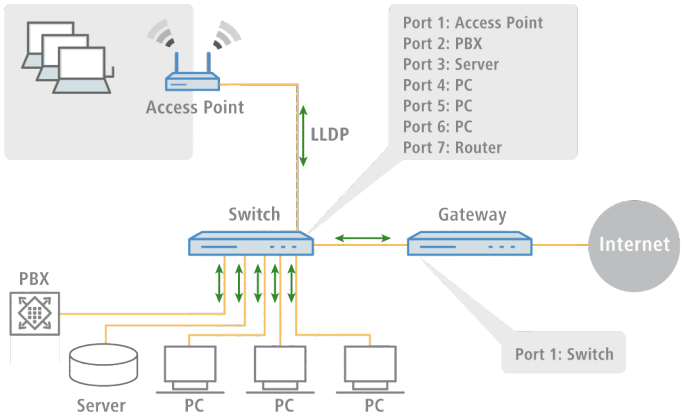
Insbesondere in komplexen Netzen bietet das herstellerunabhängige LLDP-Protokoll große Vorteile:

- Es ermöglicht die automatische Erkennung der in das Netz eingebundenen Komponenten wie Router, Switches und WLAN-Access-Points.

- Es vereinfacht die Einbindung unterschiedlichster Geräte, die den LLDP-Standard unterstützen, in ein bestehendes Netzwerk: Durch den Einsatz einer zentralen Netzwerk-Management-Software und automatisch ablaufende Prüf- und Diagnoseprozesse verringert sich der zeitliche Aufwand für Aufbau, Betrieb und Wartung eines Netzes.
- Die von den Geräten versendeten Informationen ergeben in ihrer Gesamtheit einen Überblick über die Topologie (d. h. den Aufbau und die Anordnung) des Netzes. Eine zentrale Management-Software stellt dem Administrator ein virtuelles Abbild des Netzes zur Verfügung, das sich bei Änderungen an der Topologie selbständig aktualisiert.
- Mit Hilfe einer Management-Software kann der Administrator auch komplexe Netze überwachen und auf einfache Weise verwalten. Er kann anhand der Software feststellen, welche Komponenten und Geräte zusammengeschaltet sind und auftretende Störungen problemlos lokalisieren.
- LLDP kann die Kosten für Anschaffung, Aufbau oder Umgestaltung eines Netzes verringern, da die Unternehmen durch diesen offenen Standard nicht mehr an bestimmte Hersteller gebunden sind. Sie können einzelne Netzkomponenten danach auswählen, für welche Anwendung diese jeweils am besten geeignet sind. Diese Möglichkeit war bislang nicht gegeben, wenn ein proprietäres Protokoll zum Einsatz kam.

15.14.1 Funktionsweise

LLDP funktioniert nach einem einfachen Prinzip: Auf allen Geräten mit LLDP-Unterstützung arbeitet der so genannte LLDP-Agent. Diese Software-Komponente sendet zum einen in regelmäßigen Abständen eigene Informationen an alle Schnittstellen des Gerätes. Dies erfolgt entweder mittels Unicast oder Multicast, wobei Sie die Zieladressen je nach Bedarf konfigurieren können. Zum anderen empfängt der LLDP-Agent laufend Informationen von benachbarten Geräten. Der Versand und der Empfang der betreffenden Datenpakete erfolgt unabhängig voneinander.



Die versendeten und empfangenen Datenpakete enthalten Informationen wie den Namen und die Beschreibung des Gerätes, die Kennung und Beschreibung von Ports, die IP- oder MAC-Adresse des Gerätes, die spezifischen Fähigkeiten des Gerätes (z. B. in Bezug auf Switching und Routing), VLAN-Kennungen und herstellerspezifische Details. Hierbei definiert LLDP grundlegende Informationen, die ein Datenpaket immer enthalten muss, sowie optionale zusätzliche Informationen.

Die einzelnen Geräte legen die empfangenen Informationen lokal in einer Datenstruktur ab, der so genannten MIB (Management Information Base). Eine MIB enthält somit Daten des eigenen LLDP-Agenten und des erkannten, direkten Nachbar-Agenten.

Der Informationsaustausch sorgt für eine ständige Identifikation der Geräte innerhalb des Netzwerks, da die Geräte ihre Datenpakete im Regelfall zyklisch (d. h. in konfigurierbaren Abständen) versenden. Darüber hinaus informieren sie ihre Netz-Nachbarn aber auch dann, wenn sich Änderungen innerhalb der Geräte oder an deren Netzanbindung ergeben.

Für den eigentlichen Prozess der Geräte-Identifizierung ist ausschlaggebend, dass jeder einzelne Verbindungspunkt in der Topologie als „Media Service Access Point“ (MSAP) eindeutig identifiziert ist. Ein MSAP setzt sich aus einer Gerätekennung (Chassis-ID) und einer Portkennung (Port-ID) zusammen. Die eindeutige Ermittlung bzw. Zuordnung von Geräten basiert also darauf, dass jeder MSAP in der beobachteten Netzwerk-Topologie nur einmal vorkommen darf.

Der Administrator kann die von den Geräten gemeldeten Daten dann über eine zentrale Netzwerk-Management-Software auf seinem Rechner abfragen und erfassen, wobei die Abfrage der einzelnen MIBs über das SNMP-Protokoll erfolgt. Die Management-Software dokumentiert somit die gesamte Topologie des Netzes und ermöglicht eine automatische Abbildung dieser Topologie sowie die grafische Darstellung von aktuellen Diagnosedaten.

Die Aktivierung von LLDP mittels LANconfig erfolgt unter **Schnittstellen** > **LAN**.

15.14.2 Aufbau der LLDP-Nachrichten

Der Austausch der Informationen erfolgt über spezifische Dateneinheiten, die so genannten LLDP Data Units (LLDPDU). Eine solche Dateneinheit besteht aus TLVs (Type-Length-Values), wobei jedes TLV-Feld einem bestimmten Typ entspricht und eine bestimmte Länge hat.

Gemäß LLDP-Standard IEEE 802.1AB müssen am Anfang einer LLDPU drei TLVs in der folgenden Reihenfolge stehen:

- Typ 1 = Chassis-ID
- Typ 2 = Port-ID
- Typ 3 = Time To Live

Im Anschluss an diese verbindlichen TLVs kann eine LLDPDU weitere, optionale TLVs enthalten:

- Typ 4 = Port Description
- Typ 5 = System Name
- Typ 6 = System Description
- Typ 7 = System Capabilities
- Typ 8 = Management Address

Am Ende einer LLDPDU muss dann zwingend folgende TLV stehen:

- Typ 0 = End of LLDPDU

Tabellarische Übersicht über die TLVs

TLV	Verwendung	Bezeichnung	Beispiel	Funktion
Typ 1	Erforderlich	Chassis-ID	0018.2fa6.b28c	Identifiziert das Gerät
Typ 2	Erforderlich	Port-ID	Fi-0/12	Identifiziert den Port
Typ 3	Erforderlich	Time To Live	60 sec	Signalisiert dem empfangenden Gerät, wie lange die erhaltene Information gültig sein soll
Typ 4	Optional	Port Description	GigabitEthernet0/12	Zeigt Details über den Port wie etwa die Hardware-Version an
Typ 5	Optional	System Name	PN-I/O 3	Zeigt den vom Administrator vergebenen Namen des Gerätes an
Typ 6	Optional	System Description	LCOS Software, Version 8.9.1 SE	Zeigt Details über das Gerät wie etwa die Version der Netzwerk-Software an
Typ 7	Optional	System Capabilities	Router	Zeigt die primäre Funktion sowie die Fähigkeiten des Gerätes an
Typ 8	Optional	Management Address	192.168.0.1	Zeigt die IP- oder MAC-Adresse des Gerätes an

TLV	Verwendung	Bezeichnung	Beispiel	Funktion
Typ 0	Erforderlich	End of LLDPDU	----------	Signalisiert das Ende der Dateneinheit

15.14.3 Unterstützte Betriebssysteme

Grundsätzlich funktioniert LLDP auf allen gängigen Systemen, sofern hierfür LLDP-Agenten bzw. eine entsprechende Software zur Auswertung der LLDP-Pakete zur Verfügung stehen. Für Linux gibt es diverse Open-Source-Projekte wie z. B. „LLDPD“, „Open-LLDP“ (mit Bindestrich) oder „ladvd“, die einen LLDP-Agenten bereitstellen.

Das Projekt „OpenLLDP“ zielt auf eine weitere Verbreitung und Akzeptanz des LLDP-Protokolls (IEEE 802.1AB) ab. Die Software unterstützt die Übertragung und den Empfang von LLDP-Nachrichten auf den Plattformen Linux, Mac OS X, FreeBSD und NetBSD. Allerdings scheint die Weiterentwicklung derzeit zu ruhen.

Die Microsoft-Betriebssysteme Vista und Windows 7 enthalten ein proprietäres Protokoll namens LLTD (Link Layer Topology Discovery), welches im Wesentlichen die gleiche Funktionalität wie LLDP aufweist. Auf Windows XP lässt sich die LLTD-Komponente über einen Patch nachinstallieren. Allerdings ist die Funktion des Patches gegenüber den implementierten Varianten in Vista und Windows 7 eingeschränkt, da der „ LLTD Responder“ nur IPv4-Adressen meldet, nicht jedoch IPv6-Adressen.

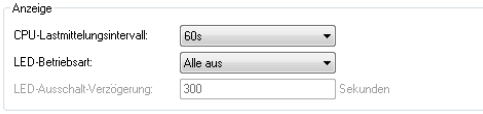
Will man auf Windows-Systemen LLDP installieren, kann man auf eine Shareware namens „haneWIN LLDP Agent“ zurückgreifen. Mit dieser funktioniert LLDP auf allen Windows-Systemen ab Windows 2000, d. h. sowohl auf 32-Bit- wie auf 64-Bit-Systemen.

Die am weitesten verbreitete freie Software zur Auswertung und Analyse ist Wireshark. In der Grundversion ist Wireshark gratis und hat sich inzwischen als Standard etabliert. Die Software unterstützt zahlreiche Betriebssysteme und kann eine Vielzahl von Protokollen (u. a. auch LLDP) lesen und auswerten. Der Schwerpunkt der Grundversion von Wireshark liegt allerdings auf der Analyse von auftretenden Problemen innerhalb des Netzes. Benötigt man weitergehende Funktionen (wie z. B. die Visualisierung des Netzverkehrs in Form von farbigen Diagrammen), kann man kostenpflichtige Zusatzmodule erwerben.

15.15 Geräte-LEDs bootpersistent ausschalten

Um einen Access Point unauffällig zu betreiben, können Sie die Betriebs- und Status-LEDs am Gerät deaktivieren. Auch nach einem Neustart bleiben die LEDs ausgeschaltet. Sie können allerdings auch festlegen, dass die LEDs kurz nach einem Neustart für eine bestimmte Zeit leuchten sollen, bevor das Gerät sie deaktiviert. Das ist z. bei von WLAN-Controllern verwalteten Access Points hilfreich, um den Verbindungsaufbau zum WLAN-Controller verfolgen zu können.

Die LED-Betriebsart können Sie unter **Management** > **Erweitert** im Abschnitt **Anzeige** festlegen.



In der Auswahlliste **LED-Betriebsart** stehen drei Optionen zur Auswahl:

Normal
: Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Alle aus
: Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Verzögert aus
: Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

Hinweis: Die Funktion "LED-Test" lässt sich trotz deaktivierter LEDs ausführen.

Hinweis: Wenn Sie diesen Wert innerhalb der zuvor eingestellten Dauer ändern und speichern, starten Sie den Timer neu.