LANCOM Referenzhandbuch
Addendum zur LCOS- Version 7.6

Revision 1 (Dezember 2008)

LANCOM
Systems

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Dezember 2008

A Addendum zur LCOS-Version 7.6

A.1 Übersicht

Dieses Addendum beschreibt die neuen Funktionen und Änderungen zwischen der LCOS-Version 7.5 und der aktuellen Version 7.6:

- Konfiguration
  - Telnet: Erweiterte Funktionen zum Editieren der Befehle
  - Telnet: Programmierung von Funktionstasten für die Konfiguration
  - WEBconfig: Neue Weboberfläche mit umfangreichem Geräte-Status, Online-Hilfe etc.
  - Dateien von einem TFTP oder HTTP-Server direkt in das Gerät laden
  - Rechteverwaltung für verschiedene Administratoren – Administratoren ohne Trace-Rechte
  - Asymmetrisches Firmsafe
  - LANconfig: Übertragen von Gerätekonfigurationen auf ähnliche Modelle
  - LANconfig: Automatisches Anlegen von Konfigurations-Backups vor Firmware-Uploads, Konfigurationsänderung und Skriptausführung
  - LANconfig: Anpassen der Symbolleiste
  - LANconfig: Objektorientierte Konfiguration der Firewall-Regeln (siehe Firewall)
  - LL2M: LANCOM Layer 2 Management Protokoll
- Diagnose
  - LANmonitor: Speichern von Support-Dateien mit Trace-Daten, Geräte-Konfiguration, Bootlog und Sysinfo
  - LANmonitor: Automatische Sicherung der Trace-Daten
  - LANmonitor: Trace-Konfiguration mit Assistenten
  - LANmonitor: Ausgabe von Show-Kommandos
  - LANmonitor: Ausgabe von Status-Informationen und Statistiken
  - LANmonitor: SSL-verschlüsselte Telnet-Verbindung
  - SYSLOG-Anzeige in LANmonitor und WEBconfig
- WAN
  - Flexible Auswahl der PPP-Authentifizierungsprotokolle
  - Die Aktions-Tabelle
  - Unterstützung des GnuDIP-Protokolls
  - COM-Port-Forwarding, Verwendung der seriellen Schnittstellen für TCP-Verbindungen
  - Flexible Definition der WAN-RIP-Gegenstellen mit Platzhaltern
  - Schnittstellen-Tags für Gegenstellen
- VPN
  - Unbegrenzte Anzahl der VPN-Gegenstellen
  - Extended Authentication Protocol (XAUTH)
  - Backup über alternative VPN-Verbindung
  - Mehrstufige Zertifikate für SSL/TLS
- Firewall
  - Objektorientierte Konfiguration der Firewall-Regeln mit LANconfig
  - Beschränkung einer Firewall-Regel auf Backup-Verbindungen
  - Beschränkung einer Firewall-Regel auf die Verbindungen einer Station
  - Vorgabe einer maximalen Anzahl von Verbindungen
  - Vorgabe eines prozentualen Anteils der Bandbreite
- Voice over IP

  Angabe der folgenden Parameter für SIP-Provider- und SIP-PBX-Lines:
  - Lokale-Portnummer
  - (Re-)Registrierung
  - Leitungsüberwachung
  - Überwachungsintervall
  - Vertrauenswürdig
  - Privacy-Methode

Angabe des folgenden Parameters für ISDN- und SIP-User:

- □ CLIR

Angabe der folgenden Parameter für Analog-Lines:

- □ Caller-ID Signaling
- □ Caller-ID Transmission Requirements

- WLAN
  - □ WLAN: Paket-Forwarding per SSID einstellbar
  - □ Mehrstufige Zertifikate für PublicSpot
  - □ DFS 2, Version 1.4: Freilassen von Kanälen für Wetter-Radar
  - □ Zentrales WLAN-Management: Interner Skript-Speicher (Skript-Management ohne HTTP-Server)
- Meldungen
  - □ SNMP-Traps: Trapversion konfigurierbar
- RADIUS
  - □ VLAN-ID in der Tabelle der RADIUS-Benutzer
  - □ Maskierung auf rufende und gerufene Station in der Tabelle der RADIUS-Benutzer
- DHCP
  - □ BOOTP: Zuweisen von unterschiedlichen IP-Adressen in Abhängigkeit vom IP-Netzwerk
- Sonstige Änderungen
  - □ Zugangslisten mit Routing-Tags

B Konfiguration

B.1 Die Konfiguration mit verschiedenen Tools

B.1.1 Telnet

Neu mit LCOS 7.6:

- Erweiterte Funktionen zum Editieren der Befehle
- Funktionstasten

Telnet-Sitzung starten

Über Telnet starten Sie die Konfiguration z.B. aus der Windows-Kommandozeile mit dem Befehl:

```
C:\>telnet 10.0.0.1
```

Telnet baut dann eine 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.

Linux und Unix 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. Die verschlüsselte Telnet-Verbindung wird dann mit dem folgenden Befehl gestartet:

```
C:\>telnet -z ssl 10.0.0.1 telnets
```

Die Sprache der Konsole auf Deutsch ändern

Der Terminalmodus steht in den Sprachen Deutsch und Englisch zur Verfügung. LANCOM Geräte werden werkseitig auf Englisch als Konsolensprache eingestellt. Im weiteren Verlauf dieser Dokumentation werden alle Konfigurationsbefehle in ihrer deutschen Form angegeben. Zur Änderung der Konsolensprache auf Deutsch verwenden Sie folgende Befehle:

Konfigurationstool	Aufruf (bei Englisch als eingestellter Konsolensprache)
WEBconfig	Expertenkonfiguration ▶ Config-Module ▶ Language
Telnet	`set /Setup/Config-Module/Language Deutsch`

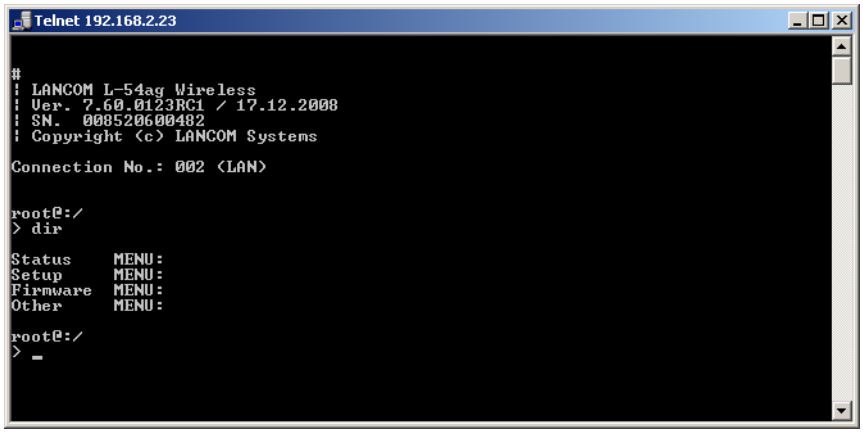
Telnet-Sitzung beenden

Um die Telnet-Sitzung zu beenden, geben Sie an der Eingabeaufforderung den Befehl `exit` ein:

```
C:\>exit
```

Die Struktur im Kommandozeilen-Interface

Das LANCOM Kommandozeilen-Interface ist stets wie folgt strukturiert:



- **Status**
  Enthält die Zustände und Statistiken aller internen Module des Gerätes
- **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 Kommandozeile

Das LANCOM Kommandozeilen-Interface kann mit den folgenden DOS- oder UNIX-ähnlichen Befehlen bedient werden. Die verfügbaren LCOS-Menübefehle können durch Aufrufen des HELP-Kommandos jederzeit auf der Kommandozeile angezeigt werden.

Zum Ausführen einiger Befehle sind Supervisor-Rechte erforderlich.

Befehl	Beschreibung
beginscript	Versetzt eine Konsolensitzung in den Script-Modus. In diesem Zustand werden die im Folgenden eingegebenen Befehle nicht direkt in den Konfigurations-RAM im LANCOM übertragen, sondern zunächst in den Script-Speicher des Gerätes.
cd [PFAD]	Wechselt das aktuelle Verzeichnis. Verschiedene Kurzformen werden unterstützt, z.B. "cd ../.." kann verkürzt werden zu "cd ..." etc.
del [PFAD]*	Löscht eine komplette Tabelle in dem mit `Path` angegebenen Zweig des Menübaums.
default [-r] [PFAD]	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.
dir [PFAD] list [PFAD] ls [PFAD] ll [PFAD]	Zeigt den Inhalt des aktuellen Verzeichnisses an. Der angehängte Parameter „-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.
do [PFAD] [<Parameter>]	Führt die Aktion [PATH] im aktuellen Verzeichnis aus. Zusätzliche Parameter können mit angegeben werden.
echo <ARG>...	Argument auf Konsole ausgeben
exit/quit/x	Beendet die Kommandozeilen-Sitzung
feature <code>	Freischaltung eines SW-Features mit dem angegebenen Feature-Code
flash Yes/No	Die Änderungen an der Konfiguration über die Befehle an der Kommandozeile werden standardmäßig (flash yes) direkt in den boot-resistenten Flash-Speicher der Geräte geschrieben. Wenn das Aktualisieren der Konfiguration im Flash unterdrückt wird (flash no), werden die Änderungen nur im RAM gespeichert, der beim Booten gelöscht wird.
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.
killscript	Löscht den noch nicht verarbeiteten Inhalt einer Scriptsession. Die Scriptsession wird über den Namen ausgewählt.
loadconfig	Konfiguration per TFTP-Client in das Gerät laden
loadfirmware	Firmware per TFTP-Client in das Gerät laden
loadscript	Script per TFTP-Client in das Gerät laden
passwd	Ändern des Passworts
passwd -n neues [altes]	Passwort ändern (Keine Eingabeaufforderung)
ping [IP-Adresse oder Name]	Sendet einen ICMP echo request an die angegebene IP-Adresse
readconfig	Anzeige der kompletten Konfiguration in der Geräte-Syntax
readmib	Anzeige der SNMP Management Information Base
readscript [-n] [-d] [-c] [-m] [PFAD]	Erzeugt in einer Konsolensitzung eine Textausgabe von allen Befehlen und Parametern, die für die Konfiguration des LANCOM im aktuellen Zustand benötigt werden.
repeat <INTERVAL> <Kommando>	Wiederholt das Kommando alle INTERVALL Sekunden, bis der Vorgang durch neue Eingaben beendet wird
sleep [-u] Wert[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 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
set [PFAD] <Wert(e)>	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.

Befehl	Beschreibung
set [PFAD] ?	Auflistung der möglichen Eingabewerte für einen Konfigurationsparameter. Wird kein Name angegeben, so werden die möglichen Eingabewerte für alle Konfigurationsparameter im aktuellen Verzeichnis angegeben
setenv <NAME> <WERT>	Umgebungsvariable setzen
unsetenv <NAME>	Umgebungsvariable löschen
getenv <NAME>	Umgebungsvariable ausgeben (kein Zeilenvorschub)
printenv	Komplette Umgebung ausgeben
show <Optionen>	Anzeige spezieller interner Daten. show ? zeigt alle verfügbaren Informationen an, z.B. letzte Boot-Vorgänge ('bootlog'), Firewall Filterregeln ('filter'), VPN-Regeln ('VPN') und Speicherauslastung ('mem' und 'heap')
sysinfo	Anzeige der Systeminformationen (z.B. Hardware/Softwareversion etc.)
testmail	Schickt eine E-Mail. Parameter siehe 'testmail ?'
time	Zeit setzen (TT.MM.JJJJ hh:mm:ss)
trace […]	Konfiguration der Diagnose-Ausgaben.
who	Aktive Sitzungen auflisten
writeconfig	Laden einer neuen Konfigurationsfile in der Geräte-Syntax. Alle folgenden Zeilen werden als Konfigurationswerte interpretiert, solange bis zwei Leerzeilen auftreten
writeflash	Laden einer neuen Firmware-Datei (nur via TFTP)
!!	Letztes Kommando wiederholen
!<num>	Kommando <num> wiederholen
!<prefix>	Letztes mit <prefix> beginnendes Kommando wiederholen
#<blank>	Kommentar

- PFAD:
  - Pfadname für ein Menü oder einen Parameter, getrennt durch / oder \
  - .. bedeutet eine Ebene höher
  - . bedeutet aktuelle Ebene
- WERT:
  - möglicher Eingabewert
  - "" ist ein leerer Eingabewert
- NAME:
  - Sequenz von _ 0..9 A..Z
  - erstes Zeichen darf keine Ziffer sein
  - keine Unterscheidung Gross/Kleinschreibung
- 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.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.
- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Parameter aufgerufen wird. Zum Beispiel zeigt der Aufruf '`ping ?`' die Optionen des eingebauten ping Kommandos an.
- Eine vollständige Auflistung der zur Verfügung stehenden Konsolen-Kommandos erhalten Sie durch die Eingabe von '`?`' auf der Kommandozeile.

Funktionen zum Editieren der Befehle

Mit den folgenden Befehlen können die Befehle auf der Kommandozeile bearbeitet werden. Die "ESC key sequences" zeigen zum Vergleich die Tastenkombinationen, die auf typischen VT100/ANSI-Terminals verwendet werden:

Funktion	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 Telnet-Sitzung, 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: ■ Wenn es genau eine Möglichkeit gibt, den Befehl bzw. den Pfad zu vervollständigen, so wird diese Möglichkeit in die Zeile übernommen. ■ 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. ■ 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.

Funktionstasten für die Kommandozeile

■ Telnet: Setup ▶ Config ▶ Funktionstasten

Mit den Funktionstasten haben Sie die Möglichkeit, häufig genutzte Befehlssequenzen zu speichern und an der Kommandozeile komfortabel aufzurufen. In der entsprechenden Tabelle werden den Funktionstasten F1 bis F12 die Befehle so zugeordnet, wie sie an der Kommandozeile eingegeben werden.

■ **Taste**

Bezeichnung der Funktionstaste.

Mögliche Werte:

□ Auswahl aus den Funktionstasten F1 bis F12.

Default:

□ F1

■ **Abbildung**

Beschreibung des Befehls bzw. der Tastenkombination, die bei Aufruf der Funktionstaste an der Kommandozeile ausgeführt werden soll.

Mögliche Werte:

□ Alle an der Kommandozeile möglichen Befehle bzw. Tastenkombinationen

Default:

□ Leer

Besondere Werte:

□ Das Caret-Zeichen ^ wird verwendet, um spezielle Steuerungsbefehle mit ASCII-Werten unterhalb von 32 abzubilden.^a

□ ^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 ^.

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.

B.1.2 WEBconfig

Neu mit LCOS 7.6:

■ Neues WEBconfig mit Suchfunktion, umfangreichem Geräte-Status, Online-Hilfe etc.

Sie können die Einstellungen des Gerätes über einen beliebigen Webbrowser vornehmen. Im LANCOM ist die Konfigurationssoftware WEBconfig integriert. Sie benötigen lediglich einen Webbrowser, um auf WEBconfig zuzugreifen. WEBconfig bietet ähnliche Setup-Assistenten wie LANconfig an und bietet damit optimale Voraussetzungen für eine komfortable Konfiguration des LANCOM – im Unterschied zu LANconfig aber unter allen Betriebssystemen, für die es einen Webbrowser gibt.

Sicher mit HTTPS

WEBconfig bietet zur sicheren (Fern-) Konfiguration die Möglichkeit der verschlüsselten Übertragung der Konfigurationsdaten über HTTPS.

```
https://<IP-Adresse oder Gerätename>
```

Für maximale Sicherheit sollten Sie stets die neueste Version Ihres Browsers verwenden. Unter Windows empfiehlt LANCOM Systems GmbH den aktuellen Internet Explorer.

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 LANCOM, 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 LANCOM-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.

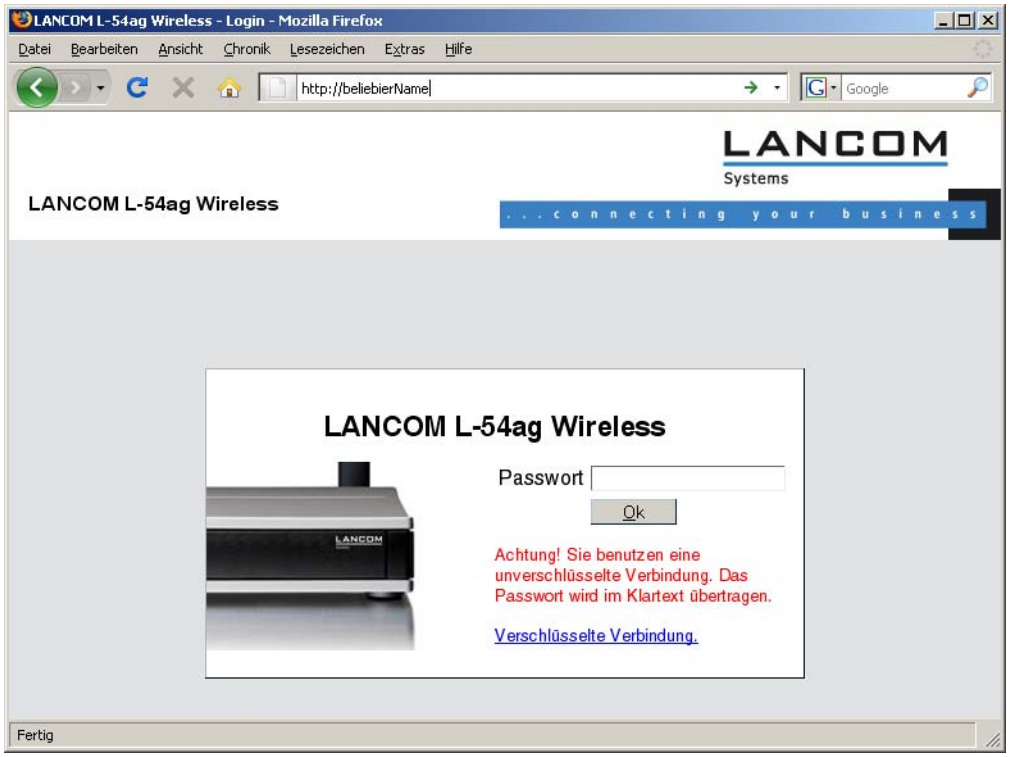
Wird ein LANCOM Wireless Router oder ein LANCOM Access Point von einem LANCOM WLAN Controller zentral verwaltet, dann wird beim Zuweisen der WLAN-Konfiguration auch der DHCP-Server vom Auto-Modus in den Client-Modus umgeschaltet.

Netz ohne DHCP-Server

Nicht für zentral verwaltete LANCOM Wireless Router oder LANCOM Access Points

In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-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.

Im werksseitigen Auslieferungszustand mit aktiviertem DHCP-Server leitet das Gerät alle eingehenden DNS-Anfragen an den internen Webserver weiter. Dadurch können unkonfigurierte LANCOMs einfach durch Eingabe eines beliebigen Names mittels eines Webbrowsers angesprochen und in Betrieb genommen werden.



Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-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 LANCOM 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 LANCOM-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 unter dem Namen "-<MAC-Adresse>" (z.B. "-00a057xxxxxx") erreicht werden.

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

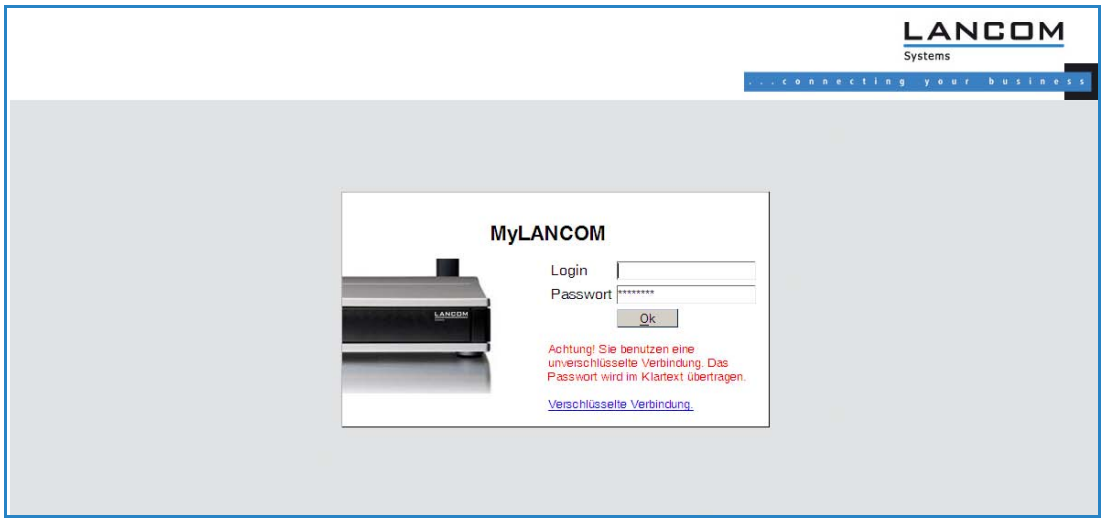
- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
  - □ Sie nutzen die Funktion "Geräte suchen" in LANconfig oder die Gerätesuche unter WEBconfig von einem anderen erreichbaren LANCOM.
  - □ Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
  - □ Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschließen.

Login

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 verwenden, tragen Sie nur das entsprechende Kennwort ein. Das Feld Benutzername bleibt in diesem Fall leer.

Der Login-Dialog bietet alternativ einen Link für eine verschlüsselte Verbindung über HTTPS. Nutzen Sie nach Möglichkeit immer die HTTPS-Verbindung mit erhöhter Sicherheit.



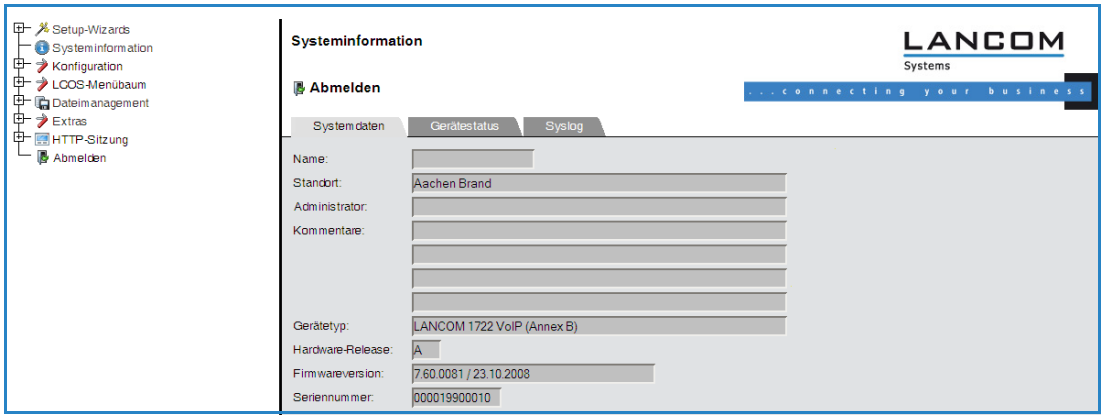
Setup Wizards

Mit den Setup-Wizards können Sie schnell und komfortabel die häufigsten Einstellungen für ein Gerät vornehmen. Wählen Sie dazu den gewünschten Assistenten aus und geben Sie auf den folgenden Seiten die benötigten Daten ein.

Die Einstellungen werden erst dann in das Gerät gespeichert, wenn Sie die Eingaben auf der letzten Seite des Assistenten bestätigen.

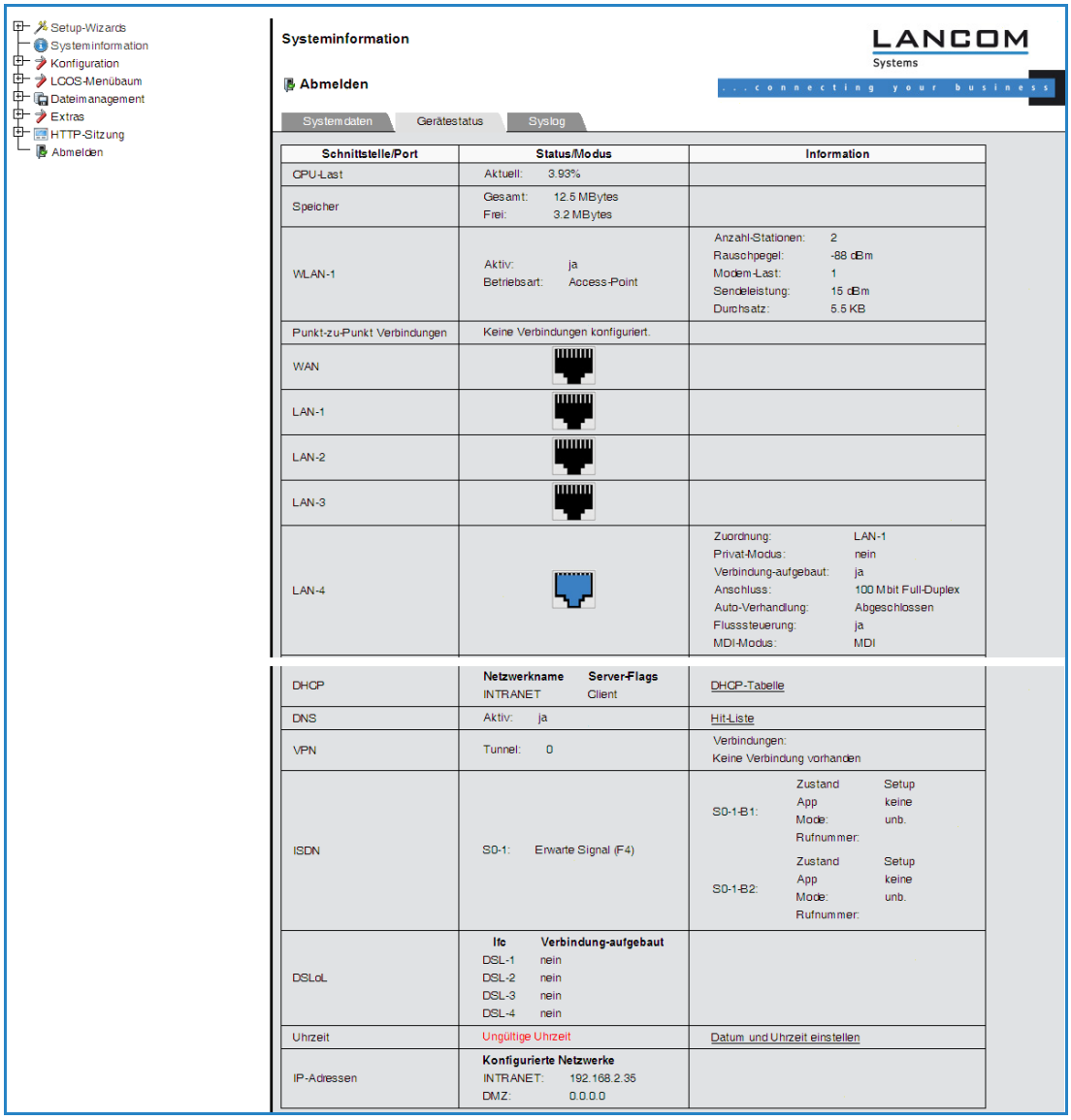
Systeminformation

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

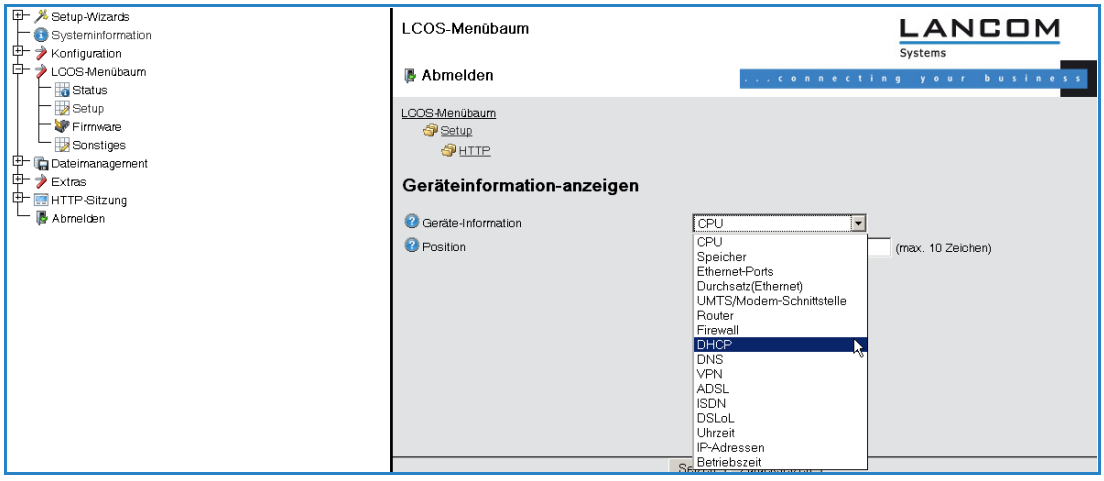


Auf der Registerkarte “Systemstatus” finden Sie umfangreiche Informationen über den aktuellen Betriebszustand des Gerätes. Dazu gehört z. B. die visuelle Darstellung der Schnittstellen mit Angabe der darauf aktiven Netzwerke. Über entsprechende Links können relevante weitere Statistiken aufgerufen werden (z. B. DHCP-Tabelle). Bei wesentlichen

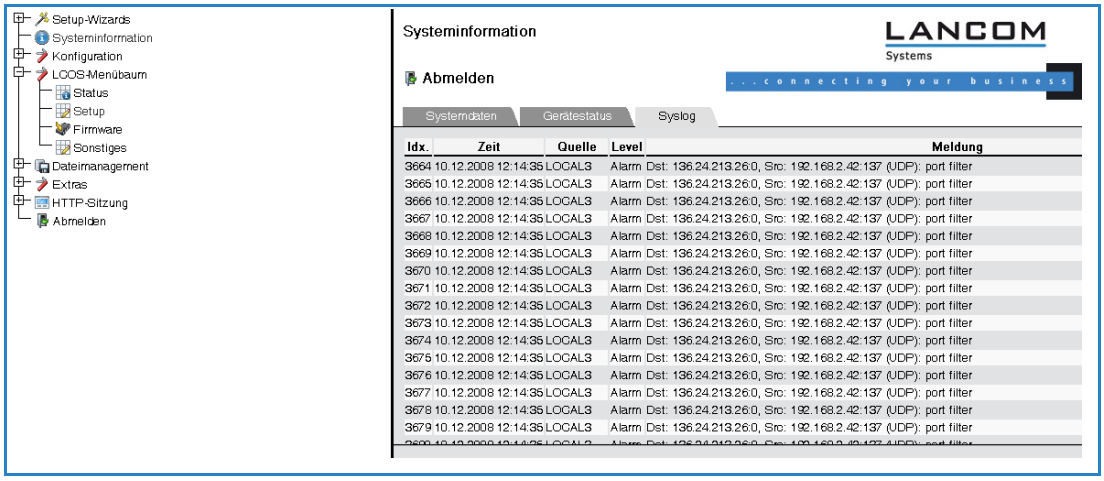
Mängeln in der Konfiguration (z. B. ungültige Zeiteinstellung) wird ein direkter Link zu den entsprechenden Konfigurationsparametern angeboten.



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



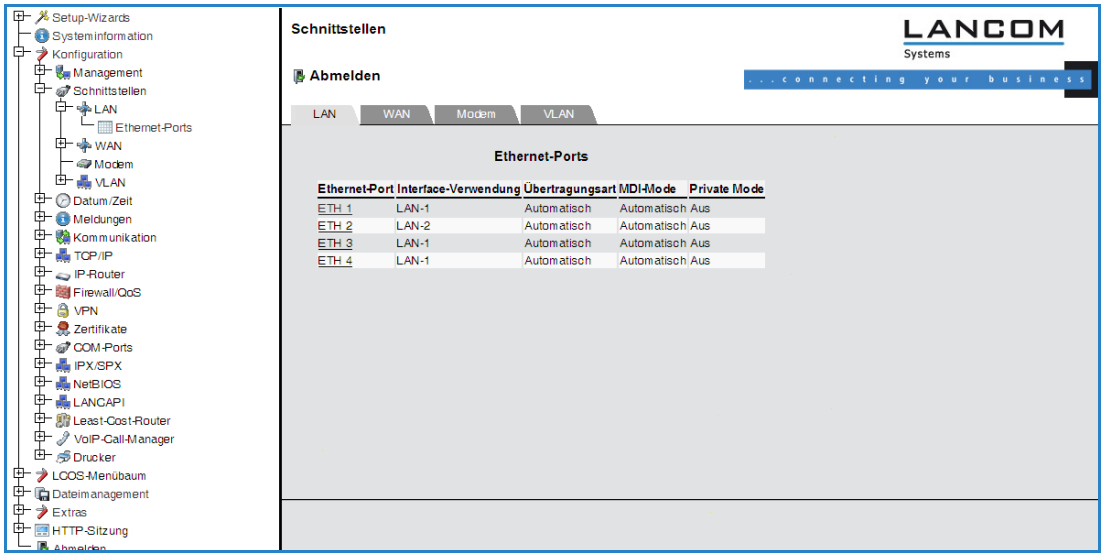
LANCOM-Geräte legen Syslog-Informationen auch im Arbeitsspeicher ab (siehe dazu Syslog). Die letzten Ereignisse können zur Diagnose auch über WEBconfig auf der Registerkarte “Systemstatus” eingesehen werden.



Konfiguration

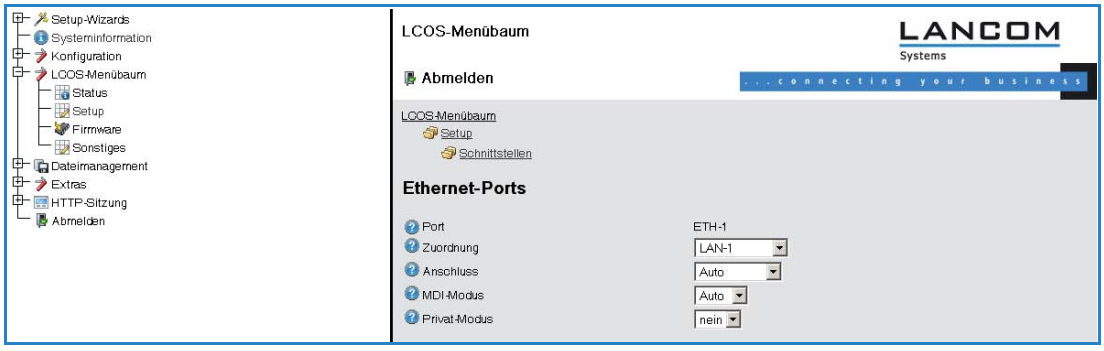
Der Menübereich "Konfiguration" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch bei LANconfig verwendet wird.

Bitte beachten Sie, dass über diese Darstellung der Konfiguration nicht alle Einstellungen vorgenommen werden können.



LCOS-Menübaum

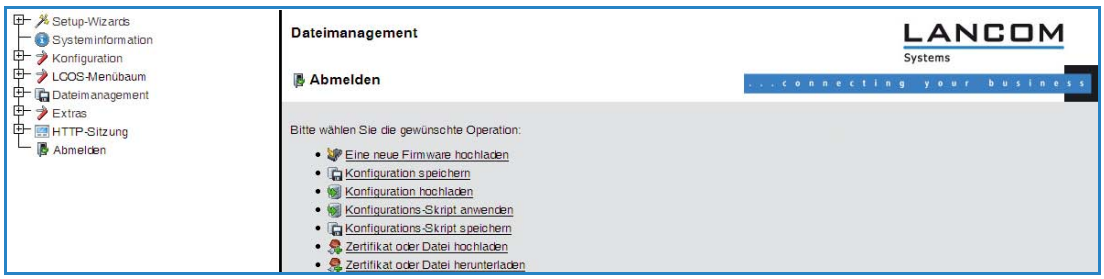
Der Menübereich "LCOS-Menübaum" bietet die Konfigurationsparameter in der gleichen Struktur an, wie Sie auch unter Telnet verwendet wird. Mit einem Klick auf das Fragezeichen können Sie für jeden Konfigurationsparameter eine Hilfe aufrufen.



Dateimanagement

Im Menübereich "Dateimanagement" finden Sie alle Aktionen, mit denen Dateien aus dem Gerät heruntergeladen oder in das Gerät hochgeladen werden:

- Eine neue Firmware hochladen
- Konfiguration speichern
- Konfiguration hochladen
- Konfigurations-Skript anwenden
- Konfigurations-Skript speichern
- Zertifikat oder Datei hochladen
- Zertifikat oder Datei herunterladen

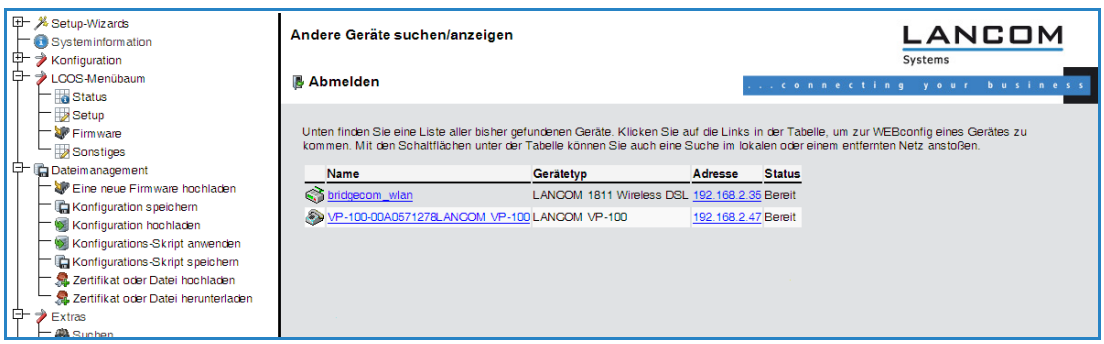


Extras

Im Menübereich "Extras" finden Sie einige Funktionen, welche die Konfiguration der Geräte erleichtern.

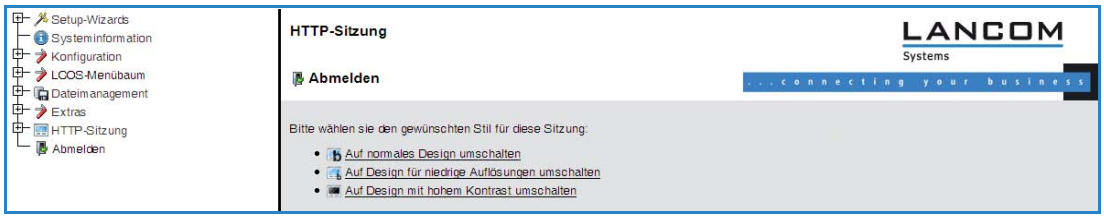
Mit der Suchfunktion können Sie z. B. in den Namen aller Konfigurationsparameter suchen. Falls Sie also zu einem bestimmten Konfigurationsparameter den Namen kennen, aber nicht wissen, über welches Menü dieser Eintrag zu erreichen ist, können Sie die gewünschte Stelle im LCOS-Menü auf diese Weise schnell auffinden.

Mit der Funktion zum Suchen und Anzeigen können Sie andere LANCOM-Geräte in Ihrem Netzwerk suchen und über einen entsprechenden Link direkt auf die Konfiguration der gefundenen Geräte wechseln.



HTTP-Sitzung

Im Menübereich "HTTP-Sitzung" können Sie die Darstellung der WEBconfig-Oberfläche zur besseren Anzeige auf Ihr Ausgabegerät anpassen, z. B. die Auflösung verringern oder den Kontrast verstärken.



B.2 Dateien von einem TFTP- oder HTTP-Server direkt in das Gerät laden

Neu in LCOS 7.60:

- Angabe von Server, Pfad und Datei in URL-Schreibweise
- Laden von Dateien in das Gerät von einem HTTP(S)-Server

Bestimmte Funktionen lassen sich über Telnet nicht oder nicht befriedigend ausführen. Dazu gehören alle Funktionen, bei denen komplette Dateien übertragen werden, etwa der Upload von Firmware oder die Speicherung und Wiederherstellung von Konfigurationsdaten. In diesen Fällen wird TFTP oder HTTP(S) eingesetzt.

B.2.1 TFTP

TFTP steht unter den Windows-Betriebssystemen standardmäßig zur Verfügung. Es ermöglicht den einfachen Dateitransfer von Dateien mit anderen Geräten über das Netzwerk.

Die Syntax des TFTP-Aufrufs ist abhängig vom Betriebssystem. Unter Windows lautet die Syntax:

```
tftp -i <IP-Adresse Host> [get|put] Quelle [Ziel]
```

Bei zahlreichen TFTP-Clients ist das ASCII-Format voreingestellt. Für die Übertragung binärer Daten (z. B. Firmware) muss daher meist die binäre Übertragung explizit gewählt werden. In diesem Beispiel für Windows erreichen Sie das durch den Parameter '-i'.

Sofern das Gerät mit einem Passwort geschützt ist, müssen Username und Passwort in den TFTP-Befehl eingebaut werden. Der Filename baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando (für Supervisoren) oder aus der Kombination von Username und Passwort (für lokale Administratoren), die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

- <Master-Passwort><Kommando> bzw.
- <Username>:<Passwort>@<Kommando>

Die Rechte zur Nutzung von TFTP können für die Administratoren eingeschränkt werden, siehe auch "Rechteverwaltung für verschiedene Administratoren".

B.2.2 Firmware, Geräte-Konfiguration oder Script über HTTP(S) laden

Durch die Unterstützung von HTTP und speziell HTTPS lässt sich der Download von Firmware, Geräte-Konfiguration oder Scripts auch für automatisierte Prozesse (z.B. Self-Provisioning) auf LANCOM-Geräten nutzen, welche die Dateien über das Internet beziehen. In der Praxis ist es zumeist sehr viel leichter, einen HTTPS-Server zentral mit eindeutiger Adresse (URI) im Internet bereit zu stellen als einen TFTP-Server - ggf. lässt sich ein bestehender Webserver um diese Funktionalität erweitern.

Ein optional für den HTTPS-Server verwendetes Zertifikat wird über WEBconfig als SSL-Root-CA-Zertifikat in das Gerät hochgeladen:

B.2.3 Firmware, Geräte-Konfiguration oder Script über HTTP(S) oder TFTP laden

Neben den Möglichkeiten, eine Firmware oder eine Konfigurationsdatei über LANconfig oder WEBconfig in ein Gerät einzuspielen, kann der Upload der entsprechenden Dateien über Telnet oder SSH auch direkt von einem HTTP(S)- oder TFTP-Server erfolgen. Dieses Vorgehen kann in größeren Installationen mit regelmäßigem Update von Firmware und/oder Konfiguration die Administration der Geräte erleichtern. Über HTTP(S) bzw. TFTP können auch Scripte – z.B. mit Teilkonfigurationen – in die Geräte geladen werden.

Dazu werden die Firmware- und Konfigurationsdateien oder Scripte auf einem HTTP(S)- bzw. TFTP-Server abgelegt. Ein TFTP-Server gleicht in der Funktionsweise einem FTP-Server, verwendet allerdings zur Datenübertragung ein anderes Protokoll. Bei der Verwendung eines HTTPS-Servers kann im Gerät ein Zertifikat hinterlegt werden, mit dem die Identität des Servers geprüft wird. Von diesem Server können die Dateien mit folgenden Befehlen abgerufen werden:

- `LoadConfig`
- `LoadFirmware`
- `LoadScript`

Der Server, das Verzeichnis und die Datei können auf zwei verschiedene Arten angegeben werden:

- Bei Nutzung des TFTP-Protokolls über die Parameter -s und -f :
  - `-s <Server-IP-Adresse oder Server-Name>`
  - `-f <Dateipfad und Dateiname>`
- Für die Nutzung von TFTP oder HTTP(S) kann der Befehl in der üblichen URL-Schreibweise angegeben werden (als Protokoll wird entweder TFTP oder HTTP(S) eingetragen):
  - `Befehl Protokoll://Server/Verzeichnis/Dateiname`

  Beim Zugriff auf einen kennwortgeschützten Bereich auf einem HTTP(S)-Server werden Benutzername und Kennwort entsprechend eingetragen:
  - `Befehl Protokoll://Benutzername:Kennwort@Server/Verzeichnis/Dateiname`

  Bei der Verwendung von HTTPS kann ein Zertifikat angegeben werden, mit dem die Identität des Servers geprüft wird:
  - `-c <Name des Zertifikats>`

Im Dateinamen inklusive Pfad sind folgende Variablen erlaubt:

- %m - LAN MAC Adresse (Hexadezimal, kleine Buchstaben, ohne Trennzeichen)
- %s - Seriennummer
- %n - Gerätename
- %l - Ort ('Standort' - aus der Konfiguration)
- %d - Gerätetyp

Beispiele:

Mit dem folgenden Befehl in einer Telnet-Sitzung wird eine Firmwaredatei mit dem Namen 'LC-1811-5.00.0019.upx' aus dem Verzeichnis 'LCOS/500' vom Server mit der IP-Adresse '192.168.2.200' in das Gerät geladen:

- `LoadFirmware -s 192.168.2.200 -f LCOS/500/LC-1811-5.00.0019.upx`

Mit dem folgenden Befehl in einer Telnet-Sitzung wird ein zur MAC-Adresse passendes Script vom Server mit der IP-Adresse '192.168.2.200' in das Gerät geladen:

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

Mit dem folgenden Befehl in einer Telnet-Sitzung wird eine Firmwaredatei mit dem Namen 'LC-1811-5.00.0019.upx' aus dem Verzeichnis 'download' vom HTTPS-Server mit der IP-Adresse 'www.myserver.com' in das Gerät geladen. dabei wird die Identität des Servers mit dem Zertifikat "sslroot.crt" geprüft:

■ `LoadFirmware -c sslroot.crt https://www.myserver.com/download/LC-1811-5.00.0019.upx`

Werden die Parameter `-s` und/oder `-f` nicht angegeben, verwendet das Gerät die Standardwerte, die unter dem Pfad `/setup/config/TFTP-Client` gesetzt werden:

- `Config-Adresse`
- `Config-Dateiname`
- `Firmware-Adresse`
- `Firmware-Dateiname`

Die Nutzung dieser Standardwerte bietet sich an, wenn die aktuellen Konfigurationen und Firmware-Versionen immer unter dem gleichen Namen an der gleichen Stelle gespeichert werden. In diesem Fall können mit den einfachen Befehlen `LoadConfig` und `LoadFirmware` die jeweils gültige Dateien geladen werden.

B.3 Rechteverwaltung für verschiedene Administratoren

Neu in LCOS 7.60:

- Administratoren ohne Trace-Rechte

In der Konfiguration des LANCOM können mehrere Administratoren angelegt werden, die über unterschiedliche Zugriffsrechte verfügen. Für ein LANCOM können bis zu 16 verschiedene Administratoren eingerichtet werden.

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 oder umbenannt werden. Um sich als root-Administrator anzumelden, geben Sie im Login-Fenster den Benutzernamen „root" ein oder Sie lassen dieses Feld frei.

Sobald in der Konfiguration des Gerätes ein Passwort für den „root"-Administrator gesetzt ist, erscheint beim Aufruf von WEBconfig auf der Startseite die Schaltfläche **Login**, mit dem das Fenster zur Anmeldung eingeblendet wird. Nach der Eingabe des korrekten Benutzernamens und Passworts erscheint das Hauptmenü der WEBconfig. In diesem Menü sind nur die Punkte vorhanden, für die der Administrator Zugriffs- bzw. Funktionsberechtigungen hat.

Ist mindestens ein weiterer Administrator in der Admin-Tabelle eingerichtet, so enthält das Hauptmenü zusätzlich eine Schaltfläche **Administrator wechseln**, die es erlaubt zu einer anderen Benutzerkennung (mit ggf. anderen Rechten) zu wechseln.

B.3.1 Die Rechte für die Administratoren

Bei den Rechten für die Administratoren werden zwei Bereiche unterschieden:

- Jeder Administrator gehört zu einer bestimmten Gruppe, der global definierte Rechte zugewiesen sind.
- Jeder Administrator verfügt außerdem über „Funktionsrechte", die den persönlichen Zugriff auf bestimmte Funktionen wie z.B. die Setup-Assistenten regeln.

Administratorengruppen

Bezeichnung unter Telnet/Terminal	Bezeichnung unter LANconfig	Rechte
Supervisor	Alle	Supervisor - Mitglied in allen Gruppen
Admin-RW	Eingeschränkt	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RW-Limit	Eingeschränkt ohne Trace-Rechte	lokaler Administrator mit Lese- und Schreibzugriff ohne Trace-Rechte
Admin-RO	Nur lesen	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
Admin-RO-Limit	Nur lesen ohne Trace-Rechte	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff und ohne Trace-Rechte
kein	keine	kein Zugriff auf die Konfiguration

- Supervisor: Hat vollen Zugriff auf die Konfiguration
- lokaler Administrator mit Lese- und Schreibrechten: Ebenfalls voller Zugriff auf die Konfiguration, dabei sind jedoch die folgenden Möglichkeiten gesperrt:
  - Firmware in das Gerät hochladen
  - Konfiguration in das Gerät einspielen
  - Konfiguration über LANconfig

Lokale Administratoren mit Schreibrechten 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.

- lokaler Administrator mit Lese- und Schreibrechten ohne Trace-Rechte: Ebenfalls voller Zugriff auf die Konfiguration, dabei sind jedoch die folgenden Möglichkeiten gesperrt:
  - Firmware in das Gerät hochladen
  - Konfiguration in das Gerät einspielen
  - Konfiguration über LANconfig
  - Trace-Ausgaben über Telnet oder LANmonitor

Lokale Administratoren mit Schreibrechten, aber ohne Trace-Rechte können keine Admistratoren mit Trace-Rechten anlegen.

- lokaler Administrator mit Leserechten: Kann die Konfiguration über Telnet oder Terminalprogramm lesen, aber keine Werte verändern. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.
- keine: Kann die Konfiguration nicht lesen. Diesen Administratoren können über die Funktionsrechte bestimmte Möglichkeiten zur Konfiguration eingeräumt werden.

Funktionsrechte

Mit den Funktionsrechten werden dem Benutzer die folgenden Möglichkeiten eingeräumt:

- Grundkonfigurations-Assistent
- Sicherheits-Assistent
- Internet-Assistent
- Assistent zur Auswahl von Internet-Providern
- RAS-Assistent
- LAN-LAN-Kopplungs-Assistent
- Uhrzeit und Datum verändern
- Nach weiteren Geräten suchen
- WLAN-Linktest
- a/b-Assistent

B.3.2 Administratorenzugänge über TFTP und SNMP

Die zusätzlichen Administratorenzugänge werden in der Regel für die Konfiguration der Geräte über Telnet, Terminalprogramme oder SSH-Zugänge genutzt. Allerdings können die zusätzlichen Administratoren auch über TFTP oder SNMP auf die Geräte zugreifen.

Zugang über LANconfig

Ein Benutzer mit Supervisorrechten kann sich bei LANconfig anmelden, wenn er im Loginfenster im Feld für das Passwort seine Benutzerdaten in der Kombination <Username>:<Passwort> eingibt.

Zugang über TFTP

Im TFTP wird der Username und das Passwort im Quell- (TFTP-Read-Request) oder Ziel-Filenamen (TFTP-Write-Request) kodiert. Der Filename baut sich entweder aus dem Master-Passwort und dem auszuführenden Kommando oder aus der Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, und nachgestelltem Kommando zusammen. Ein über TFTP abgesetztes Kommando sieht daher wie folgt aus:

- <Master-Passwort><Kommando> bzw.
- <Username>:<Passwort>@<Kommando>

Beispiele (das LANCOM hat die Adresse mylancom.intern, das Master-Passwort lautet 'RootPwd' und es ist der User 'LocalAdmin' mit dem Passwort 'Admin' eingerichtet):

- Konfiguration aus dem Gerät auslesen (nur für den Supervisor)

  ```
  tftp mylancom.intern GET RootPwdreadconfig mylancom.lcf
  ```

- Konfiguration in das Gerät schreiben (nur für den Supervisor)

  ```
  tftp mylancom.intern PUT mylancom.lcf RootPwdwriteconfig
  ```

- Geräte-MIB aus dem Gerät auslesen (für lokalen Administrator)

  ```
  tftp mylancom.intern GET localadmin:Admin@readmib mylancom.mib
  ```

Für die Menüs und ausführbaren Befehle gelten die gleichen Rechte-Beschränkungen wie unter Telnet.

Zugang über SNMP-Management-Systeme

Auch bei der Verwaltung von Netzwerken mit Hilfe von SNMP-Tools wie HP OpenView können über die verschiedenen Administratoren-Zugänge die Rechte gezielt gesteuert werden.

Unter SNMP werden Username und Passwort in der „Community" kodiert. Dort kann entweder die Community 'public' ausgewählt werden oder entweder das Master-Passwort oder eine Kombination von Username und Passwort, die durch einen Doppelpunkt getrennt sind, angegeben werden.

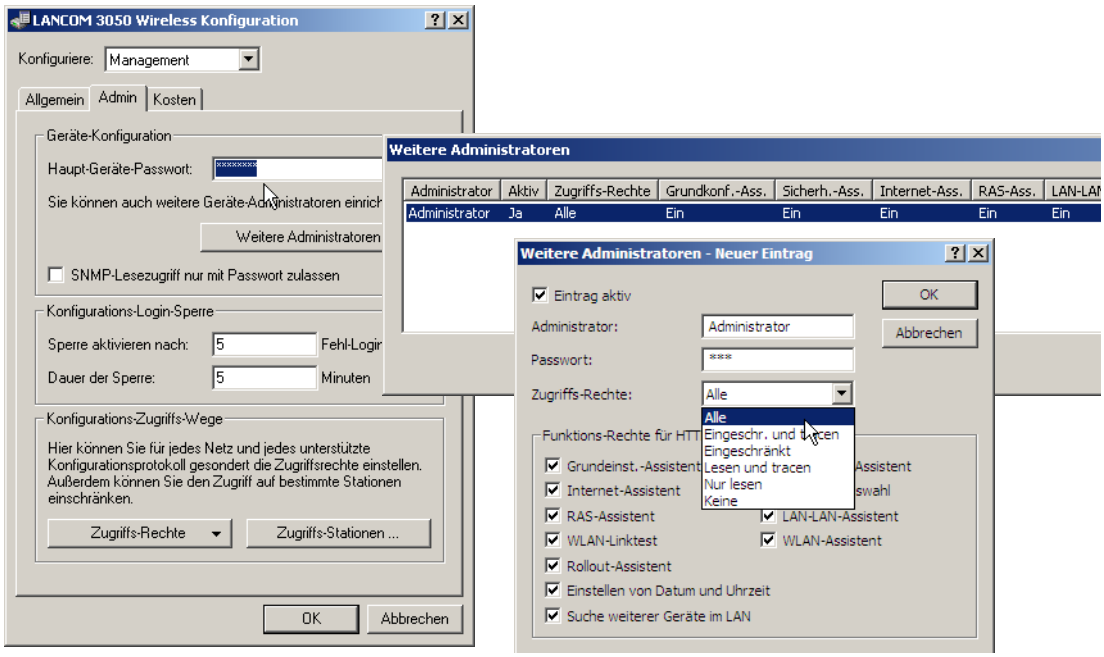
Die Community 'public' entspricht von den Rechten her einem lokalen Administrator mit Read-Only-Rechten, solange der SNMP-Lesezugriff ohne Passwort erlaubt wird. Wird dieser Zugriff verboten, so darf die Community 'public' auf keinen Menüpunkt zugreifen.

Ansonsten gelten für die Menüs die gleichen Rechte-Beschränkungen wie unter Telnet.

B.3.3 Konfiguration der Benutzerrechte

LANconfig

Bei der Konfiguration mit LANconfig finden Sie die Liste der Administratoren im Konfigurationsbereich 'Management' auf der Registerkarte 'Admin' unter der Schaltfläche **Weitere Administratoren**.



Geben Sie hier folgende Werte ein:

- Name für den neuen Administrator mit Passwort.
- Zugriffsrechte
- Funktionsrechte

Sie können die Einträge über den Schalter 'Eintrag aktiv' vorübergehend deaktivieren, ohne sie ganz zu löschen.

WEBconfig, Telnet oder Terminalprogramm

Unter WEBconfig oder Telnet bzw. Terminalprogramm finden Sie die Admin-Tabelle auf folgenden Pfaden:

Konfigurationstool	Menü/Tabelle
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Config-Modul ▶ Admin.-Tabelle
Terminal/Telnet	`Setup/Config-Modul/Admin.-Tabelle`

Zur Darstellung der Benutzergruppen stehen die folgenden Werte zur Verfügung:

Bezeichnung	Rechte
Supervisor	Supervisor - Mitglied in allen Gruppen
Admin-RW	lokaler Administrator mit Lese- und Schreibzugriff
Admin-RW-Limit	lokaler Administrator mit Lese- und Schreibzugriff, ohne Trace-Rechte
Admin-RO	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff
Admin-RO-Limit	lokaler Administrator mit Lesezugriff aber ohne Schreibzugriff, ohne Trace-Rechte
kein	kein Zugriff auf die Konfiguration

Zur Darstellung der Funktionsrechte stehen die folgenden Hexadezimalwerte zur Verfügung:

Wert	Rechte
0x00000001	Der Benutzer darf den Grundkonfigurations-Assistenten ausführen
0x00000002	Der Benutzer darf den Sicherheits-Assistenten ausführen
0x00000004	Der Benutzer darf den Internet-Assistenten ausführen
0x00000008	Der Benutzer darf den Assistenten zur Auswahl von Internet-Providern ausführen
0x00000010	Der Benutzer darf den RAS-Assistenten ausführen
0x00000020	Der Benutzer darf den LAN-LAN-Kopplungs-Assistenten ausführen
0x00000040	Der Benutzer darf die Uhrzeit und das Datum stellen (gilt auch für Telnet und TFTP)
0x00000080	Der Benutzer darf nach weiteren Geräten suchen
0x00000100	Der Benutzer darf den WLAN-Linktest ausführen (gilt auch für Telnet)
0x00000200	Der Benutzer darf den a/b-Assistenten ausführen
0x00000400	Der Benutzer darf den WTP-Zuordnungs-Assistenten ausführen
0x00000800	Der Benutzer darf den Public-Spot-Assistenten ausführen
0x00001000	Der Benutzer darf den WLAN-Assistenten ausführen
0x00002000	Der Benutzer darf den Rollout-Assistenten ausführen
0x00004000	Der Benutzer darf den Dynamic-DNS-Assistenten ausführen
0x00008000	Der Benutzer darf den VoIP-CallManager-Assistenten ausführen
0x00010000	Der Benutzer darf den WLC-Profil-Assistenten ausführen

Der Eintrag ergibt sich aus der jeweiligen Summe in den ersten, zweiten und dritten Spalten von rechts. Soll der Benutzer z.B. die Funktionen „Sicherheits-Assistent", „Auswahl der Internet-Provider", „RAS-Assistent", „Uhrzeit ändern" und „WLAN-Linktest" ausführen können, ergeben sich folgende Werte:

- erste Spalte von rechts: 2 (Sicherheits-Assistent) + 8 (Auswahl der Internet-Provider) = „a" (Hexadezimal)
- zweite Spalte von rechts: 1 (RAS-Assistent) + 4 (Uhrzeit ändern) = „5" (Hexadezimal)
- dritte Spalte von rechts: 1 (WLAN-Linktest) = „1" (Hexadezimal)

Für dieses Beispiel tragen Sie in die Funktionsrechte also den Wert „0000015a" ein.

Anders ausgedrückt handelt es sich hierbei um eine ODER-Verknüpfung der Hexadezimal-Werte:

Bezeichnung	Wert
Sicherheits-Assistent	0x00000002
Auswahl des Providers	0x00000008
RAS-Assistent	0x00000010
Uhrzeit ändern	0x00000040
WLAN-Linktest	0x00000100
ODER-verknüpft	0x0000015a

Beispiele:

Mit dem folgenden Befehl legen Sie einen neuen Benutzer in der Tabelle an, der als lokaler Administrator „Mueller" mit dem Passwort „BW46zG29" den Internetprovider auswählen darf. Der Benutzer wird dabei sofort aktiviert:

```
set Mueller BW46zG29 ja Admin-RW 00000008
```

Mit dem folgenden Befehl erweitern Sie die Funktionsrechte dahingehend, das Benutzer „Mueller" auch den WLAN-Link-Test ausführen kann (die Sternchen stehen für die nicht zu verändernden Werte):

```
set Mueller * * * 00000108
```

B.3.4 Einschränkungen der Konfigurationsbefehle

Die Verfügbarkeit der Befehle bei der Konfiguration der Geräte über Telnet oder Terminalprogramm hängt von den Rechten der Benutzer ab:

Befehl	Supervisor	lokaler Administrator	Bemerkung
activateimage	✔		
cfgreset	✔		
linktest	✔		Der Befehl 'linktest' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, einen WLAN-Linktest durchzuführen
readconfig	✔		
writeconfig	✔		
writeflash	✔		
setenv	✔	✔	
testmail	✔	✔	
time	✔	✔	Der Befehl 'time' kann auch ausgeführt werden, wenn der Benutzer das Funktionsrecht besitzt, die Systemzeit einzustellen
unsetenv	✔	✔	
delete/rm	✔	✔	
readmib	✔	✔	
WLA	✔	✔	
set	✔	✔	

Alle weiteren Befehle (wie 'cd', 'ls', 'trace', etc...) dürfen von allen Benutzern verwendet werden. Um Befehle ausführen zu können, die eine Konfigurationsänderung bewirken (z.B. 'do' oder 'time'), muss der jeweilige Benutzer mindestens Schreibrechte besitzen.

Die oben aufgeführten Befehle sind nicht in allen LCOS-Versionen und nicht für alle LANCOM-Modelle verfügbar.

B.3.5 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 LAN einzuräumen. Sollten z.B. bei der Konfiguration von Netzwerkgeräten wie einem LANCOM VP-100 Fragen auftauchen, kann der jeweilige Support besser weiterhelfen, wenn er direkt auf das Gerät im LAN des Kunden zugreifen kann. Die Standardmethode für den Zugriff auf Geräte im LAN über inverses Masquerading (Port-Forwarding) erfordert jedoch in manchen Fällen eine entsprechende Konfiguration der Firewall – außerdem werden die einmal geöffneten Zugänge oft nicht wieder gelöscht und stellen damit ein Sicherheitsrisiko dar.

Als Alternative zu den dauerhaften Zugängen über festes Port-Forwarding können vorübergehende Fernwartungszugänge eingerichtet werden, die nach einer bestimmten inaktiven Zeit automatisch wieder geschlossen werden. Dazu erzeugt z.B. der Support-Mitarbeiter, der auf ein Gerät im Netzwerk des Kunden zugreifen soll, einen „TCP/HTTP-Tunnel", über den er über TCP Port 80 Zugang zu dem entsprechenden Gerät erhält.

Dieser Zugang ist nur gültig für die IP-Adresse, von welcher der Tunnel erzeugt wurde. Der Zugriff auf das freizugebende Gerät im Netzwerk ist also nicht übertragbar!

TCP/HTTP-Tunnel konfigurieren

Zur Konfiguration der TCP/HTTP-Tunnel im LANCOM stehen folgende Parameter bereit:

Konfigurationstool	Aufruf
WEBconfig, Telnet	Experten-Konfiguration > Setup > HTTP

- **Max.-Tunnel-Verbindungen**

  Maximale Anzahl der gleichzeitig aktiven TCP/HTTP-Tunnel.

  - Mögliche Werte: Maximal 255 Tunnel.
  - Default: 3 Tunnel.

- **Tunnel-Idle-Timeout**

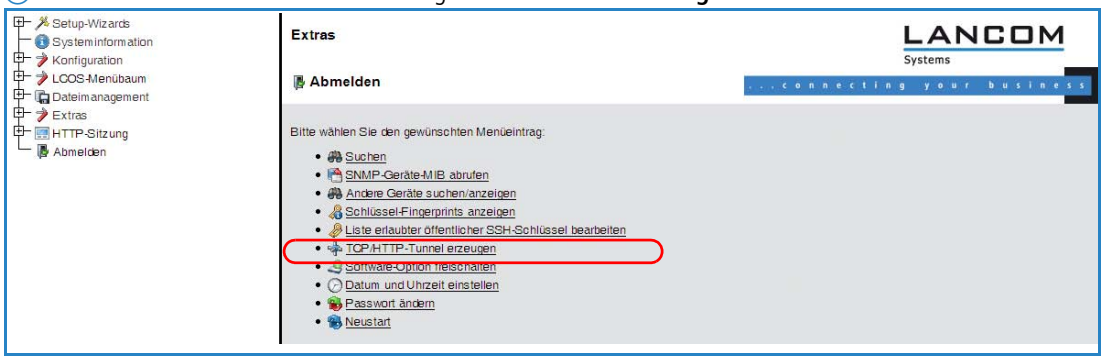
  Lebensdauer eines Tunnels ohne Aktivität. Nach Ablauf dieser Zeit wird der Tunnel automatisch geschlossen, wenn darüber keine Daten übertragen werden.

  - Mögliche Werte: Maximal 4294967295 Sekunden.
  - Default: 300 Sekunden.

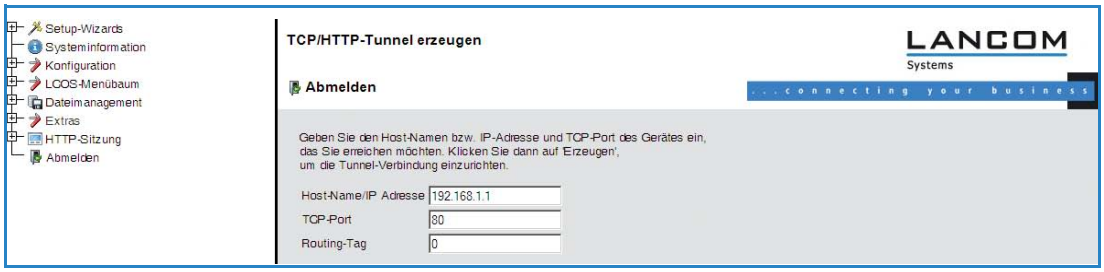
TCP/HTTP-Tunnel erzeugen

① Die HTTP-Tunnel werden auf der Startseite von WEBconfig eingerichtet. Melden Sie sich in WEBconfig auf dem LANCOM Router an, hinter dem das freizugebende Gerät erreicht werden kann. Holen Sie dazu ggf. beim zuständigen Administrator die benötigten Login-Daten ein.

② Wählen Sie im Bereich 'Extras' den Eintrag **TCP/HTTP-Tunnel erzeugen**.



③ Geben Sie den Namen bzw. die IP-Adresse des Gerätes ein, das Sie vorübergehend für den Zugriff über HTTP freischalten möchten.



④ Wählen Sie dazu einen Port aus, der für den HTTP-Tunnel verwendet werden soll und geben sie ggf. das Routing-Tag des IP-Netzwerks an, in dem sich das freizugebende Gerät befindet und bestätigen Sie die Angaben mit **Erzeugen**.

⑤ Der folgende Dialog zeigt eine Bestätigung über den neu erstellten Tunnel und bietet einen Link auf das freizugebende Gerät.

Anstelle von HTTP- oder HTTPS-Fernwartungszugängen sind Fernwartungstunnel mit beliebigen andere TCP-Diensten möglich, beispielsweise TELNET-Verbindungen (TCP-Port 23) oder SSH (TCP-Port 22).

Tunnel vorzeitig löschen

Der neu erstellte HTTP-Tunnel wird automatisch nach Ablauf der Tunnel-Idle-Timeout-Zeit ohne Aktivität gelöscht. Um den Tunnel vorzeitig zu löschen, können Sie über **LCOS-Menübaum ▶ Status ▶ TCP-IP ▶ HTTP** die Liste der aktiven Tunnel aufrufen und die nicht mehr benötigten Tunnel gezielt löschen.

Aktive TCP-Verbindungen in diesem Tunnel werden mit dem Löschen des Tunnels **nicht** beendet, es können aber keine neuen Verbindungen mehr aufgebaut werden.

B.4 Neue Firmware mit LANCOM FirmSafe

Neu in LCOS 7.60:

- Asymmetrisches Firmsafe

B.4.1 Asymmetrisches Firmsafe

Durch den großen Funktionsumfang in der Firmware ist es nicht bei allen Geräten möglich, zwei vollwertige Firmwareversionen gleichzeitig zu speichern. Bei diesen Geräten wird das asymmetrische Firmsafe verwendet. Dabei enthält das Gerät immer eine vollständige Firmware sowie eine 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, um eine funktionsfähige Firmware in das Gerät zu laden. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, 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 wird zunächst eine Konverter-Firmware in das Gerät geladen. 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 bleibt 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.

B.5 Projektmanagement mit LANconfig

Neu in LCOS 7.60:

- Übertragen von Gerätekonfigurationen auf ähnliche Modelle
- Automatisches Anlegen von Konfigurations-Backups vor Firmware-Upload, Konfigurationsänderung und Skriptausführung.
- Anpassen der Symbolleiste

B.5.1 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.

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 LCOS-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** ▶ **Konfigurationsverwaltung** ▶ **Als Datei sichern**.

③ Trennen Sie das Ausgangsgerät vom Netzwerk, um Adresskonflikte zu vermeiden.

④ Spielen Sie die Konfiguration über **Gerät** ▶ **Konfigurationsverwaltung** ▶ **Aus Datei wiederherstellen** in das Zielgerät ein. Die Meldungen über die Konvertierung der Konfiguration werden in einem Info-Dialog angezeigt.

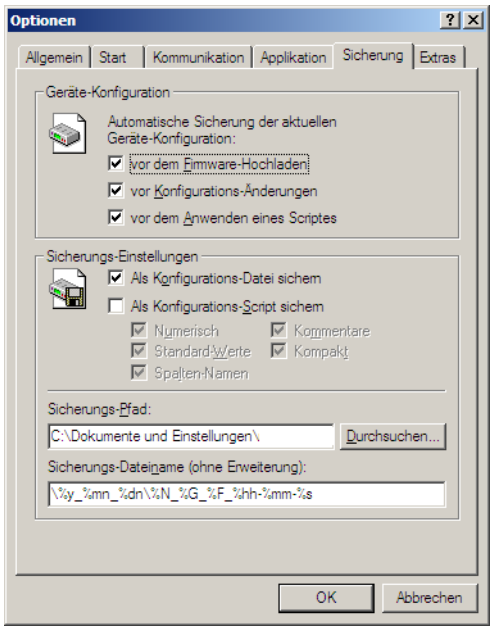
Bitte beachten Sie, dass diese Funktion in erster Linie für den Ersatz von Geräten gedacht ist und nicht für die Konfiguration von neuen Geräten, die parallel im gleichen Netz wie das Ausgangsgerät betrieben werden sollen. Da auch die zentralen Kommunikationseinstellungen wie z. B. die IP-Adresse des 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.

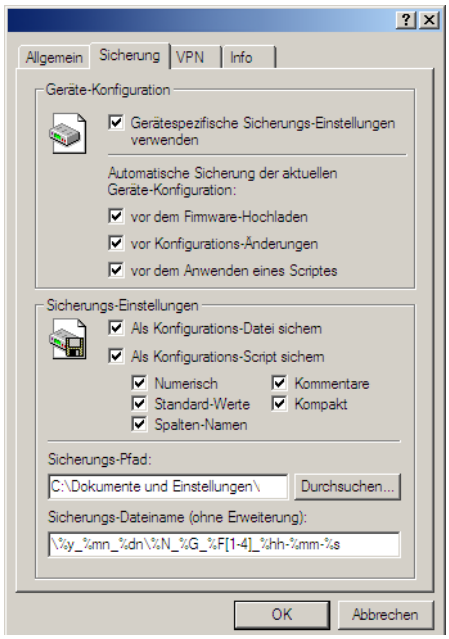
B.5.2 Automatische Sicherung der Konfiguration mit LANconfig

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** ▶ **Sicherung**. Für die einzelnen Geräte können ergänzend spezielle Sicherungseinstellungen definiert werden. Klicken Sie dazu das entsprechende Gerät mit der rechten Maustaste und wählen Sie im Kontextmenü den Eintrag **Eigenschaft** ▶ **Sicherung**.

Wählen Sie hier folgende Optionen aus:

- Werden für dieses Gerät die globalen oder die gerätespezifischen Sicherungseinstellungen verwendet (nur im gerätespezifischen Dialog)?
- Vor welchem Ereignis die Konfiguration gespeichert werden soll (Firmware-Upload, Konfigurationsänderung und Skriptausführung).
- In welchem Format die Konfiguration gespeichert werden soll (Konfigurationsdatei, Skript ggf. mit Optionen).
- In welchem Verzeichnis die Konfiguration gespeichert werden soll.
- Wie der Dateiname der Sicherungs-Datei aufgebaut werden soll. Dabei können Platzhalter für die Geräteinformationen (IP-Adresse, Hardware-Typ etc.) und Zeitinformationen verwendet werden. Weitere Informationen zu den Platzhaltern finden Sie in der Online-Hilfe.

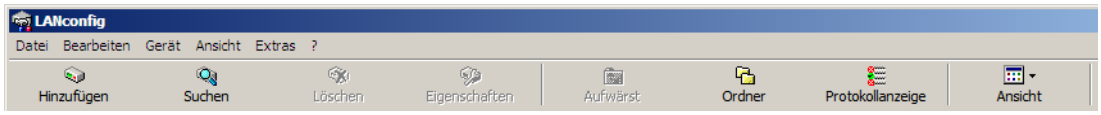




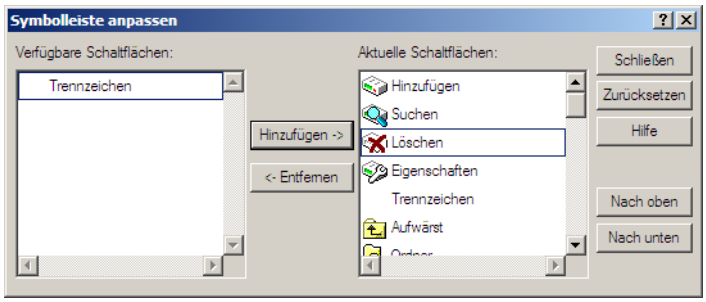
B.5.3 Anpassen der Symbolleiste

Zur benutzerdefinierten Anpassung der Symbolleiste können im LANconfig unter **Ansicht ▶ Symbolleiste** die folgenden Optionen gewählt werden:

- Schaltflächen: Blendet die Schaltflächen ein oder aus.
- Große Symbole: Zeigt eine größere Darstellung der Symbole.
- Text anzeigen: Zeigt unter den Symbolen jeweils einen Text zur Bezeichnung der Aktion.



- 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.

B.6 LANCOM Layer 2 Management Protokoll (LL2M)

Neu mit LCOS 7.6:

- LANCOM Layer 2 Management Protokoll (LL2M)

B.6.1 Einleitung

Alle Wege zur Konfiguration eines LANCOM setzen eine IP-Verbindung zwischen dem Konfigurationsrechner und dem LANCOM 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 Atacken 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 LCOS integriert und wird über die Kommandozeile ausgeführt. Der LL2M-Server ist ebenfalls im LCOS 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.

B.6.2 Konfiguration des LL2M-Servers

WEBconfig: LCOS-Menübaum/Setup/Config/LL2M

■ **In-Betrieb**

Schaltet den LL2M-Server ein oder aus. Ein aktivierter LL2M-Server kann nach dem Booten/Einschalten des Gerätes für die Dauer des Zeit-Limits von einem LL2M-Client angesprochen werden.

Mögliche Werte:

□ Ja, nein

Default:

□ Ja

■ **Zeit-Limit**

Definiert die Zeitspanne in Sekunden, in der ein aktivierter LL2M-Server nach dem Booten/Einschalten des Gerätes von einem LL2M-Client angesprochen werden kann. Nach Ablauf des Zeit-Limits wird der LL2M-Server automatisch deaktiviert.

Mögliche Werte:

□ 0 bis 4294967295

Default:

□ 0

Besondere Werte:

□ 0 deaktiviert das Zeit-Limit, in diesem Zustand bleibt der LL2MServer dauerhaft aktiv.

B.6.3 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 Telnet-Sitzung auf einem LANCOM, 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.

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 Befehl LL2Mdetect kann mit den folgenden Parametern eingeschränkt werden.

□ -a <MAC-Adresse>: Schränkt den Befehl nur auf die Geräte mit der angegebenen MAC-Adresse ein. Die MAC-Adresse wird in der Form "00a057010203", "00-a0-57-01-02-03" oder "00:a0:57:01:02:03" angegeben.

Wird keine MAC-Einschränkung gesetzt, geht der detect als Multicast (oder optional 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 LANCOM-MAC-Adressen.

□ -t <Geräte-Typ>: Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Typs ein.

- □ -r <Hardware-Release>: Schränkt den Befehl nur auf die Geräte des entsprechenden Hardware-Releases ein.
- □ -f <Version>: Schränkt den Befehl nur auf die Geräte der entsprechenden Firmware-Version ein.
- □ -s <Seriennummer>: Schränkt den Befehl nur auf die Geräte der entsprechenden Seriennummer ein.
- □ -b : Versendet die LL2Mdetect-Anfrage als Broadcast und nicht als Multicast.
- □ -v <VLAN-ID>: Versendet die LL2Mdetect-Anfrage nur auf dem angegebenen VLAN. Wenn keine VLAN-ID angegeben ist, wird die VLAN-ID der ersten definierten IP-Netzwerks verwendet.

Beispiel:

- □ ll2mdetect -r A: Dieser Befehl versendet eine SYSINFO-Anfrage an alle Geräte mit der Hardware-Release “A”.

Die Antwort des LL2MServers enthält 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 können durch Semikolon getrennt in einem LL2M-Befehl kombiniert werden. Je nach Kommando werden Aktionen auf dem entfernten Gerät ausgeführt und die Rückmeldungen des entfernten Gerätes werden zur Anzeige an den LL2M-Client übertragen. Der Befehl LL2Mexec entspricht folgender Syntax:

- □ ll2mexec <User>[:<Password>]@<MAC-Adresse>

Der Befehl LL2Mexec kann mit dem folgenden Parameter eingeschränkt werden.

- □ -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.

Beispiel:

- □ ll2mexec root@00a057010203 set name MyLANCOM: Dieser Befehl meldet den LL2M-Client als “root” auf dem LL2M-Server mit der MAC-Adresse “00a057010203” an. Das Kennwort wird in der Konsolensitzung interaktiv abgefragt. Dann setzt der LL2M-Client den Namen des entfernten Gerätes auf den Wert “MyLANCOM”.

C Diagnose

C.1 Tracen mit dem LANmonitor

Neu in LCOS 7.60:

- Speichern von Support-Dateien mit Trace-Daten, Geräte-Konfiguration, Bootlog und Sysinfo
- Automatische Sicherung der Trace-Daten
- Trace-Konfiguration mit Assistenten
- Ausgabe von Show-Kommandos
- Ausgabe von Status-Informationen und Statistiken
- SSL-verschlüsselte Telnet-Verbindung

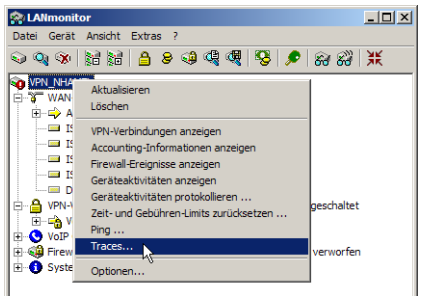
Die Abfrage von Traces kann sehr komfortabel über den LANmonitor vorgenommen werden. Klicken Sie dazu mit der rechten Maustaste auf den Geräteeintrag und wählen Sie im Kontextmenü den Eintrag **Traces**.

Zur Abfrage von Traces über den LANmonitor muss ein Telnet-Zugriff auf das Gerät erlaubt sein. Beim Starten des Trace-Dialogs versucht der LANmonitor zunächst eine SSL-verschlüsselte Telnet-Verbindung zum Gerät aufzubauen. Falls das Gerät keine SSL-Verbindungen unterstützt, wechselt der LANmonitor automatisch auf unverschlüsseltes Telnet.
Wenn der SNMP-Zugriff auf das Gerät passwortgeschützt ist, sind zudem die Zugangsdaten für einen Administrator mit Trace-Rechten erforderlich.

Einleitung

Mit der Trace-Funktion im LANmonitor können über die normalen Trace-Funktionen hinaus, wie sie von der Telnet-Oberfläche bekannt sind, weitere Funktionen genutzt werden, die eine Erstellung und Auswertung der Traces erleichtern. So kann z. B. die aktuelle Trace-Konfiguration, mit der die benötigten Trace-Befehle aktiviert werden, in einer Konfigurationsdatei gespeichert werden. Eine solche Trace-Konfiguration kann ein erfahrener Service-Techniker vorbereiten und einem weniger erfahrenen Anwender zur Verfügung stellen, der damit die gewünschte Trace-Ausgabe eines Gerätes erzeugen kann. Auch die Trace-Ergebnisse können komfortabel in einer Datei gespeichert werden und an den Techniker zur Auswertung zurückgegeben werden.

Um das Trace-Fenster für ein Gerät zu öffnen, klicken Sie im LANmonitor mit der rechten Maustaste auf den Eintrag des Gerätes und wählen im Kontext-Menü den Eintrag “Traces”.



Der LANmonitor bietet die folgenden Schaltflächen zur Bedienung des Trace-Moduls:

Öffnet eine vordefinierte Konfiguration für die Trace-Ausgabe. Damit können Sie eine Trace-Ausgabe genau so erstellen, wie Sie z. B. von einem Service-Techniker benötigt wird.

Speichert die aktuelle Trace-Konfiguration, um diese an einen Anwender weiterzugeben.

Öffnet eine Datei mit Trace-Ergebnissen zur Ansicht im Trace-Modul.

Speichert die aktuellen Trace-Ergebnisse in einer Datei.

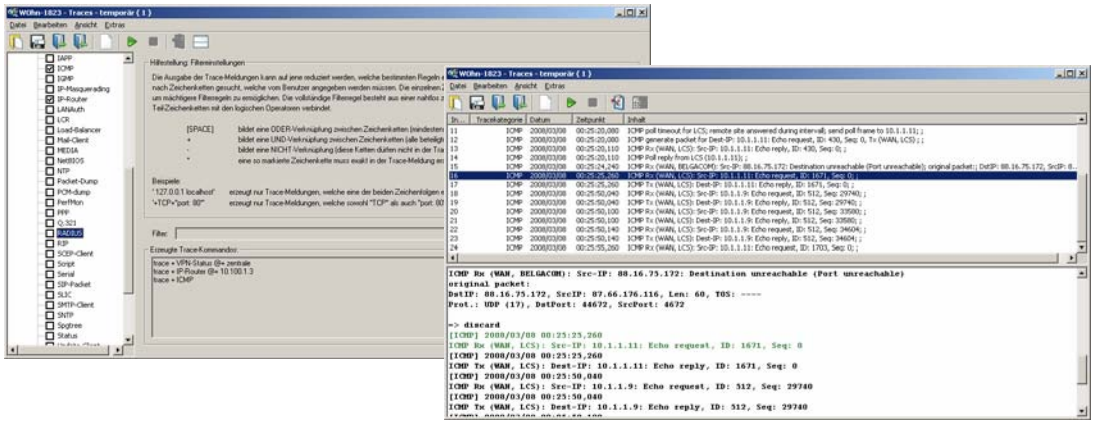
Löscht die aktuelle Anzeige der Trace-Ergebnisse.

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.

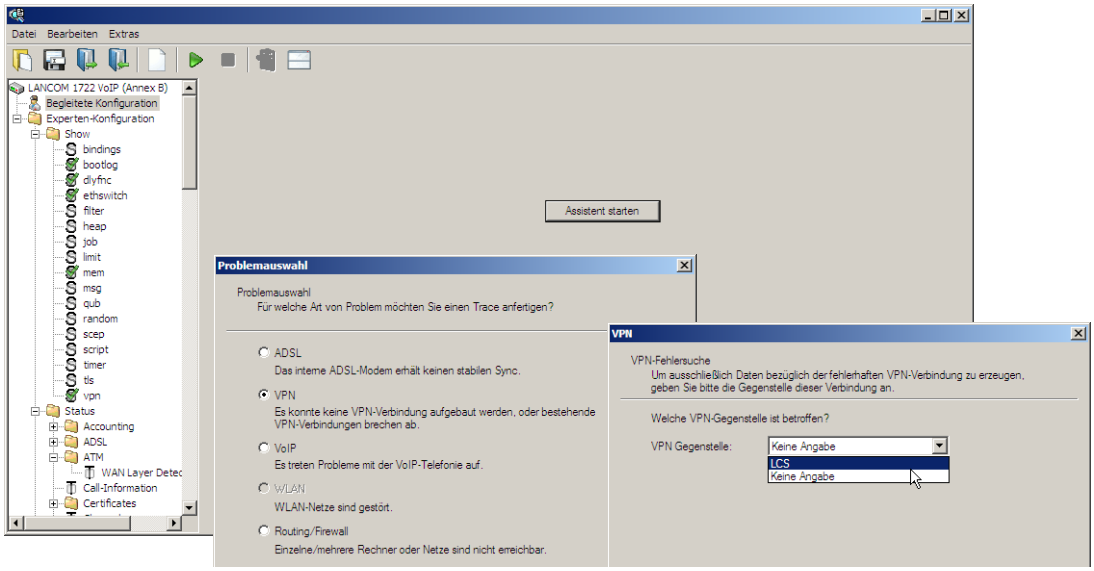
Wechselt in den Modus zur Anzeige der Trace-Ausgabe.



Konfiguration der Trace-Ausgaben mit dem Trace-Assistenten

Besonders einfach können die Trace-Einstellungen mit dem Assistenten vorgenommen werden. Wählen Sie dazu im linken Bereich des Trace-Dialogs die **Begleitende Konfiguration** und klicken Sie im Hauptfenster **Assistent starten**. In den folgenden Dialogen können Sie die Aufgabenstellung für den Trace auswählen (z. B. VPN) und den Trace ggf. weiter einschränken (z B. auf eine bestimmte VPN-Gegenstelle). Beim Abschluss des Assistenten wählen Sie aus, ob der Assistent die bestehende Trace-Konfiguration ersetzen oder ergänzen soll.

Beim Ersetzen der Trace-Konfiguration werden alle bisherigen Trace-Einstellungen gelöscht (mit Ausnahme des Bootlog-Traces, der automatisch enthalten ist). Speichern Sie daher ggf. vor Ausführung des Assistenten die bisherige Tracekonfiguration für eine spätere Verwendung.



Experten-Konfiguration der Trace-Ausgaben

Über die Einstellungen des Assistenten hinaus können, mit Hilfe der Experten-Konfiguration, die Traces und weitere Anzeigen genauer eingestellt werden. Die Experten-Konfiguration unterteilt sich in drei Bereiche:

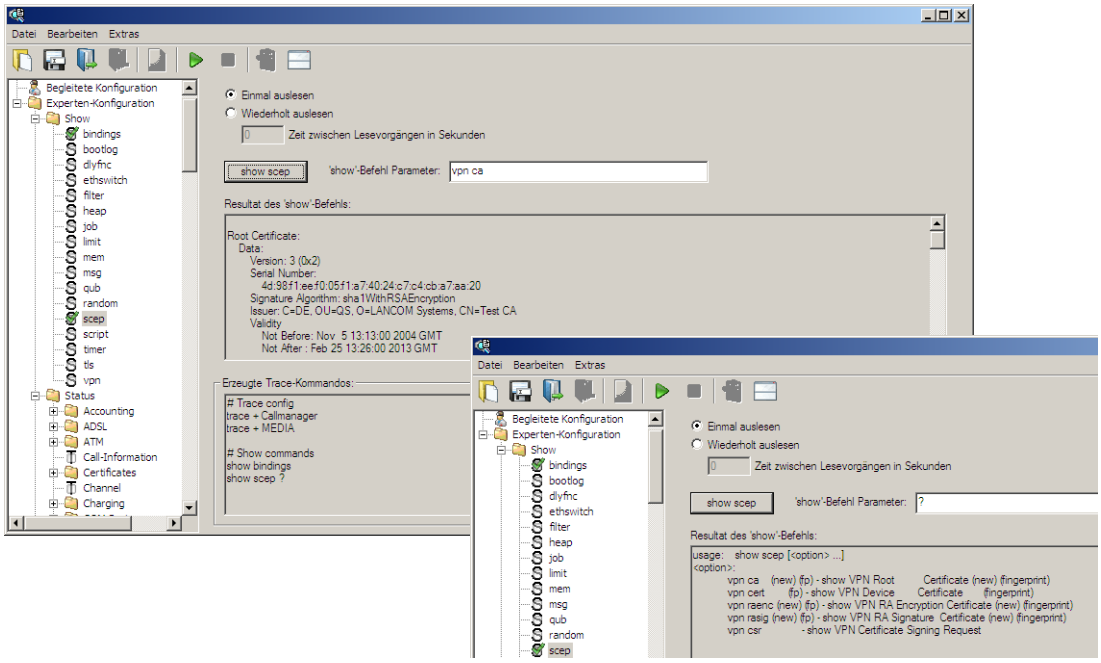
- Show

  Für jeden Gerätetyp können bestimmte Informationen mit einem Show-Kommando aufgerufen werden – 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 und dann den Show-Button, um die aktuelle Ausgabe des Show-Kommandos aufzurufen. Je nach gewähltem Eintrag können bzw. müssen noch ergänzende Parameter angegeben werden. Eine Information über diese Parameter erhalten Sie, wenn Sie in das Eingabefeld ein Fragezeichen eingeben und den Show-Button klicken.

Um die Ausgabe des Show-Kommandos in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem aktivierten Show-Kommando kann separat eingestellt werden, ob es nur einmal beim Start des Traces ausgeführt wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

Die Einstellungen der Show-Kommandos werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert.



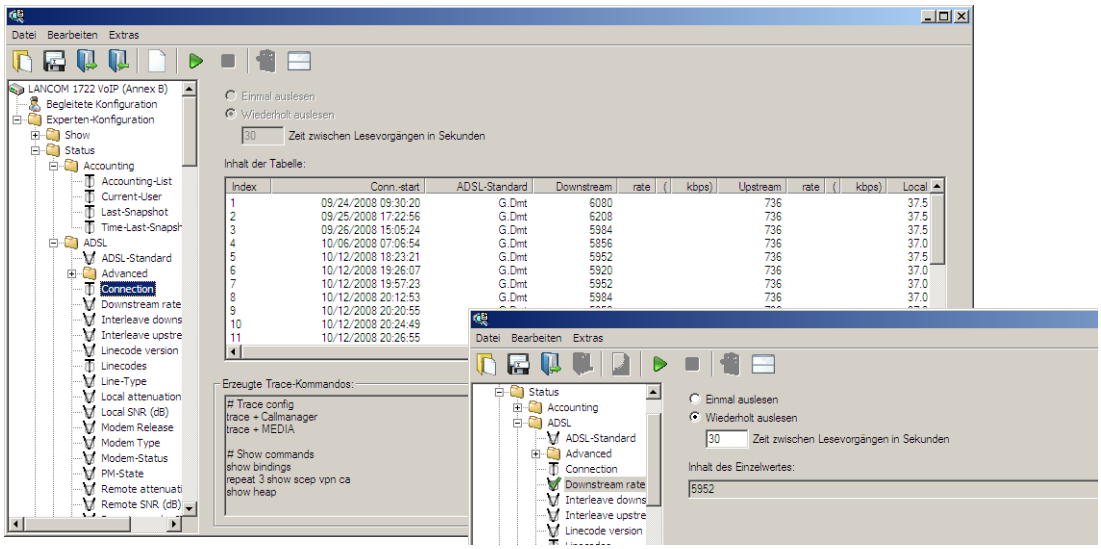
■ Status

Über die Kommandozeile (Telnet) oder über WEBconfig können umfangreiche Statusinformationen und Statistiken über ein Gerät abgefragt werden. Alle verfügbaren Status-Informationen können auch über den Trace-Dialog eingesehen werden. Tabellen und Einzelwerte werden dabei über spezielle Symbole dargestellt.

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 dem Namen des Eintrags. Zu jedem aktivierten Status-Eintrag kann separat eingestellt werden, ob er nur einmal beim Start des Traces ausgelesen wird oder in regelmäßigen Intervallen, die in Sekunden eingestellt werden.

Die Einstellungen der Status-Informationen werden zusammen mit den eigentlichen Trace-Einstellungen in der Trace-Konfiguration gespeichert. Die Status-Informationen werden zusammen mit den eigentlichen Trace-Daten gespeichert.



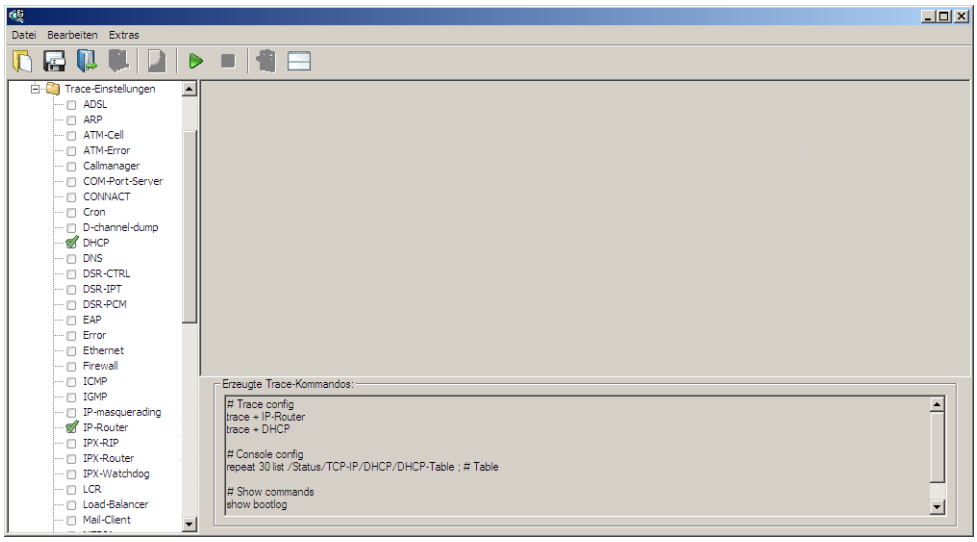
■ Trace-Einstellungen

Im Bereich der Trace-Einstellungen können die Traces aktiviert werden, die für das aktuelle Gerät ausgegeben werden sollen.

Um die Ausgabe des Traces in die Trace-Daten zu übernehmen, klicken Sie auf das entsprechende Kontrollkästchen vor dem Namen des Eintrags. Zu jedem Trace können Sie einen Filter eingeben. Wenn Sie z. B. nur die IP-Traces einer bestimmten Workstation anzeigen möchten, geben Sie die entsprechende IP-Adresse als Filter des IP-Router-Traces ein.

Anzeige der Trace-Daten

Die komplette Konfiguration des Traces wird im unteren Bereich des Dialogs angezeigt: Alle aktiven Trace-, Status- und Show-Einträge werden mit den jeweiligen Filtern und Parametern dort aufgelistet.



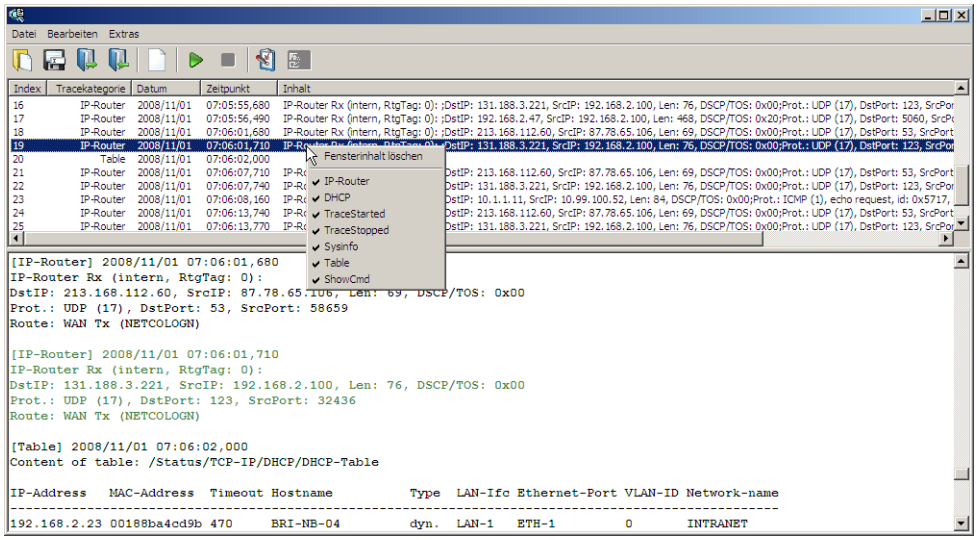
Um die Ausgabe der Trace-Daten zu starten, wechseln Sie mit dem Start-Button in den Anzeige-Modus. In dieser Ansicht werden die laufenden Trace-Ausgaben angezeigt:

- Im oberen Bereich werden die Trace-Ereignisse chronologisch aufgelistet.
- Im unteren Bereich werden die Ergebnisse der Ereignisse nacheinander aufgeführt.

Zur leichteren Navigation in langen Trace-Ausgaben können Sie im oberen Bereich auf ein Trace-Ereignis klicken, das entsprechende Ergebnis wird dann in der Liste aktiviert und in grün hervorgehoben.

Mit einem rechten Mausklick auf ein Trace-Ereignis öffnen Sie ein Kontext-Menü, in dem Sie die einzelnen Trace-Ergebnisse ein- und ausblenden können.

Die Trace-Daten werden erfasst, solange die Trace-Ausgabe aktiv ist. Um eine Überlastung des Arbeitsspeichers auf der Workstation mit dem LANmonitor zu vermeiden, werden die Trace-Daten automatisch in eine Backup-Datei gespeichert. Die zeitlichen Intervalle und die maximale Größe einer Sicherungsdatei können Sie unter **Extras ▶ Sonstige Einstellungen ▶ Tracebackup** einstellen.



Sichern und Wiederherstellen der Trace-Konfiguration

Zur späteren Wiederverwendung oder Weitergabe an einen anderen Benutzer kann die komplette Konfiguration der Trace-Ausgabe über **Datei ▶ Tracekonfiguration speichern** auf einen Datenträger geschrieben und später mit **Datei ▶ Tracekonfiguration laden** wieder geöffnet werden.

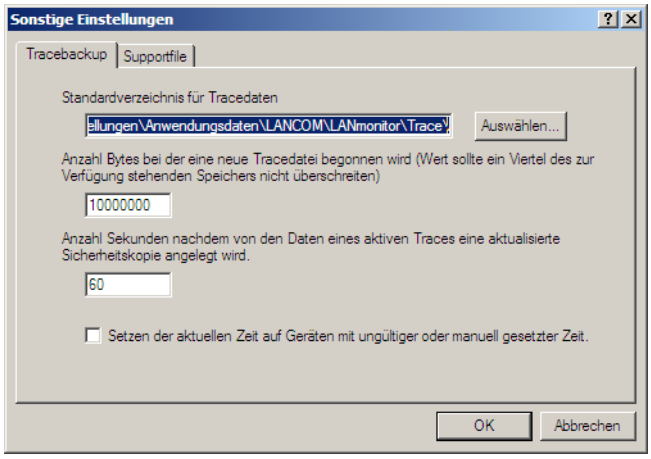
Sichern und Wiederherstellen der Trace-Daten

Auch die eigentlichen Trace-Daten können zur späteren Bearbeitung oder Weitergabe an einen anderen Benutzer über **Datei ▶ Tracedaten speichern** auf einen Datenträger geschrieben und später mit **Datei ▶ Tracedaten laden** wieder geöffnet werden.

Backup-Einstellungen für die Traces

Beim Starten eines Traces über LANmonitor wird automatisch eine Backup-Datei mit den aktuellen Trace-Daten gespeichert. Die Einstellungen für das Trace-Backup können Sie unter **Extras ▶ Sonstige Einstellungen ▶ Tracebackup** vornehmen. Stellen Sie dabei die folgenden Parameter ein:

- Verzeichnis für die Trace-Backups
- Maximale Größe einer Trace-Backup-Datei. Wenn diese Größe mit einem aktiven Trace erreicht wird, wird automatisch eine weitere Trace-Backup-Datei angelegt.
- Speicherintervall der Trace-Backup-Datei. Wenn diese Zeit erreicht ist, wird automatisch eine aktualisierte Version der Trace-Backup-Datei gespeichert. In der Trace-Backup-Datei sind also die Informationen zwischen dem letzten Backup und dem aktuellen Zeitpunkt nicht enthalten.
- Zusätzlich kann die aktuelle Zeit der Workstation mit dem LANmonitor als Zeit für den Trace gesetzt werden, z. B. wenn das getracte Gerät selbst nicht über eine gültige Zeitinformation verfügt.

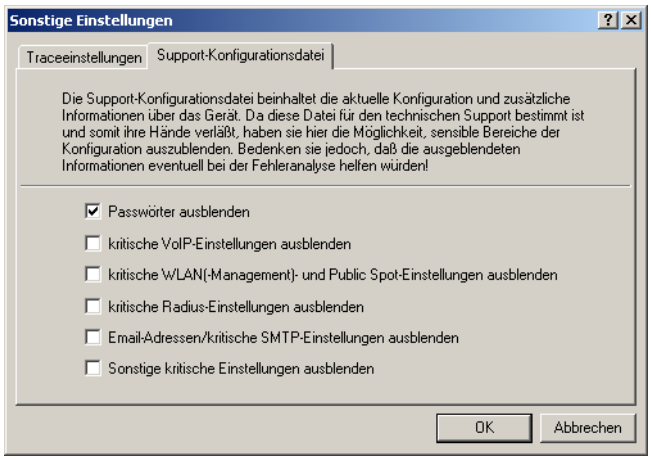


Support-Datei speichern

Mit einer Support-Datei können alle für den Support relevanten Informationen komfortabel in eine Datei geschrieben werden:

- Tracedaten wie in den aktuellen Einstellungen konfiguriert (wie mit der Funktion "Tracedaten speichern")
- aktuelle Gerätekonfiguration
- Bootlog
- Sysinfo

Beim Speichern der Gerätekonfiguration können dabei sicherheitsrelevante Informationen, die für den Support nicht von Bedeutung sind, ausgeblendet werden. Im Trace-Fenster unter **Extras ▶ Sonstige Einstellungen ▶ Supportfile** können Sie auswählen, welche Informationen nicht in der Support-Datei gespeichert werden sollen:



Die so 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.

C.2 SYSLOG

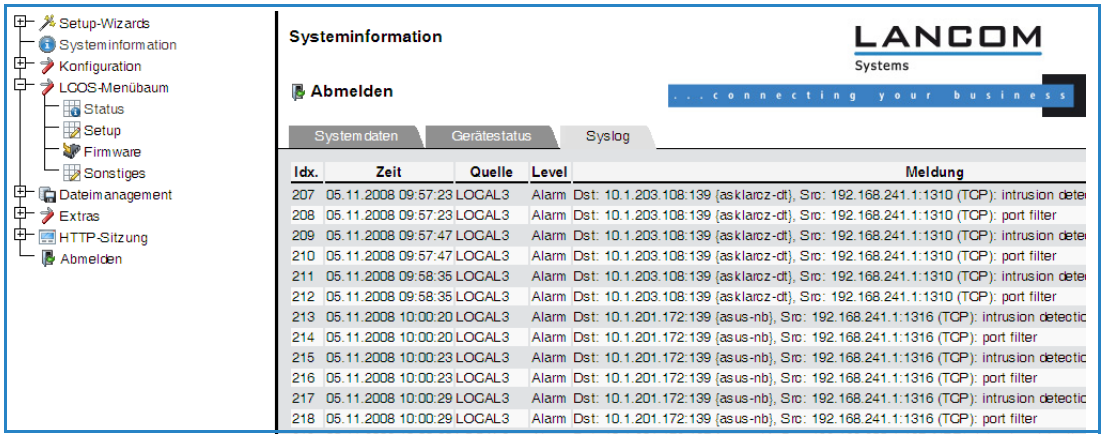
C.2.1 Einleitung

Über das SYSLOG-Protokoll werden die Aktivitäten eines LANCOM-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.

Die SYSLOG-Meldungen werden nur dann in den geräteinternen Speicher geschrieben, wenn das LANCOM 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:



C.2.2 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 LANCOM auf fünf Stufen reduziert. Die nachfolgende Tabelle zeigt die Zuordnung zwischen dem LANCOM-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
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 LANCOM einstellen können. Zusätzlich gibt Ihnen die letzte Spalte der Tabelle die standardmäßige Zuordnung zwischen den internen Quellen des LANCOM 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.

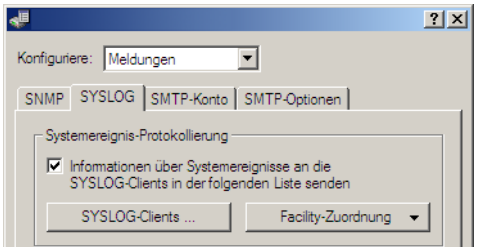
Für die Auswertung der SYSLOG-Meldungen im internen Speicher müssen die LANCOM-Geräte über eine gültige Zeitinformation verfügen.

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.

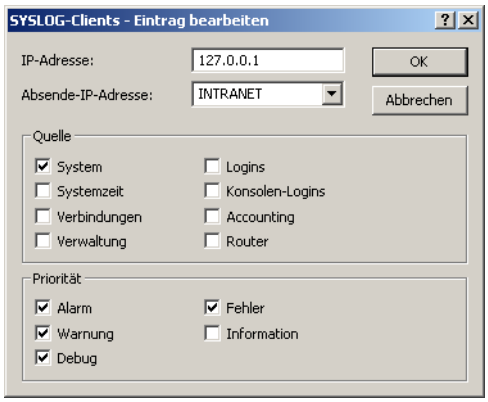
C.2.3 Konfiguration von SYSLOG über LANconfig

Die Parameter zur Konfiguration von SYSLOG finden Sie unter LANconfig im Konfigurationsbereich “Meldungen” auf der Registerkarte “SYSLOG”.

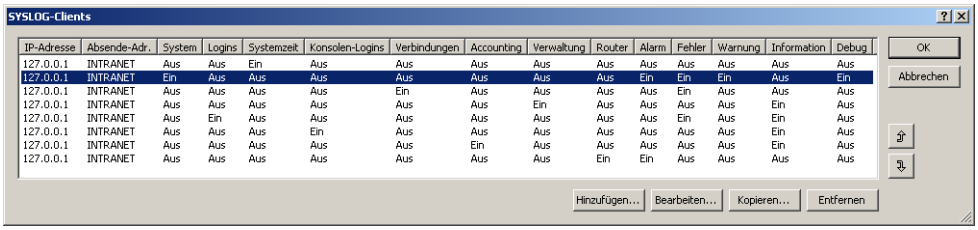


Anlegen von SYSLOG-Clients

Bei der Definition eines SYSLOG-Clients legen Sie zunächst die IP-Adresse fest, an welche die SYSLOG-Nachrichten geschickt werden sollen. Geben Sie dazu optional eine abweichende Absende-IP-Adresse an. Wählen Sie aus, welche der LANCOM-internen Quellen Nachrichten an diesen SYSLOG-Client versenden sollen. Mit der Auswahl von bestimmten Prioritäten können Sie den Umfang der Nachrichten weiter einschränken, z. B. nur auf Alarm- oder Fehlermeldungen.



Ab LCOS-Version 7.6 ist die Tabelle der SYSLOG-Clients im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Clients unter LANconfig:

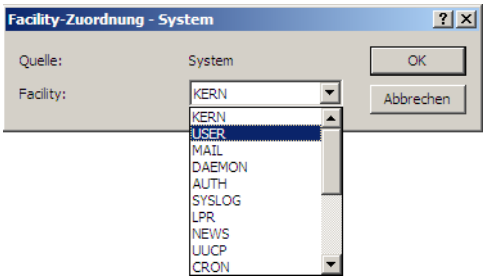


Weitere Informationen über die Bedeutung der vordefinierten SYSLOG-Clients sowie die Updatemöglichkeiten für bestehende LANCOM-Geräte finden Sie im Abschnitt “Tabelle der SYSLOG-Clients” bei der Konfiguration von SYSLOG über Telnet oder WEBconfig.

Zuordnung von LANCOM-internen Quellen zu SYSLOG-Facilities

Das SYSLOG-Protokoll verwendet bestimmte Bezeichnungen für die Quellen der Nachrichten, die so genanntne Facilities. Jede interne Quelle der LANCOM-Geräte, die eine SYSLOG-Nachricht erzeugen kann, muss daher einer SYSLOG-Facility zugeordnet sein.

Die standardmäßige Zuordnung kann bei Bedarf verändert werden. So können z. B. alle SYSLOG-Meldungen eines LANCOMs mit einer bestimmten Facility (Local7) versendet werden. Mit der entsprechenden Konfiguration des SYSLOG-Clients können so alle LANCOM-Meldungen in einer gemeinsamen Log-Datei gesammelt werden.



C.2.4 Konfiguration von SYSLOG über Telnet oder WEBconfig

Pfad: Setup/SYSLOG

■ **Aktiv**

Aktiviert den Versand von Informationen über Systemereignisse an die konfigurierten SYSLOG-Clients.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Port**

Port, der für den Versand der SYSLOG-Nachichten verwendet wird.

Mögliche Werte:

□ Max. 5 Zeichen

Default:

□ 514

Facility-Zuordnung

Pfad: Setup/SYSLOG/Facility-Mapper

■ **Facility**

Zuordnung der Quellen zu bestimmten Facilities.

Mögliche Werte:

□ KERNEL
□ AUTH
□ CRON
□ AUTHPRIV
□ LOCAL0
□ LOCAL1
□ LOCAL2
□ LOCAL3

■ **Quelle**

Zuordnung der Quellen zu bestimmten Facilities.

Mögliche Werte:

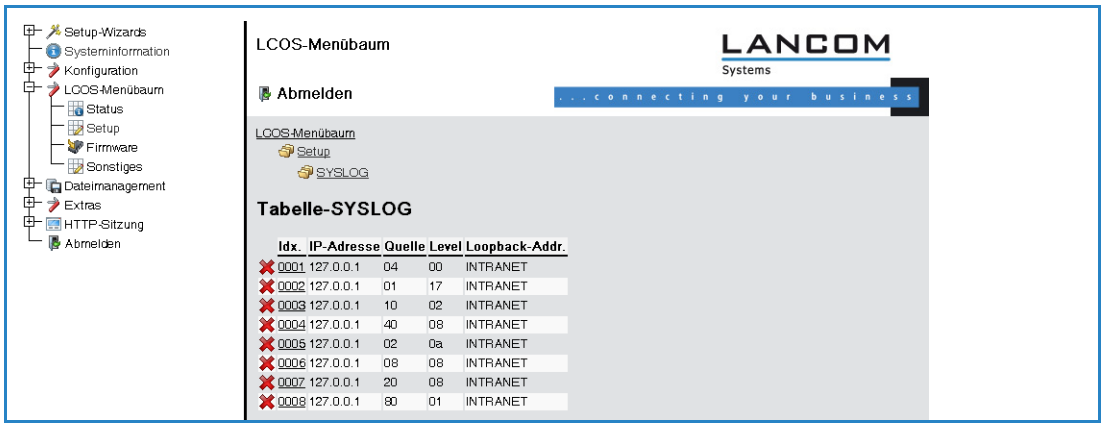
□ System
□ Logins
□ Systemzeit
□ Konsolen-Logins
□ Verbindungen

- □ Accounting
- □ Verwaltung
- □ Router

Tabelle der SYSLOG-Clients

Pfad: Setup/SYSLOG/Tabelle-SYSLOG

Ab LCOS-Version 7.6 ist die Tabelle der SYSLOG-Clients im Auslieferungszustand mit sinnvollen Einstellungen vorbelegt, um wichtige Ereignisse für die Diagnose im internen SYSLOG-Speicher abzulegen. Der folgende Screenshot zeigt diese vordefinierten SYSLOG-Clients unter WEBconfig:



Alle vordefinierten SYSLOG-Clients übertragen die Nachrichten an die IP-Adresse 127.0.0.1, also an das LANCOM selbst. Als Absende-IP-Adresse wird jeweils die IP-Adresse aus dem Netzwerk "INTRANET" verwendet. Die einzelnen Einträge haben die folgenden Funktionen:

Index	Quelle	Level	Bedeutung
0001	04	00	Systemzeit ohne Angabe eines Levels.
0002	01	17	Systemnachrichten mit dem Level Alarm, Fehler, Warnung oder Debug.
0003	10	02	Verbindungsnachrichten mit dem Level Fehler.
0004	40	08	Verwaltungsnachrichten mit dem Level Information.
0005	02	0a	Logins mit dem Level Fehler oder Information.
0006	08	08	Konsolen-Logins mit dem Level Information.
0007	20	08	Accountingnachrichten mit dem Level Information.
0008	80	01	Routernachrichten mit dem Level Alarm.

Wenn Sie ein bestehendes Gerät updaten, werden die Einstellungen für SYSLOG **nicht** auf diese Standardwerte gesetzt, sodass eventuell vorhandene Einstellungen erhalten bleiben. In diesem Fall können Sie die Einstellungen gemäß dieser Tabelle von Hand eintragen. Alternativ finden Sie in der "KnowledgeBase" im Support-Bereich der LANCOM-Webseite ein Script, mit dem Sie automatisch die vordefinierten SYSLOG-Clients einspielen können.

- **Idx.**

  Position des Eintrags in der Tabelle.

- **IP-Adresse**

  IP-Adresse des SYSLOG-Clients.

  Mögliche Werte:

  - □ Gültige IP-Adresse

  Default:

  - □ Leer

- **Quelle**

  Quelle, die zum Versenden einer Meldung führt. Jede Quelle wird durch einen bestimmten Code dargestellt.

  Mögliche Werte:

  - □ System: 01

- □ Logins: 02
- □ Systemzeit: 04
- □ Konsolen-Logins: 08
- □ Verbindungen: 10
- □ Accounting: 20
- □ Verwaltung: 40
- □ Router: 80

Default:

- □ 00

Besondere Werte:

- □ 00: Es wird keine Quelle spezifiziert.

■ **Level**

SYSLOG-Level, mit dem die Meldung verschickt wird. Jedes Level wird durch einen bestimmten Code dargestellt.

Mögliche Werte:

- □ Alarm: 01
- □ Fehler: 02
- □ Warning: 04
- □ Information: 08
- □ Debug: 10

Default:

- □ 00

Besondere Werte:

- □ 00: Es wird kein Level spezifiziert.

■ **Loopback-Addr.**

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten 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' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- □ Name einer Loopback-Adresse.
- □ Beliebige andere IP-Adresse.

Default:

- □ leer

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.

D WAN

D.1 Flexible Auswahl der PPP-Authentifizierungsprotokolle

D.1.1 Einleitung

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 LANCOM das Protokoll für die Authentifizierung fest eingestellt ist, kommt die Verbindung ggf. nicht zustande, da kein gemeinsames Authentifizierungsprotokoll ausgehandelt werden kann.

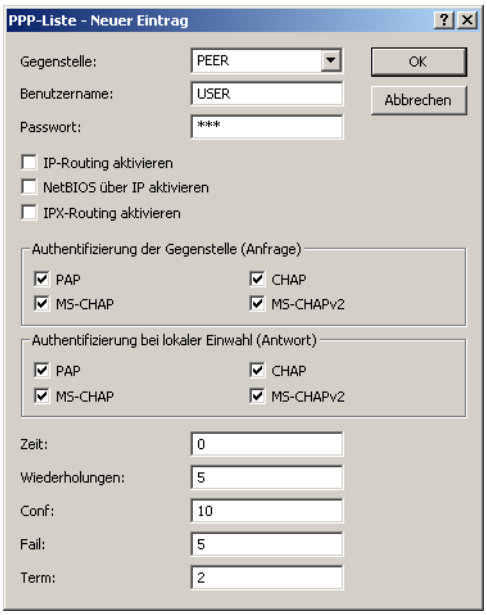
Prinzipiell ist es möglich, während der Verbindungsaushandlung eine erneute Authentifizierung durchzuführen und dafür ein anderes Protokoll auszuwählen, wenn dies zum Beispiel erst durch den Usernamen erkannt werden konnte. Diese erneute Aushandlung wird aber nicht in allen Szenarien unterstützt. Insbesondere bei der Einwahl über UMTS muss daher explizit vom LANCOM der Wunsch von der Providerseite nach CHAP abgelehnt werden, um für eine Weiterleitung der Anfragen beim Provider PAP-Userdaten bereitstellen zu können.

Mit der flexiblen Einstellung der Authentifizierungsprotokolle im LANCOM wird sichergestellt, dass die PPP-Verbindung wie gewünscht zustande kommt. Dazu können ein oder mehrere Protokolle definiert werden, die zur Authentifizierung von Gegenstellen im LANCOM (eingehende Verbindungen) bzw. beim Login des LANCOM in andere Gegenstellen (ausgehende Verbindungen) akzeptiert werden.

- Das LANCOM fordert beim Aufbau eingehender Verbindungen das niedrigste der zulässigen Protokolle, lässt aber je nach Möglichkeit der Gegenstelle auch eines der höheren (im LANCOM aktivierten) Protokolle zu.
- Das LANCOM 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



Telnet: Setup ▶ WAN ▶ PPP

D.1.2 Konfiguration

In der PPP-Liste können Sie für jede Gegenstelle, die mit Ihrem Netz Kontakt aufnimmt, eine eigene Definition der PPP-Verhandlung festlegen.

- **Gegenstelle**

  Name der Gegenstelle, mit dem sich diese bei Ihrem Router anmeldet.

- □ Mögliche Werte: max. 16 Zeichen
- □ Default: kein Eintrag
- □ Besondere Werte: DEFAULT (siehe Abschnitt "Die Bedeutung der DEFAULT-Gegenstelle")

■ **Username**

Name, mit dem sich Ihr Router bei der Gegenstelle anmeldet. Ist hier kein Eintrag vorhanden, wird der Gerätename Ihres Routers verwendet.

- □ Mögliche Werte: max. 64 Zeichen
- □ Default: kein Eintrag

■ **Passwort**

Passwort, das von Ihrem Router an die Gegenstelle übertragen wird (falls gefordert) bzw. das bei einer aktiven Überprüfung der Gegenstelle durch das LANCOM von der Gegenstelle erwartet wird.

- □ Mögliche Werte: max. 32 Zeichen
- □ Default: kein Eintrag

■ **Authent.request**

Verfahren zur aktiven Überprüfung der Gegenstelle.

- □ Mögliche Werte: PAP, CHAP, MS-CHAP, MS-CHAPv2, keine
- □ Default: kein Eintrag

■ **Authent-response**

Verfahren, die bei der passiven Überprüfung der Gegenstelle akzeptiert werden.

- □ Mögliche Werte: PAP, CHAP, MS-CHAP, MS-CHAPv2, keine
- □ Default: PAP, CHAP, MS-CHAP, MS-CHAPv2

Das LANCOM verwendet nur die hier aktivierten Protokolle, eine andere Verhandlung mit der Gegenstelle ist nicht möglich.

■ **Zeit**

Zeit zwischen zwei Überprüfungen der Verbindung mit LCP (siehe auch LCP). Diese Zeit geben Sie in Vielfachen von 10 Sekunden ein (also z. B. 2 für 20 Sekunden). Der Wert ist gleichzeitig die Zeit zwischen zwei Überprüfungen der Verbindung nach CHAP. Diese Zeit geben Sie in Minuten ein.

- □ Mögliche Werte: max. 2 Zeichen
- □ Default: 0

Für Gegenstellen mit Windows-Betriebssystem muss die Zeit auf '0' gesetzt werden!

■ **Wiederholungen**

Anzahl der Wiederholungen für den Überprüfungsversuch. Mit mehreren Wiederholungen schalten Sie den Einfluss kurzfristiger Leitungsstörungen aus. Erst wenn alle Versuche erfolglos bleiben, wird die Verbindung abgebaut. Der zeitliche Abstand zwischen zwei Wiederholungen beträgt 1/10 der Zeit zwischen zwei Überprüfungen, dies ist gleichzeitig die Anzahl der „Configure Requests", die der Router maximal aussendet, bevor er von einer Leitungsstörung ausgeht und selber die Verbindung abbaut.

- □ Mögliche Werte: max. 2 Zeichen
- □ Default: 0

■ **Conf, Fail, Term**

Mit diesen Parametern wird die Arbeitsweise des PPPs beeinflusst. Die Parameter sind in der RFC 1661 definiert und werden hier nicht näher beschrieben. Falls Sie keine PPP-Verbindungen aufbauen können, finden Sie in dieser RFC im Zusammenhang mit der PPP-Statistik des Routers Hinweise zur Behebung der Störung. Im Allgemeinen sind die Default-Einstellungen ausreichend. Diese Parameter können nur über LANconfig, SNMP oder TFTP verändert werden!

- □ Mögliche Werte: max. 3 Zeichen
- □ Default: 0

■ **Rechte**

Gibt die Protokolle an, die zu dieser Gegenstelle geroutet werden können.

- □ Mögliche Werte: IP, NetBIOS über IP, IPX
- □ Default: keine

D.1.3 Die Bedeutung der DEFAULT-Gegenstelle

Bei der PPP-Verhandlung meldet sich die einwählende Gegenstelle mit ihrem Namen beim LANCOM an. Anhand des Namens kann das LANCOM 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.

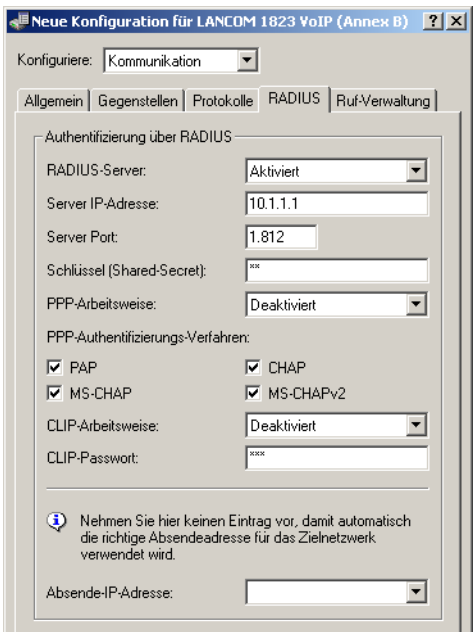
Wenn bei der Authentifizierung mit den unter DEFAULT eingetragenen Protokollen ein Protokoll verwendet wurde, das für die Gegenstelle nicht erlaubt ist, dann wird eine erneute Authentifizierung mit den erlaubten Protokollen durchgeführt.

D.1.4 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

■ **Aktiv**

Aktiviert die Verwendung eines externen RADIUS-Servers für die Authentifizierung von PPP-Verbindungen oder Einwahlzugängen.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Auth.-Port**

Der TCP/UDP-Port, über den der externe RADIUS-Server erreicht werden kann.

Mögliche Werte:

□ Gültige Portnummer

Default:

□ 1812

■ **Auth.- Protokolle**

Verfahren zur Sicherung der PPP-Verbindung, die der externe RADIUS-Server erlaubt.

Mögliche Werte:

□ PAP, CHAP, MS-CHAP, MS-CHAPv2, keine

Default:

□ PAP, CHAP, MS-CHAP, MS-CHAPv2

■ **CLIP Operation**

Bei der Einwahl von Gegenstellen kann die interne Rufnummernliste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

Mögliche Werte:

□ Ja: Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von Einwahlgegenstellen. Ein in der Rufnummernliste vorhandener, passender Eintrag hat allerdings Vorrang.

□ Nein: Es wird kein externer RADIUS-Server für die Authentifizierung von Einwahlgegenstellen verwendet.

□ Exklusiv: Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von Einwahlgegenstellen. Die Rufnummernliste wird nicht berücksichtigt.

Default:

□ Nein

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass der Name des Eintrags der Rufnummer der einwählenden Gegenstelle entspricht.

■ **CLIP Passwort**

Kennwort für die Anmeldung von Einwahlgegenstellen an einem externen RADIUS-Server.

Mögliche Werte:

□ Max. 31 Zeichen.

Default:

□ leer

Die Einwahlgegenstellen müssen im RADIUS-Server so konfiguriert werden, dass alle Einträge für Rufnummern das hier konfigurierte Kennwort verwenden.

■ **Loopback-Addr.**

Absenderadresse, die statt der ansonsten automatisch für die Zieladresse gewählten Absenderadresse verwendet wird.

Mögliche Werte:

□ Name eines definierten IP-Netzwerks.

□ 'INT' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'Intranet'.

□ 'DMZ' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.

□ Name einer Loopback-Adresse.

□ Beliebige andere IP-Adresse.

Default:

□ leer

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.

■ **PPP- Operation**

Bei der Einwahl von PPP-Gegenstellen können die internen Benutzer-Authentifizierungsdaten aus der PPP-Liste oder alternativ ein externer RADIUS-Server zur Authentifizierung verwendet werden.

Mögliche Werte:

□ Ja: Aktiviert die Nutzung eines externen RADIUS-Servers für die Authentifizierung von PPP-Gegenstellen. Ein in der PPP-Liste vorhandener, passender Eintrag hat allerdings Vorrang.

□ Nein: Es wird kein externer RADIUS-Server für die Authentifizierung von PPP-Gegenstellen verwendet.

□ Exklusiv: Aktiviert die Nutzung eines externen RADIUS-Servers als ausschließliche Möglichkeit für die Authentifizierung von PPP-Gegenstellen. Die PPP-Liste wird nicht berücksichtigt.

Default:

□ Nein

■ **Protokoll**

Für die Authentifizierung bei einem externen Server kann als Übertragungsprotokoll RADIUS über UDP oder RADSEC über TCP mit TLS verwendet werden.

Mögliche Werte:

□ RADIUS, RADSEC

Default:

□ RADIUS

■ **Schluessel**

Kennwort, das für den Zugriff auf den externen RADIUS-Server benötigt wird.

Mögliche Werte:

□ max. 32 Zeichen

Default:

□ leer

■ **Server-Adresse**

Adresse des externen RADIUS-Servers.

Mögliche Werte:

□ gültige IP-Adresse

Default:

□ leer

D.2 Die Aktions-Tabelle

D.2.1 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.

4.2.2 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. "MyLANCOM.dynDNS.org").

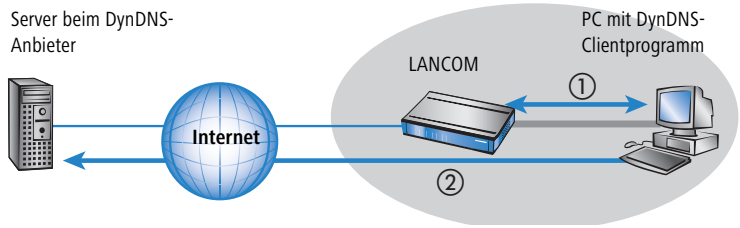
Der Vorteil liegt auf der Hand: Wenn Sie z.B. eine Fernwartung über WEBconfig/HTTP durchführen wollen, dann brauchen Sie lediglich den Dynamic DNS-Namen zu kennen. Außerdem können die DynDNS-Namen auch zum Aufbau von VPN-Verbindungnen zwischen Gegenstellen mit wechselnden IP-Adressen genutzt werden.

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 LANCOM 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.

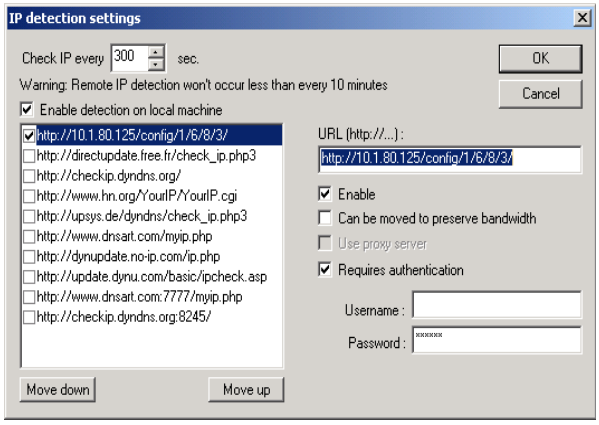
Dynamic-DNS-Client auf der Workstation

Dynamic DNS Anbieter unterstützen eine Reihe von PC-Clientprogrammen, die über verschiedene Methoden die aktuell zugewiesene IP-Adresse eines LANCOMs ermitteln können ①, und im Falle einer Änderung an den jeweiligen Dynamic DNS Server übertragen ②.



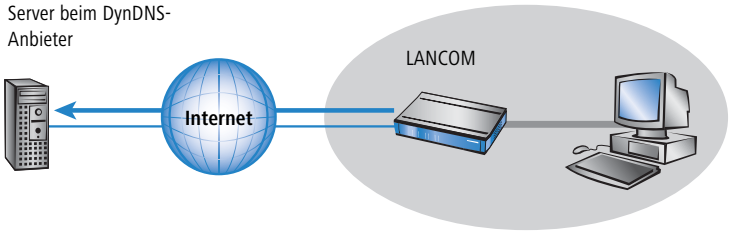
Die aktuelle WAN-seitige IP-Adresse eines LANCOMs kann unter folgender Adresse ausgelesen und dann in ein geeignetes Clientprogramm eingetragen werden:

```
http://<Adresse des LANCOM>/config/1/6/8/3/
```



Dynamic-DNS-Client im LANCOM über HTTP

Alternativ kann das LANCOM die aktuelle WAN-IP auch direkt an den DynDNS-Anbieter übertragen:

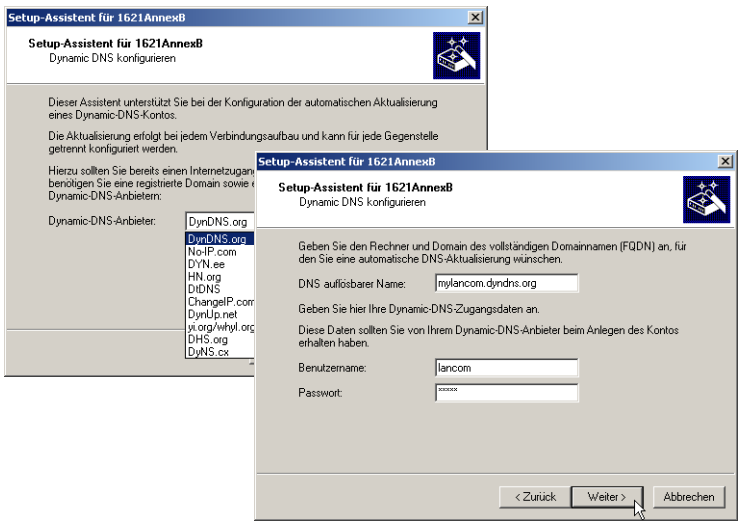


Dazu wird eine Aktion definiert, die z. B. nach jedem Verbindungsaufbau automatisch eine HTTP-Anfrage an den DynDNS-Server sendet, dabei die benötigten Informationen über das DynDNS-Konto übermittelt und so ein Update der Registrierung auslöst. Eine solche HTTP-Anfrage an den Anbieter DynDNS.org sieht 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 LANCOMs 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 anbieter-spezifische Parameter, die hier nicht näher beschrieben werden. Außerdem legt der Setup-Assistent weitere Aktionen an, mit denen das Verhalten des LANCOMs gesteuert wird für den Fall, dass die Aktualisierung nicht im ersten Durchlauf erfolgreich durchgeführt werden konnte.

Dynamic-DNS-Client im LANCOM 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 LANCOM 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 (3945 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 LANCOMs (%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 LANCOMs ausgewertet werden, um bei Bedarf weitere Aktionen einzuleiten.

D.2.3 Weitere Beispiele für Aktionen

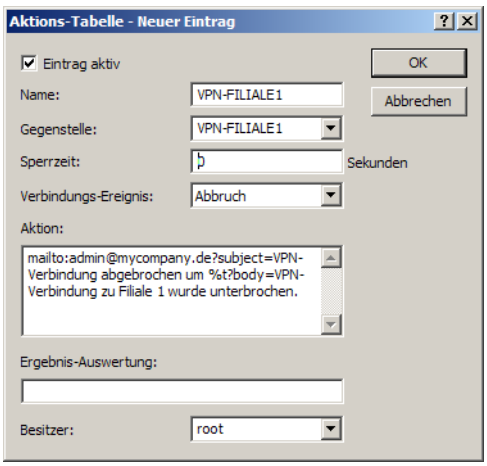
Information über Verbindungsabbruch als SMS auf Mobiltelefon melden

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 LANCOM 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.

Wenn die Mail an ein entsprechendes Mail2SMS-Gateway gesendet wird, kann die Benachrichtigung auch direkt auf ein Mobiltelefon zugestellt werden.

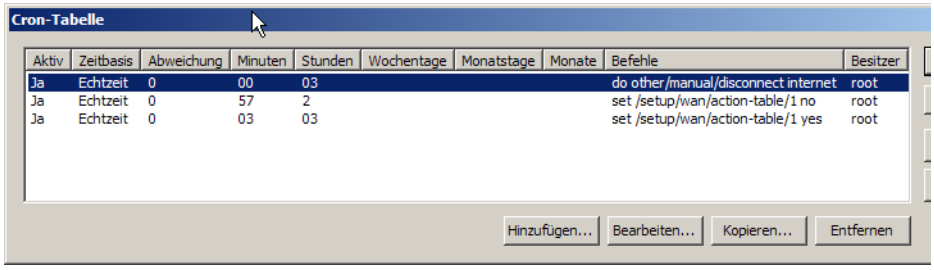
In einem komplexen Aufbau mit mehreren Filialen wird im LANCOM der Zentrale für jede Gegenstelle ein passender Eintrag angelegt. Zur Überwachung der Zentrale selbst wird eine Aktion in einem Gerät in einer der Filialen angelegt. So kann der Administrator auch dann benachrichtigt werden, wenn das VPN-Gateway 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.



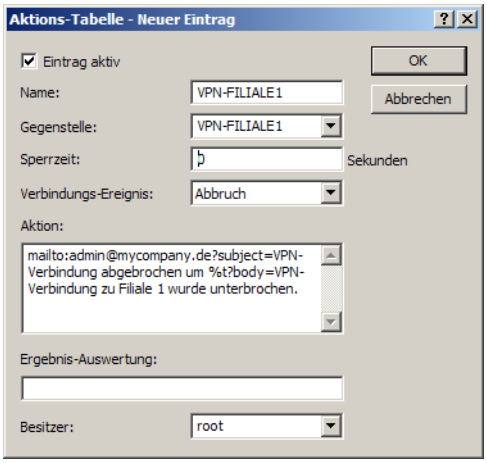
D.2.4 Konfiguration

Änderungen mit LCOS 7.6:

- "Fehler" als Bedingung für den Zustandswechsel der WAN-Verbindung
- "Aufbaufehler" als Bedingung für den Zustandswechsel der WAN-Verbindung
- Unterstützung des GnuDIP-Protokolls

In der Aktions-Tabelle können Sie Aktionen definieren, die ausgeführt werden, wenn sich am Zustand einer WAN-Verbindung etwas ändert.

LANconfig: Kommunikation ▶ Allgemein ▶ Aktions-Tabelle



Telnet: Setup ▶ WAN ▶ Aktions-Tabelle

- **Index**

  Der Index gibt die Position des Eintrags in der Tabelle an und muss daher eindeutig sein. Die Einträge der Aktions-Tabelle werden der Reihe nach ausgeführt, sobald der entsprechende Zustandswechsel der WAN-Verbindung eintritt. Mit dem Eintrag im Feld "Pruefen-auf" kann das Überspringen von Zeilen je nach Auswertung der Aktion ausgelöst werden. Der Index legt die Position der Einträge in der Tabelle fest (in aufsteigender Reihenfolge) und beeinflusst somit maßgeblich das Verhalten der Aktionen, wenn die Option "Pruefen-auf" verwendet

wird. Über den Index kann außerdem ein Eintrag aus der Aktions-Tabelle über einen Cron-Job angesprochen werden, z. B. um einen Eintrag zu bestimmten Zeiten zu aktivieren oder zu deaktivieren.

Mögliche Werte:

□ max. 10 Zeichen

Default:

□ 0

■ **Aktiv**

Aktiviert oder deaktiviert diesen Eintrag.

Mögliche Werte:

□ Ja

□ Nein

Default:

□ Ja

■ **Hostname**

Name der Aktion. Dieser Name kann mit dem Platzhalter %h (Hostname) in den Feldern "Aktion" und "Pruefen-auf" referenziert werden.

Mögliche Werte:

□ max. 64 Zeichen

Default:

□ leer

■ **Gegenstelle**

Name der Gegenstelle, deren Zustandswechsel die in diesem Eintrag definierte Aktion auslösen soll.

Mögliche Werte:

□ max. 16 Zeichen

Default:

□ leer

■ **Sperrzeit (max. 10 Zeichen)**

Unterbricht die wiederholte Ausführung der in diesem Eintrag definierten Aktion für die eingestellte Zeit in Sekunden.

Mögliche Werte:

□ max. 10 Zeichen

Default:

□ 0

■ **Bedingung**

Die Aktion wird ausgeführt, wenn der hier eingestellte Zustandswechsel der WAN-Verbindung eintritt.

Mögliche Werte:

□ Aufbau – Die Aktion wird ausgeführt, wenn die Verbindung erfolgreich aufgebaut wurde.

□ Abbau – Die Aktion wird ausgeführt, wenn die Verbindung durch das Gerät selbst beendet wurde (z. B. durch eine manuelle Trennung oder den Ablauf einer Haltezeit).

□ Ende – Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde (unabhängig vom Grund für den Abbau).

□ Fehler – Die Aktion wird ausgeführt, wenn die Verbindung beendet wurde, das Gerät selbst aber diesen Abbau nicht ausgelöst oder erwartet hat.

□ Aufbaufehler – Die Aktion wird ausgeführt, wenn ein Verbindungsaufbau gestartet wurde, die Verbindung aber nicht erfolgreich aufgebaut werden konnte.

Default:

□ Aufbau

■ **Aktion (max. 250 Zeichen)**

Hier beschreiben Sie die Aktion, die beim Zustandswechsel der WAN-Verbindung ausgeführt werden soll. In jedem Eintrag darf nur eine Aktionen ausgeführt werden.

Mögliche Werte für die Aktionen (maximal 250 Zeichen):

- □ exec: – Mit diesem Prefix leiten Sie alle Befehle ein, wie sie 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 Prefix leiten Sie eine DNS-Namensauflösung ein. Sie können z. B. mit der Aktion "dnscheck:myserver.dyndns.org" die IP-Adresse des angegebenen Servers ermitteln.
- □ http: – Mit diesem Prefix 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 wird in den folgenden Absätzen beschrieben.
- □ https: – Wie "http:", nur über eine verschlüsselte Verbindung.
- □ gnudip: – Mit diesem Prefix 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
  Der Zeilenumbruch dient nur der Lesbarkeit und wird nicht in die Aktion eingetragen. Die Bedeutung des Platzhalters %a wird in den folgenden Absätzen beschrieben.
- □ repeat: – Mit diesem Prefix und der Angabe einer Zeit in Sekunden werden alle Aktionen mit der Bedingung "Aufbau" wiederholt ausgeführt, sobald die Verbindung aufgebaut ist. Mit der Aktion "repeat:300" werden z. B. alle Aufbau-Aktionen alle fünf Minuten wiederholt.
- □ mailto: – Mit diesem Prefix lösen Sie den Versand einer E-Mail aus. Sie können z. B. mit der folgenden Aktion eine E-Mail an den Systemadministrator versenden, wenn eine Verbindung beendet wurde:
  mailto:admin@mycompany.de?subject=VPN-Verbindung abgebrochen um %t?body=VPN-Verbindung zu Filiale 1 wurde unterbrochen.

Mögliche Variablen zur Erweiterung der Aktionen:

- □ %a – WAN-IP-Adresse der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %H – Hostname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %h – wie %h, nur Hostname in Kleinbuchstaben
- □ %c – Verbindungsname der WAN-Verbindung, in deren Kontext diese Aktion ausgeführt wird.
- □ %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.

Das Ergebnis der Aktionen kann im Feld "Pruefen-auf" ausgewertet werden.

Default:

- □ leer

■ **Pruefen-auf**

Das Ergebnis der Aktion kann hier ausgewertet werden, um je nach Ergebnis eine bestimmte Anzahl von Einträge beim Abarbeiten der Aktions-Tabelle zu überspringen.

Mögliche Werte für die Aktionen (maximal 50 Zeichen):

- □ contains= – Dieses Prefix prüft, ob das Ergebnis der Aktion die definierte Zeichenkette enthält.
- □ isequal= – Dieses Prefix 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.

Mögliche Variablen zur Erweiterung der Aktionen:

- □ Wie bei der Definition der Aktion.

Default:

- □ leer

Beispiel:

- □ Mit einem DNS-Check wird die IP-Adresse einer Adresse der Form "myserver.dyndns.org" abgefragt. Mit der Prüfung "contains=%a?skipiftrue=2" können die beiden folgenden Einträge der Aktions-Tabelle übersprun-

gen werden, 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 die Aktion nicht ausgeführt werden.

  Mögliche Werte:

  □ Auswahl aus den im Gerät definierten Administratoren. Maximal 16 Zeichen.

  Default:

  □ root

D.3 Verwendung der seriellen Schnittstelle im LAN

D.3.1 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 LANCOM-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 LANCOM 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.

D.3.2 Betriebsarten

Ein COM-Port-Server kann in zwei verschiedenen Betriebsarten genutzt werden:

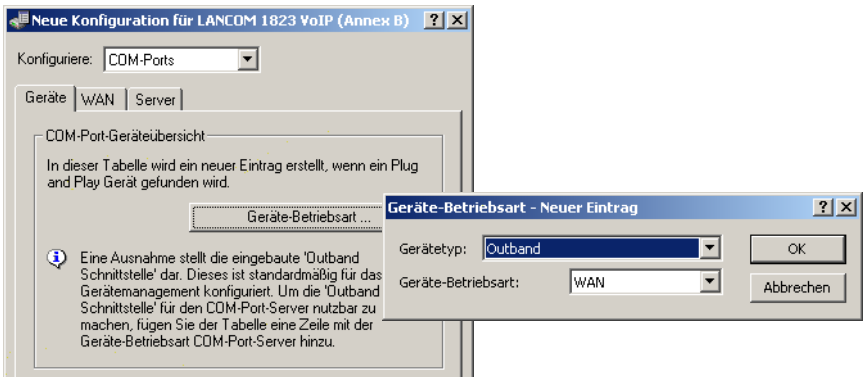
- Server-Modus: Der COM-Port-Server wartet auf einem definierten TCP-Port auf Anfragen zum Aufbau von TCP-Verbindungen. Diese Betriebsart wird z. B. für Fernwartungen genutzt.
- Client-Modus: Sobald ein an die serielle Schnittstelle angeschlossenes Gerät aktiv wird, öffnet der COM-Port-Client eine TCP-Verbindung 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.

D.3.3 Konfiguration der seriellen Schnittstellen

Die seriellen Schnittstellen können im LANCOM 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.

- □ Mögliche Werte: Alle im Gerät verfügbaren seriellen Schnittstellen.
- □ Default: Outband

■ **Dienst**

Aktivierung des Ports für den COM-Port-Server.

- □ Mögliche Werte: WAN, COM-Port-Server.
- □ Default: WAN

D.3.4 Konfiguration des COM-Port-Servers

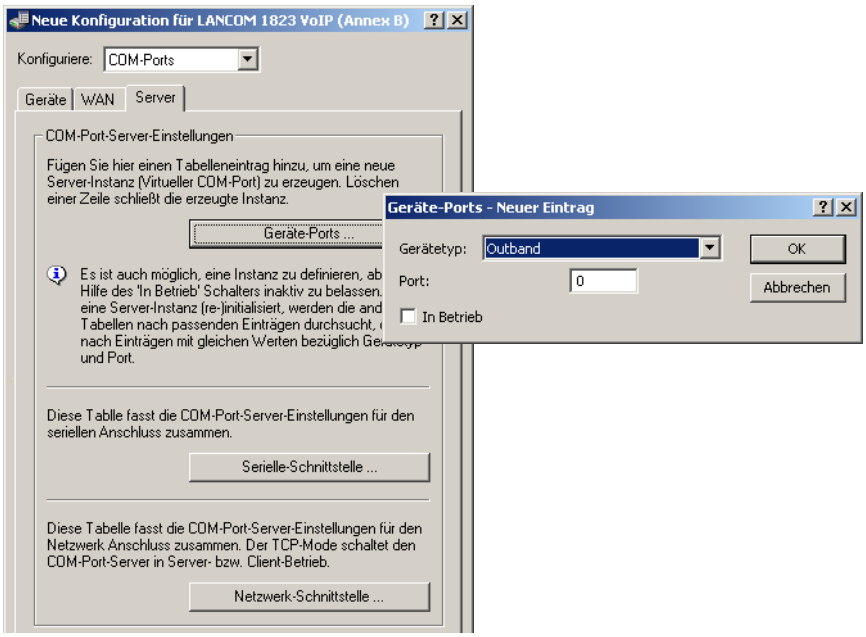
Die Konfiguration des COM-Port-Servers umfasst drei Tabellen. Allen drei Tabellen gemeinsam ist die Identifikation eines bestimmten Ports auf einer seriellen Schnittstelle über die Werte Device-Type und Port-Nummer. Da manche seriellen Geräte wie z. B. eine CardBus-Karte mehrere Ports haben, muss der 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



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Geraete

■ **Device-Type**

Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

- □ Mögliche Werte: Alle im Gerät verfügbaren seriellen Schnittstellen.
- □ Default: Outband

■ **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.

- □ Mögliche Werte: max. 10 Zeichen.
- □ Default: 0
- □ Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

■ **Operating**

Aktiviert den COM-Port-Server auf dem gewählten Port der gewählten Schnittstelle.

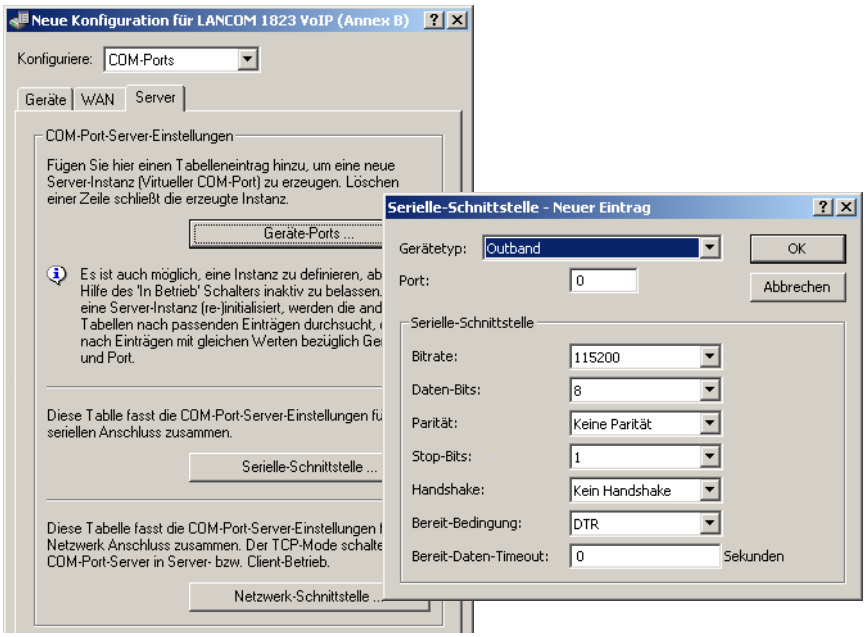
- □ Mögliche Werte: nein, ja.
- □ Default: nein

COM-Port-Einstellungen

Diese Tabelle enthält die Einstellungen für die Datenübertragung auf der seriellen Schnittstelle.

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



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ COM-Port-Einstellungen

- **Device-Type**

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

  - Mögliche Werte: Alle im Gerät verfügbaren seriellen Schnittstellen.
  - Default: Outband

- **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.

  - Mögliche Werte: max. 10 Zeichen.
  - Default: 0
  - Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

- **Bit-Rate**

  Verwendete Bitrate auf dem COM-Port.

  - Mögliche Werte: gängige Werte für die Bitrate von 110 bis 230400
  - Default: 9600

- **Daten-Bits**

  Anzahl der Daten-Bits.

  - Mögliche Werte: 7, 8
  - Default: 8

- **Paritaet**

  Auf dem COM-Port verwendetes Prüfverfahren.

  - Mögliche Werte: keine, gerade, ungerade
  - Default: keine

- **Stop-Bits**

  Anzahl der Stop-Bits.

  - Mögliche Werte: 1, 2
  - Default: 1

- **Handshake**

  Auf dem COM-Port verwendete Datenflusskontrolle.

  - Mögliche Werte: keiner, RTS/CTS
  - Default: RTS/CTS

- **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. Außer-

dem 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".

- Mögliche Werte: DTR, Daten
- Default: DTR

- **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.

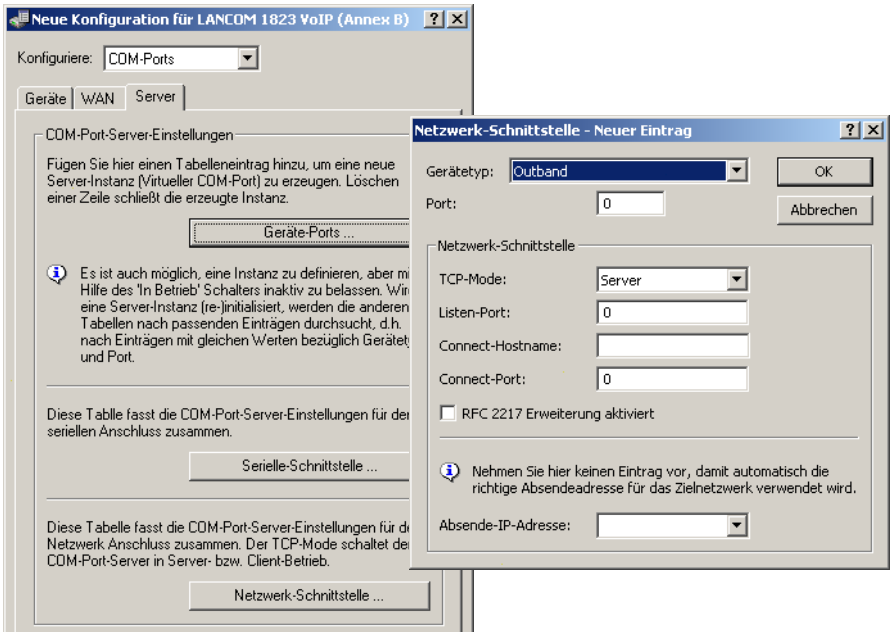
  - Mögliche Werte: max. 10 Zeichen
  - Default: 0
  - Besondere Werte: 0 schaltet den Bereit-Daten-Timeout aus.

Netzwerk-Einstellungen

Diese Tabelle enthält alle Einstellungen, die das Verhalten des COM-Ports im Netzwerk definieren.

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



Telnet: Setup ▶ COM-Ports ▶ COM-Port-Server ▶ Netzwerk-Einstellungen

- **Device-Type**

  Auswahl aus der Liste der im Gerät verfügbaren seriellen Schnittstellen.

  - Mögliche Werte: Alle im Gerät verfügbaren seriellen Schnittstellen.
  - Default: Outband

- **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.

  - Mögliche Werte: max 10 Zeichen.
  - Default: 0
  - Besondere Werte: 0 für serielle Schnittstellen mit nur einem Port wie z. B. Outband.

- **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 wer-

den 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 LANCOM die offenen Verbindungen bei einem Neustart des Gerätes.

- Mögliche Werte: Server, Client
- Default: Server

Listen-Port

Auf diesem TCP-Port erwartet der COM-Port im TCP-Server-Modus eingehende Verbindungen.

- Mögliche Werte: max 10 Zeichen.
- Default: 0

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.

- Mögliche Werte: max. 48 Zeichen. Der Host darf entweder als DNS-Name oder als IP-Adresse angegeben werden.
- Default: leer

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.

- Mögliche Werte: max. 10 Zeichen.
- Default: 0

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.

- Mögliche Werte: max. 16 Zeichen.
- Default: leer

RFC2217-Erweiterungen

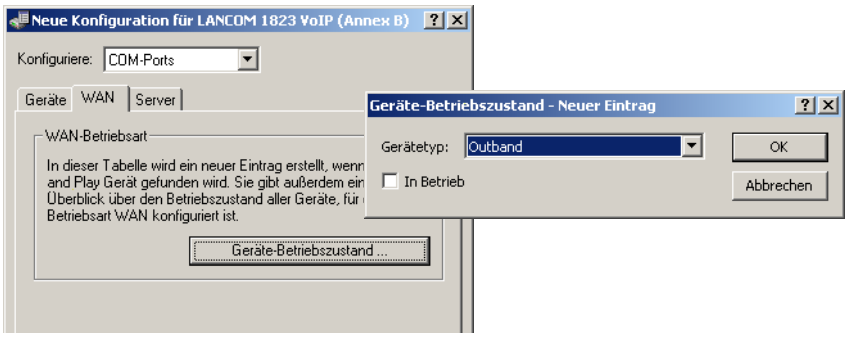
Die RFC2217-Erweiterungen können für beide TCP-Modi aktiviert werden. Wenn diese Erweiterungen eingeschaltet sind, signalisiert ein LANCOM seine Bereitschaft, Telnet Steuerungssequenzen zu akzeptieren, mit der Sequenz IAC DO COM-PORT-OPTION. In der Folge werden auf dem COM-Port die entsprechenden Optionen 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.

- Mögliche Werte: nein, ja.
- Default: nein

D.3.5 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



Telnet: Setup ▶ COM-Ports ▶ WAN ▶ Geraete

■ **Device-Type**

Liste der im Gerät verfügbaren seriellen Schnittstellen.

□ Mögliche Werte: Alle im Gerät verfügbaren seriellen Schnittstellen.

■ **Aktiv**

Status des angeschlossenen Gerätes:

□ Mögliche Werte: nein, ja

D.3.6 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 LANCOMs 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.

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.
  - □ Mögliche Werte: gängige Werte für die Bitrate von 110 bis 230400
- **Daten-Bits**
  Anzahl der Daten-Bits.
  - □ Mögliche Werte: 7, 8
- **Paritaet**
  Auf dem COM-Port verwendetes Prüfverfahren.
  - □ Mögliche Werte: keine, gerade, ungerade
- **Stop-Bits**
  Anzahl der Stop-Bits.
  - □ Mögliche Werte: 1, 2
- **Handshake**
  Auf dem COM-Port verwendete Datenflusskontrolle.
  - □ Mögliche Werte: keiner, RTS/CTS

Byte-Counters

In dieser Tabelle werden die eingehenden und ausgehenden Datenpakete auf dem seriellen Port und der Netzwerk-Seite angezeigt.

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.

D.3.7 COM-Port-Adapter

Zum Anschluss von Geräten mit seriellen Schnittstellen an ein LANCOM stehen folgende Möglichkeiten bereit:

Adapter	LANCOM-Geräte
COM-Port-Adapter	Alle mit serieller Konfigurationsschnittstelle
USB-Seriell-Adapter	Alle mit USB-Schnittstelle
CardBus-Seriell-Adapter	Alle mit CardBus-Einschub
LANCOM Modem-Adapter-Kit	Alle mit serieller Konfigurationsschnittstelle

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
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

D.4 RIP

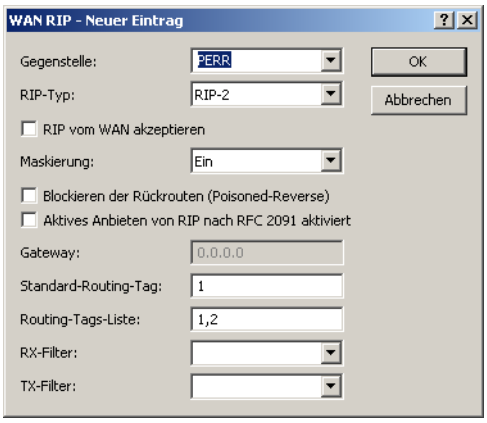
D.4.1 WAN-RIP

Neu mit LCOS 7.6:

- Flexible Definition der WAN-RIP-Gegenstellen mit Platzhaltern.

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

■ **Gegenstelle**

Name der Gegenstelle, mit der Routing Informationen per RIP ausgetauscht werden sollen.

Mögliche Werte:

□ Auswahl aus der Liste der definierten Gegenstellen (max. 16 Zeichen).

Default:

□ Leer

Besondere Werte:

□ Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen per WAN-RIP dynamische Routinginformationen per RIP austauschen, während für alle anderen User und Filialen eine statische Netzvergabe existiert, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "RIP_" bekommen. In der WAN-RIP-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "RIP_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

■ **RIP-Typ**

Der RIP-Typ gibt an, mit welcher RIP-Version die lokalen Routen propagiert werden.

Mögliche Werte:

□ Aus
□ RIP-1
□ RIP-1-kompatibel
□ RIP-2

Default:

□ Aus

■ **RIP-lernen**

In der Spalte RIP-Accept wird angegeben, ob RIP aus dem WAN akzeptiert wird und Routen von dieser Gegenstelle gelernt werden sollen. Dazu muss gleichzeitig der RIP-Typ gesetzt sein.

Mögliche Werte:

□ Ein/Aus

Default:

□ Aus

■ **Maskierung**

In der Spalte Masquerade wird angegeben ob und wie auf der Strecke maskiert wird. Durch diesen Eintrag ist es möglich, das WAN-RIP auch mit einer leeren Routing-Tabelle zu starten.

Mögliche Werte:

□ Auto: Der Maskierungstyp wird aus der Routing-Tabelle entnommen. Existiert für die Gegenstelle kein Routing-Eintrag, so wird nicht maskiert.
□ An: Alle IP Verbindungen zu dieser Gegenstelle werden maskiert.

- □ Intranet: IP Verbindungen aus Intranet Netzen werden maskiert, IP Verbindungen aus DMZ Netzen werden transparent übertragen.

■ **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.

Mögliche Werte:

- □ Ja/Nein

Default:

- □ Nein

■ **RFC 2091**

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 (triggered 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.

Mögliche Werte:

- □ Ja/Nein

Default:

- □ Nein

■ **Gateway**

IP-Adresse des nächsten erreichbaren Routers im Zusammenhang mit RFC 2091.

Mögliche Werte:

- □ Gültige IP-Adresse

Default:

- □ 0.0.0.0

Besondere Werte:

- □ Bei Eingabe von 0.0.0.0 wird die Gateway-Adresse aus der PPP-Verhandlung bestimmt.

In einem Router in der Zentrale kann die RFC 2091 ausgeschaltet werden und die Gateway-Adresse auf 0.0.0.0 bleiben, da sich die Zentrale immer an die Anfragen der Filialen hält.

Das LANCOM fällt automatisch auf Standard-RIP zurück, wenn das angegebene Gateway RFC 2091 nicht unterstützt.

■ **Dft-Rtg-Tag**

In der Spalte Dft-Rtg-Tag steht das für die WAN-Verbindung geltende „Default-Routing-Tag“. Alle ungetaggten Routen werden beim Versenden im WAN mit diesem Tag getaggt.

Mögliche Werte:

- □ 0 bis 65535

Default:

- □ 0

■ **Rtg-Tag-List**

In der Spalte Rtg-Tag-List steht eine kommaseparierte Liste der Tags, die auf dem Interface akzeptiert werden. Wenn diese Liste leer ist, dann werden alle Tags akzeptiert. Steht mindestens ein Tag in der Liste, dann werden nur die Tags in dieser Liste akzeptiert. Ebenso werden beim Senden von getaggten Routen auf das WAN nur Routen mit erlaubten Tags propagiert.

Alle vom WAN gelernten Routen werden intern als ungetaggte Routen behandelt und auf das LAN mit dem Default-Tag (0) propagiert. Auf das WAN hingegen werden sie mit dem Tag propagiert, mit dem sie auch gelernt wurden.

Mögliche Werte:

□ Maximal 33 Zeichen

Default:

□ Leer

■ **Rx-Filter**

Geben Sie hier den Filter an, der beim Empfang von RIP-Paketen verwendet werden soll.

Mögliche Werte:

□ Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

Default:

□ Leer

■ **Tx-Filter**

Geben Sie hier den Filter an, der beim Versand von RIP-Paketen verwendet werden soll.

Mögliche Werte:

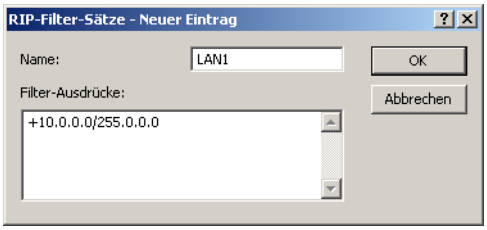
□ Auswahl aus der Liste der definierten RIP-Filter (max. 16 Zeichen).

Default:

□ Leer

D.4.2 RIP-Filter

LANconfig: IP-Router ▶ Allgemein ▶ RIP-Filter-Sätze



Telnet: Setup ▶ IP-Router ▶ 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.

■ **Name**

Name des Filtereintrags.

Mögliche Werte:

□ 18 alphanumerische Zeichen. Die beiden letzten Zeichen können nur aus dem Rautezeichen kombiniert mit einer Ziffer bestehen (z. B. #1). Für die Zuweisung zu LAN- und WAN-Netzen können also nur 16 Zeichen verwendet werden.

Beispiele:

□ LAN#1, LAN#2, WAN1 etc.

Mit dem Rautezeichen # können mehrere Einträge zu einem einzigen Filter verbunden werden. Die Einträge LAN#1 und LAN#2 bilden zusammen also einen Filter „LAN“, der in der RIP-Tabelle aufgerufen werden kann.

■ **Filter**

Kommaseparierte Liste von Netzwerken, die akzeptiert (+) oder abgelehnt (-) werden sollen.

□ Beispiel für akzeptiertes Netzwerk: +10.0.0.0/255.0.0.0

□ Beispiel für abgelehntes Netzwerk: -192.168.0.0/255.255.0.0

□ Mögliche Werte: 64 Zeichen aus `,+-/0123456789.`

Die Angabe des Pluszeichens für akzeptierte Netzwerke ist optional.

Die in der Filtertabelle definierten Filter können in der LAN-RIP- und WAN-RIP-Tabelle in den Spalten RX- und TX-Filter referenziert werden. Dabei werden mit RX die Filter angesprochen, die das Lernen der Routen von diesen Netzwerken erlauben oder sperren – mit TX werden die Netzwerke definiert, zu denen das Propagieren der Routen erlaubt oder gesperrt werden soll.

Die Filterung über Routing-Tags bleibt davon unberührt, d. h., wenn eine Route schon aufgrund ihres Tags nicht gelernt bzw. propagiert werden darf, dann kann das nicht über die Filtertabellen erzwungen werden.

D.5 Advanced Routing and Forwarding

D.5.1 Schnittstellen-Tags für Gegenstellen

Neu mit LCOS 7.6:

- Zuweisung von Schnittstellen-Tags über die Gegenstelle

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:

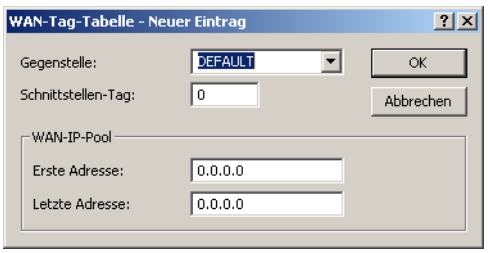
- mit Hilfe von entsprechenden Firewall-Regeln, die nur Datenpakete von bestimmten Gegenstellen, IP-Adressen oder Ports erfassen
- anhand der Routing-Tabelle
- über eine explizite Zuordnung der Tags zu den Gegenstellen.

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 bstimmt werden. Ein- und ausgehende Kommunikation kann somit einfacher bidirektional in virtuelle Router unterteilt werden.

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
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 .

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

Über die Tag-Tabelle kann den eingehenden Datenpaketen anhand der Gegenstelle direkt ein Schnittstellen-Tag zugewiesen werden.

■ Telnet: Setup ▶ IP-Router ▶ Tag-Tabelle

■ **Gegenstelle**

Name der Gegenstelle, zu deren Paketen beim WAN-seitigem Empfang Schnittstellen-Tags hinzugefügt werden sollen.

Mögliche Werte:

- □ Auswahl aus der Liste der definierten Gegenstellen (max. 16 Zeichen).

Default:

- □ Leer

Besondere Werte:

- □ Mit dem * als Platzhalter können in einem Eintrag mehrere Gegenstellen konfiguriert werden. Sollen z. B. mehrere Gegenstellen (RAS-Benutzer) einer Firma getaggt werden, können alle entsprechenden Gegenstellen einen Namen mit dem Prefix "Firma1_" bekommen. In der Tag-Tabelle wird dann nur noch ein Eintrag mit der Gegenstelle "Firma1_*" aufgenommen, um alle Gegenstellen zu konfigurieren.

■ **Rtg-Tag**

Dieses Schnittstellen-Tag wird den eingehenden Paketen der Gegenstelle zugewiesen.

Mögliche Werte:

- □ 0 bis 65535

Default:

- □ 0

■ **Start-WAN-Pool**

Der Start-WAN-Pool stellt den Beginn des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

Mögliche Werte:

- □ Max. 15 Zeichen

Default:

□ 0.0.0.0

Besondere Werte:

□ Wenn der Pool leer ist (Start- und End-Adresse sind 0.0.0.0), dann wird der globale Pool verwendet.

■ **Ende-WAN-Pool**

Der End-WAN-Pool stellt das Ende des Adress-Pools für die Gegenstelle bzw. die Gruppe von Gegenstellen dar (bei Verwendung von Platzhaltern bei der Angabe der Gegenstelle). Bei der Einwahl von RAS-Benutzern wird der Gegenstelle eine Adresse aus dem hier definierten Adress-Pool zugewiesen.

Mögliche Werte:

□ Max. 15 Zeichen

Default:

□ 0.0.0.0

Besondere Werte:

□ Wenn der Pool leer ist (Start- und End-Adresse sind 0.0.0.0), dann wird der globale Pool verwendet.

E VPN

E.1 Unbegrenzte Anzahl der VPN-Gegenstellen

Durch die Umstellung einiger Tabellen des LCOS auf dynamische Größen können u. a. in den VPN-Setup-Tabellen beliebig viele Gegenstellen eingetragen werden. Die von der Lizenz abhängige Anzahl gleichzeitig möglicher Verbindungen bleibt dabei unverändert.

E.2 Extended Authentication Protocol (XAUTH)

E.2.1 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.

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).

E.2.2 XAUTH im LCOS

Im LANCOM 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:

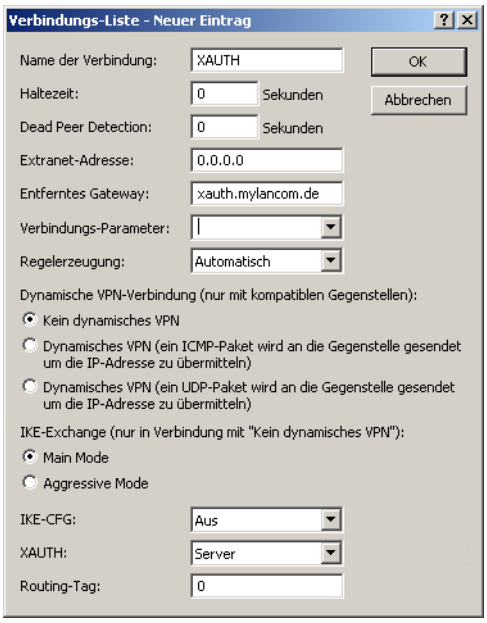
XAUTH-Betriebsart	Server	Client
XAUTH-Benutzername	Gegenstelle aus der PPP-Tabelle. Es wird dabei der Eintrag aus der PPP-Tabelle gewählt, bei dem die PPP-Gegenstelle dem übermittelten XAUTH-Benutzernamen entspricht. Die PPP-Gegenstelle muss dabei auch der verwendeten VPN-Gegenstelle entsprechen.	Benutzername aus der PPP-Tabelle. 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.

Da in der LCOS-Version 7.60 in der Betriebsart als XAUTH-Server der übermittelte XAUTH-Benutzername dem Namen der VPN-Gegenstelle entsprechen muss, kann für jede VPN-Gegenstelle nur ein Benutzer über XAUTH authentifiziert werden. Eine Authentifizierung über einen RADIUS-Server ist in LCOS 7.60 nicht vorgesehen.

E.2.3 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

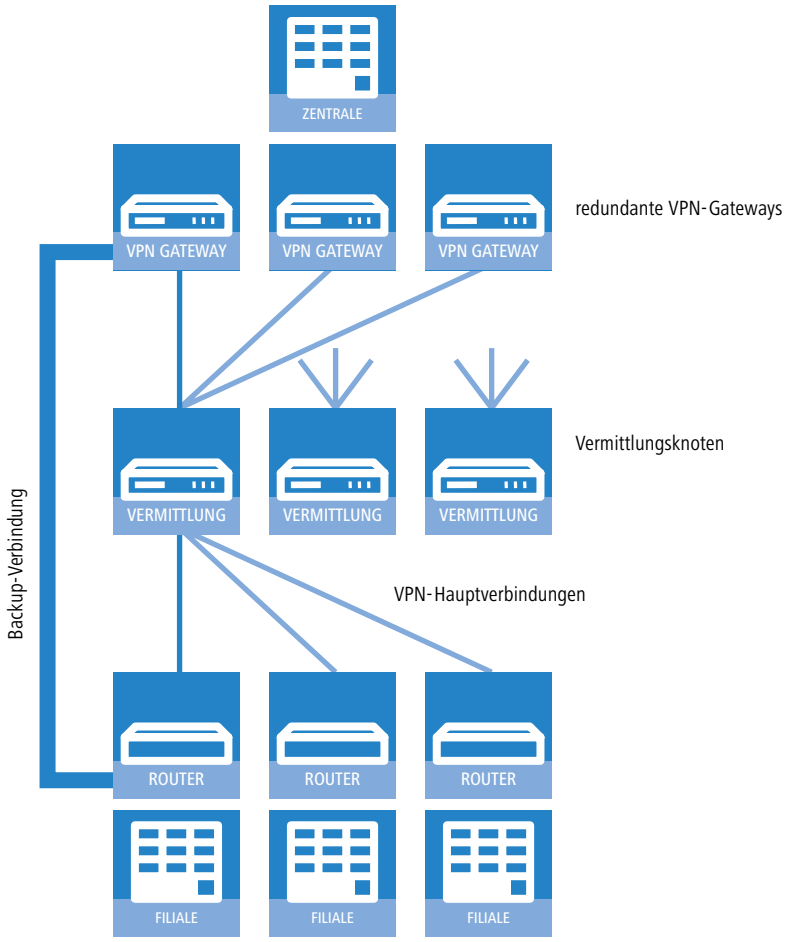
Wenn die XAUTH-Authentifizierung für eine VPN-Gegenstelle aktiviert ist, muss die Option IKE-CFG auf den gleichen Wert eingestellt werden.

E.3 Backup über alternative VPN-Verbindung

E.3.1 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.

E.3.2 Backup-fähige Netzstruktur

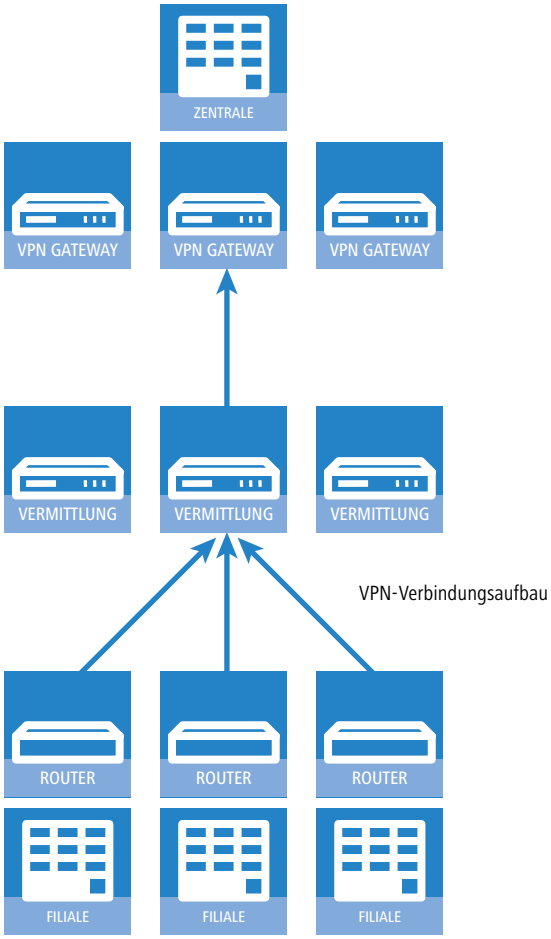
Um auch für diese Anwendungen ein funktionsfähiges Backup aufbauen zu können, müssen die in den folgenden Abschnitten beschriebenen Aspekte erfüllt sein.

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.

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.

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.

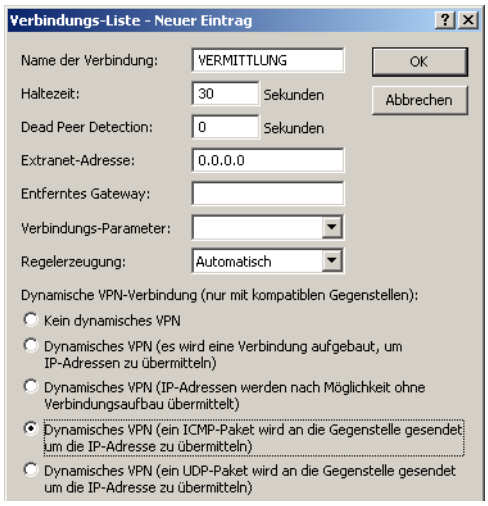
Um das zu verhindern, wird zunächst eine "Dynamic VPN"-Verhandlung mit der Gegenstelle der Hauptverbindung durchgeführt. Verläuft diese Verhandlung erfolgreich, kann die Hauptverbindung wieder aufgebaut werden. Dazu wird zunächst die Backup-Verbindung getrennt und zusätzlich der Backup-Status zurückgesetzt. So wird verhindert, dass die Backup-Verbindung sofort wieder aufgebaut wird. Erst danach wird die Hauptverbindung mit den ursprünglichen VPN-Regeln wieder etabliert.

Die Nutzung der "Dynamic VPN"-Verbindung zwischen Filiale und Vermittlungsknoten ist eine notwendige Voraussetzung für die hier beschriebene Backup-Funktion.

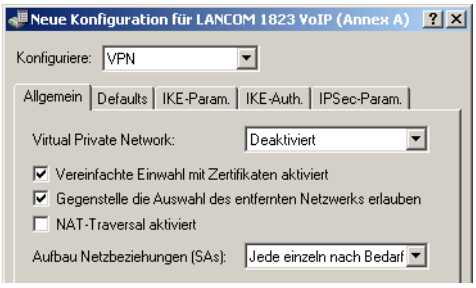
E.3.3 Konfiguration des VPN-Backups

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.

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.

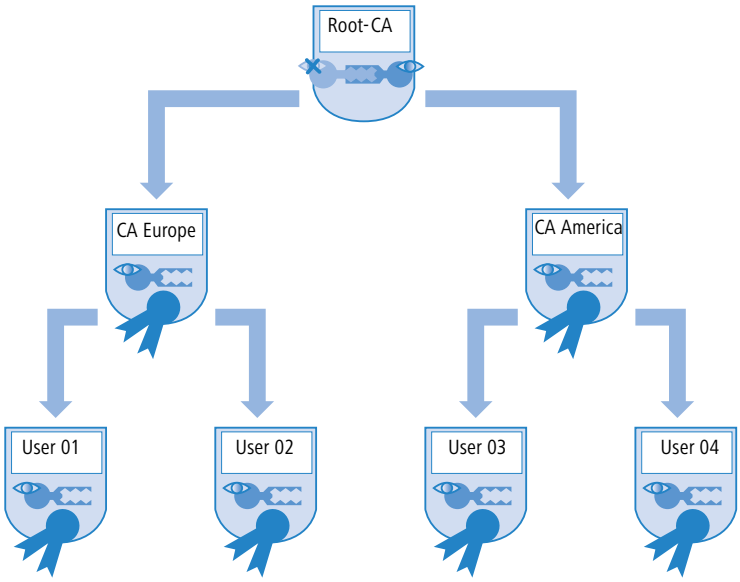
E.4 Mehrstufige Zertifikate für SSL/TLS

Neu mit LCOS 7.6:

- Mehrstufige Zertifikate für SSL/TLS

E.4.1 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.

E.4.2 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 LANCOM senden. Die Zertifikatskette wird im LANCOM auf Gültigkeit geprüft.

E.4.3 VPN mit mehrstufigen Zertifikaten

Für den zertifikatsbasierten Aufbau von VPN-Verbindungen werden im Dateisystem des LANCOM 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 LANCOM 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 LANCOM kann dieses Zertifikat dann gegen die vorhandene Hierarchie prüfen.

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.

F Firewall

F.1 Konfiguration der Firewall mit LANconfig

Neu in LCOS 7.60:

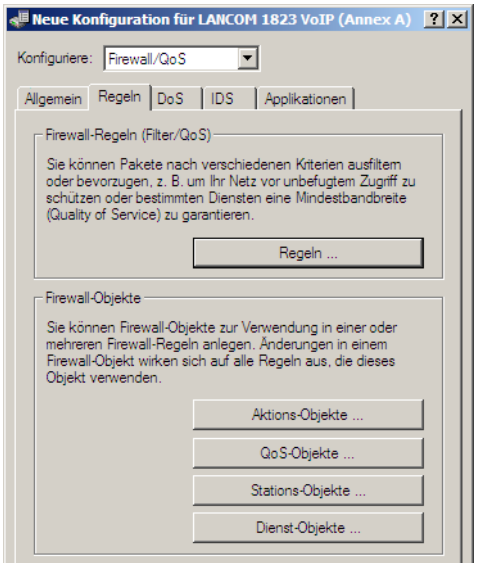
- Objektorientierte Definition der Firewall-Regeln

F.1.1 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.

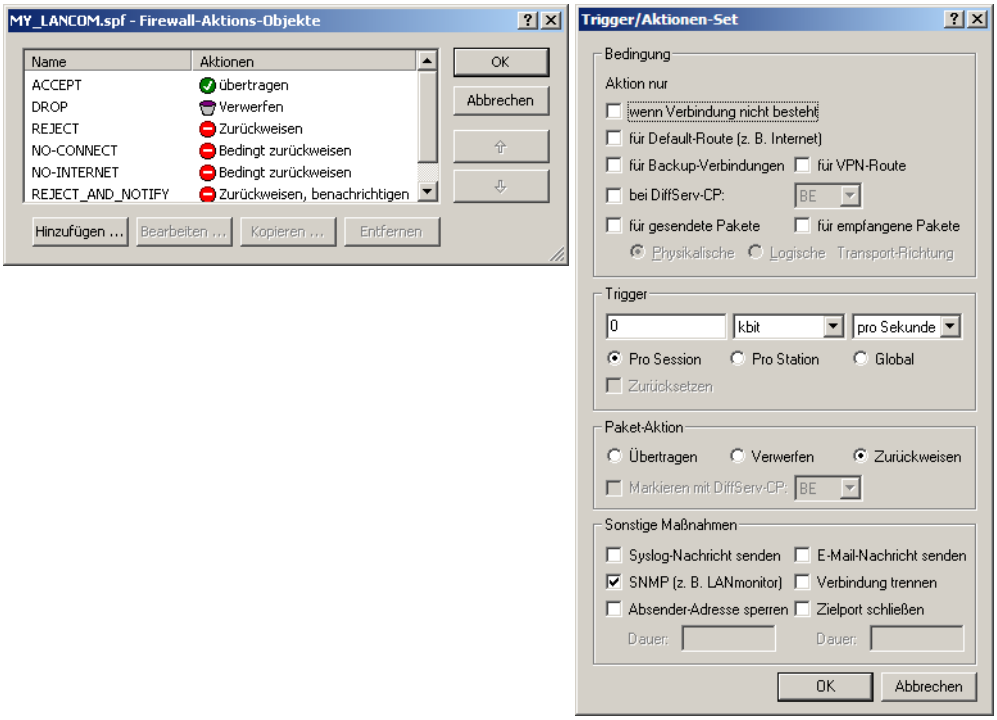
Bitte beachten Sie, dass sich eine Änderung der Firewall-Objekte auf alle Firewall-Regeln auswirkt, die dieses Objekt verwenden. Daher werden beim Ändern von Firewall-Objekten alle Firewall-Regeln angezeigt, die ebenfalls diese Objekte verwenden.

Existierende Firewalls (in der %-Schreibweise) werden beim Öffnen der Konfiguration mit LANconfig nicht automatisch auf die objektorientierte Form umgestellt. In der LANCOM KnowledgeBase finden Sie vorgefertigte Firewalleinstellungen, welche die neuen Objekte benutzen.



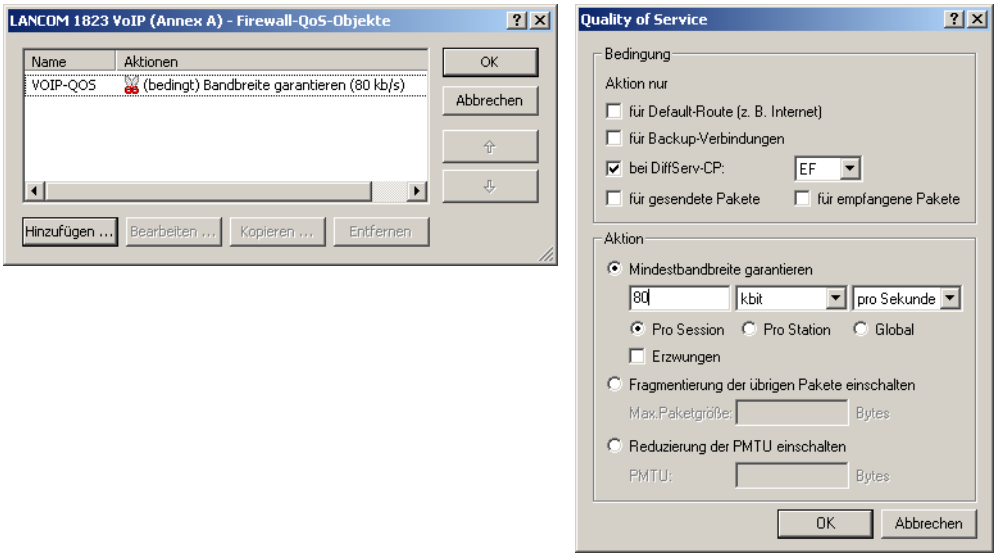
Aktions-Objekte

Hier legen Sie die Firewall-Aktion fest, bestehend aus Bedingung, Limit, Paket-Aktion und sonstigen Maßnahmen, die durch die Firewall-Regeln verwendet werden sollen.



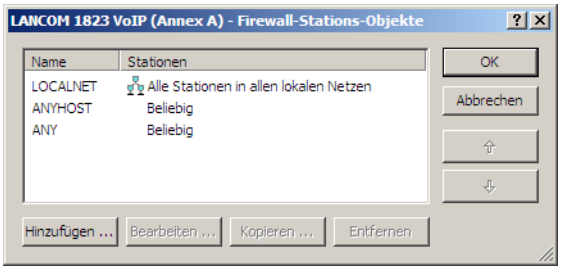
QoS-Objekte

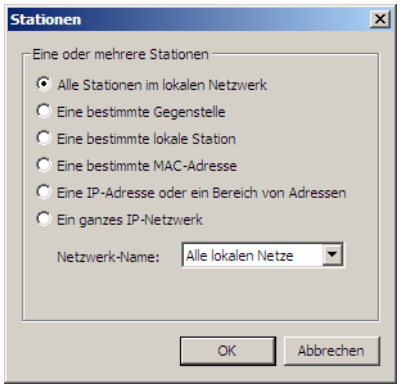
Hier können Sie die Mindestbandbreiten für die Datenpakete zur Verfügung stellen, die durch die Firewall-Regeln verwendet werden sollen.



Stations-Objekte

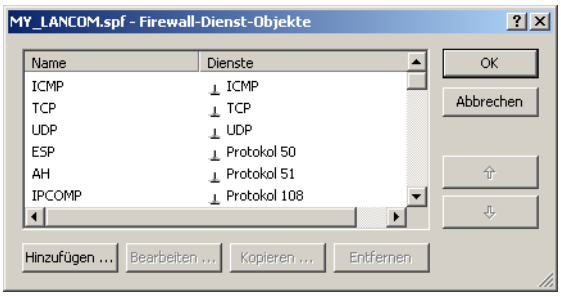
Hier werden die Stationen festgelegt, die als Absender oder Adressat der Pakete durch die Firewall-Regeln verwendet werden sollen. Die Stations-Objekte sind dabei nicht auf Quelle oder Ziel festgelegt, sondern können in den Firewall-Regeln je nach Bedarf verwendet werden.

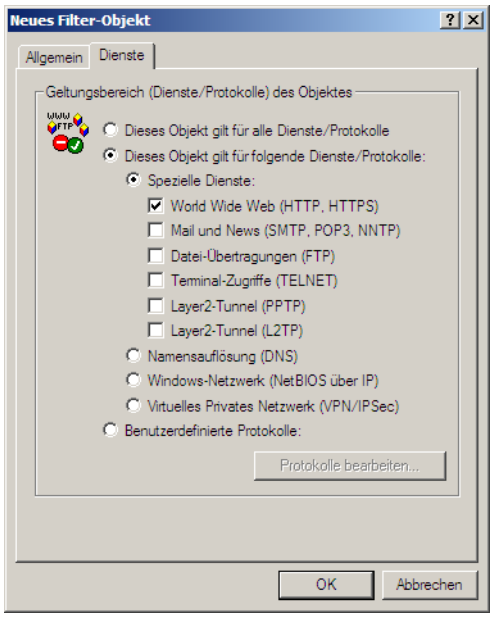




Dienst-Objekte

Hier werden die IP-Protokolle, Quell- und Zielports definiert, die durch die Firewall-Regeln verwendet werden sollen.

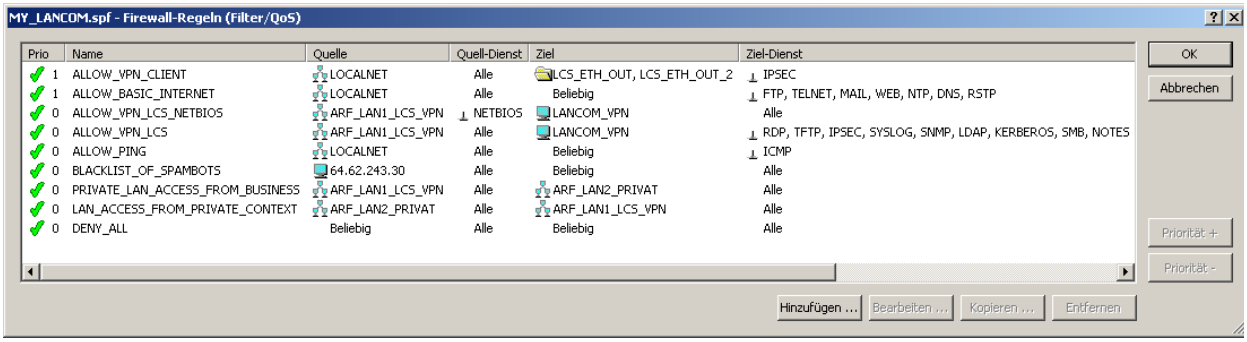




F.1.2 Definition der Firewall-Regeln

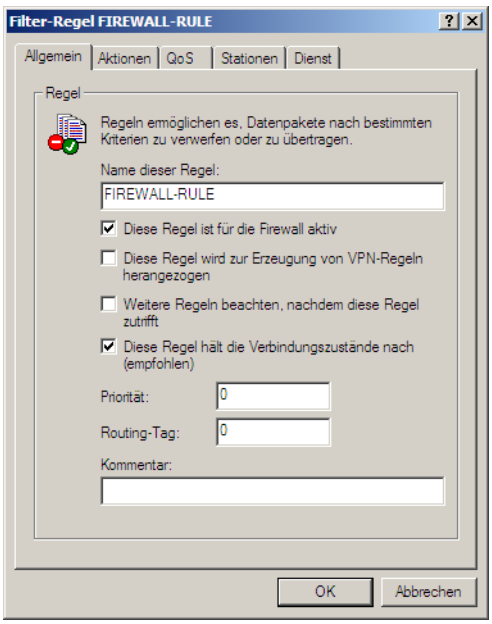
Die Firewall-Regeln werden in einer übersichtlichen Tabelle mit folgenden Informationen dargestellt:

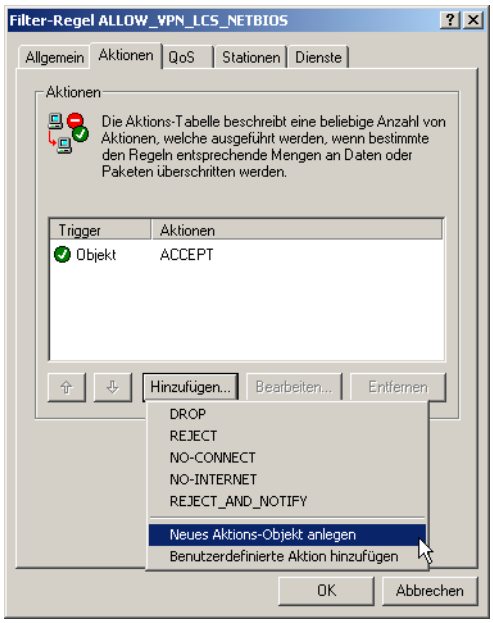
- In der Spalte äußerst links zeigen Symbole den Zustand der Firewall-Regel an:
  - Grünes Häkchen: Firewall-Regel ist aktiv.
  - Rotes Kreuzchen: Firewall-Regel ist nicht aktiv.
  - Schloss: Firewall-Regel wird zur manuellen Erzeugung von VPN-Regeln verwendet.
  - Zwei verkettete Pfeile: Wenn diese Firewall-Regel zutrifft, bitte weitere Regeln beachten.
- Name der Firewall-Regel
- Quelle
- Ziel
- Quell- und Ziel-Dienst
- Aktion/QoS
- Kommentar



Neue Firewall-Regel hinzufügen

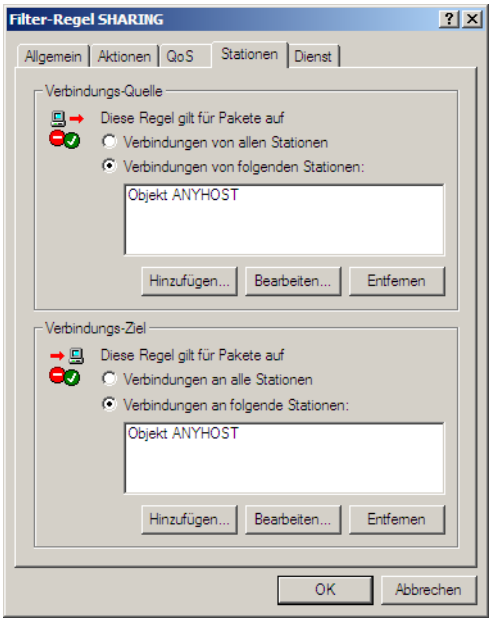
Beim Anlegen einer neuen Firewall-Regel werden zunächst die allgemeinen Daten erfasst. Auf den folgenden Registerkarten für Aktionen, QoS, Stationen oder Dienste werden die schon definierten Objekte zur direkten Verwendung angeboten. Alternativ können von dieser Stelle aus neue Objekte angelegt werden, die auch in anderen Regeln verwendet werden können oder benutzerdefinierte Einträge, die nur in der aktiven Firewall-Regel zum Einsatz kommen.

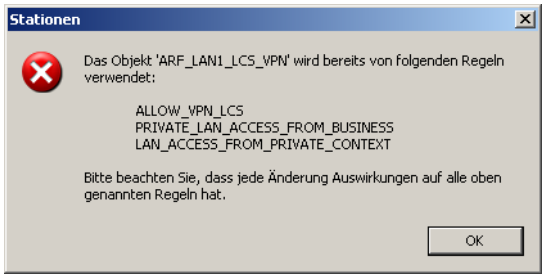




Firewall-Regel bearbeiten

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.





F.2 Konfiguration der Firewall-Regeln mit WEBconfig oder Telnet

Änderungen mit LCOS 7.6:

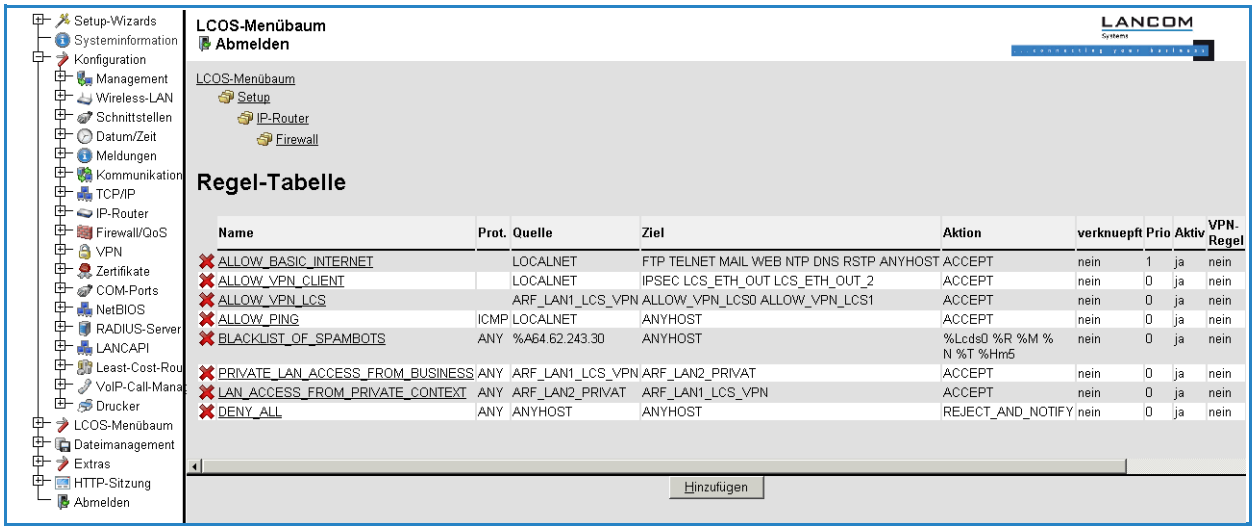
- Neue Bedingung @b für die Beschränkung der Firewall-Regel auf Backup-Verbindungen
- Neues Limit %u für die Beschränkung der Firewall-Regel auf die Verbindungen einer Station
- Neues Limit %i für die Vorgabe einer maximalen Anzahl von Verbindungen
- Neues Limit %b für die Vorgabe eines prozentualen Anteils der Bandbreite
- Objektorientierte Definition der Firewall-Regeln

F.2.1 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.

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.



Existierende Firewalls in der %-Schreibweise werden nicht automatisch auf die objektorientierte Form umgestellt. Allerdings stehen in der LANCOM KnowledgeBase vorgefertigte Firewalleinstellungen bereit, die die neuen Objekte verwenden.

Bei Geräten mit einer LCOS-Version 7.6 oder neuer sind automatisch die wichtigsten Objakte 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 im LCOS 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 LCOS-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

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 LCOS-Syntax enthalten (z.B. %P6 für TCP).

Bei der direkten Eingabe der Pegel-Parameter in der LCOS-Syntax gelten die gleichen Regeln, wie sie in den folgenden Abschnitten für Protokolle, Quelle und Ziel sowie die Firewall-Aktionen angegeben sind.

- **Name**

  Geben Sie hier einen eindeutigen Namen für diese Firewall-Regel an.

  □ Mögliche Werte: max. 32 Zeichen

- **Prot.**

  Angabe der Protokolle, für welche dieser Eintrag gelten soll (sofern in Quelle und Ziel neben den Ports/Diensten keine Protokolle definiert sind).

  □ Mögliche Werte: max. 10 Zeichen. Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben oder Verweise auf einen Eintrag der Objekttabelle.

- **Quelle**

  Angabe der Quell-Objekte (ein oder mehrere Netze, Stationen, Protokolle und Ports), für welche dieser Eintrag gelten soll.

  □ Mögliche Werte: max. 40 Zeichen. Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben oder Verweise auf einen Eintrag der Objekttabelle.

- **Ziel**

  Angabe der Ziel-Objekte (ein oder mehrere Netze, Stationen, Protokolle und Ports), für welche dieser Eintrag gelten soll.

  □ Mögliche Werte: max. 40 Zeichen. Direkte Eingabe nach der LCOS-Syntax wie in der Objekttabelle beschrieben oder Verweise auf einen Eintrag der Objekttabelle.

Werden in einem Quell- oder Zielobjekt Protokolle und Ports gemischt eingetragen, so gelten die jeweiligen Ports für alle in der Regel aufgeführten Protokolle!

Beispiel: Ziel = FTP, DNS mit den Objektdefinitionen FTP = TCP, Port 21 und NTP = UDP, Port 123. Die resultierende Regel schaltet die Ports 21 und 123 jeweils für UDP und TCP frei (UDP Port 21 und 123 sowie TCP Port 21 und 123).

Für TCP und UDP ist das in der Regel kein Problem, da die Well-Known-Ports i.d.R. auf TCP und UDP gleich definiert sind (vgl. www.iana.org/assignments/port-numbers).

Ist dieses Verhalten für eine detaillierte Kontrolle unerwünscht, so dürfen nur Objekte mit gleichem Protokoll in einer Regel verwendet werden, bzw. es ist pro Dienst/Protokollobjekt eine eigene Regel anzulegen.

- **Aktion**

  Aktion, die ausgeführt werden soll, wenn die Firewall-Regel auf ein Paket zutrifft.

  □ Mögliche Werte: max. 40 Zeichen. Direkte Eingabe nach der LCOS-Syntax wie in der Aktionstabelle beschrieben oder Verweise auf einen Eintrag der Aktionstabelle.

- **verknuepft**

  Verbindet die Regel mit weiteren Regeln.

  □ Mögliche Werte: Ja, Nein

- □ Default: Nein

■ **Prio**

Priorität der Regel.

- □ Mögliche Werte: 0 bis 255

■ **Aktiv**

Schaltet die Regel ein oder aus.

- □ Mögliche Werte: Ja, Nein
- □ Default: Ja

■ **VPN-Regel**

Aktiviert die Regel für das manuelle Erstellen von VPN-Regeln.

- □ Mögliche Werte: Ja, Nein
- □ Default: Nein

■ **Stateful**

Wenn diese Option aktiviert ist, wird geprüft, ob ein Verbindungaufbau korrekt abläuft. Fehlerhafte Pakete im Verbindungsaufbau werden verworfen. Ist diese Option nicht aktiviert, dann werden alle Pakete akzeptiert, auf die diese Regel zutrifft (einfache Paketfilter-Firewall).

Durch das Nachhalten des Verbindungsstatus, bei dem jedes Paket einer bestimmten Session zugeordnet wird, ergibt sich effektiv eine Richtungsabhängigkeit der Filter, so dass nur der Datenverkehr der aufbauenden Session von der angegebenen Quelle zum Ziel möglich ist. Ports für die Antwortpakete einer definierten Session werden dabei dynamisch geöffnet.

Desweiteren wird über diese Option die automatische Protokollerkennung für FTP, IRC und PPTP aktiviert, die benötigt wird, um für die jeweiligen Datenverbindungen einen Port in der Firewall öffnen zu können.

Auch die Prüfung auf Portscans/SYN-Floodings wird über diese Option aktiviert oder deaktiviert. Damit können bestimmte, stark frequentierte Server von der Prüfung ausgenommen werden, ohne die Limits für halboffene Verbindungen (DOS) oder Portanfragen (IDS) so hoch einzustellen, dass sie letztendlich unwirksam werden.

- □ Mögliche Werte: Ja, Nein
- □ Default: Ja

■ **Rtg-Tag**

Routing-Tag für die Regel.

Mögliche Werte:

- □ 0 bis 65535

Default:

- □ 0

■ **Kommentar**

Kommentar für diesen Eintrag.

- □ Mögliche Werte: max. 64 Zeichen

F.2.2 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.

■ **Name**

Geben Sie hier einen eindeutigen Namen für dieses Objekt an.

- □ Mögliche Werte: max. 32 Zeichen

■ **Beschreibung**

In der Objekttabelle können die Stationen und Dienste beschrieben werden.

Mögliche Werte:

- □ %L: lokales Netz
- □ %H: Gegenstellen – Name muss in DSL-/ISDN-/PPTP- oder VPN-Gegenstellenliste stehen
- □ %D: Hostname – Hinweis zu Hostnamen beachten
- □ %E: MAC-Adresse – 00:A0:57:01:02:03
- □ %A: IP-Adresse – %A10.0.0.1, 10.0.0.2; %A0 (alle Adressen)
- □ %M: Netzmaske – %M255.255.255.0
- □ %P: Protokoll (TCP/UDP/ICMP etc.) – %P6 (für TCP)
- □ %S: Dienst (Port) – %S20-25 (für Ports 20 bis 25)

Besondere Werte:

- □ Gleichartige Beschreibungen können durch Komma getrennte Listen, wie z.B. Host-Listen/Adresslisten (%A10.0.0.1, 10.0.0.2) oder durch Bindestrich getrennte Bereiche wie z.B. Portlisten (%S20-25) erzeugen.
- □ Die Angabe einer '0' oder eines Leerstrings bezeichnet das Any-Objekt.

Bei der Konfiguration über die Konsole (Telnet oder Terminalprogramm) müssen die kombinierten Parameter (Port, Ziel, Quelle) jeweils in Anführungszeichen (Zollzeichen: ") eingeschlossen werden.

Hostnamen können nur dann verwendet werden, wenn das LANCOM die Namen in IP-Adressen auflösen kann. Dafür muss das LANCOM 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.

F.2.3 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.

■ **Name**

Geben Sie hier einen eindeutigen Namen für diese Aktion an.

- □ Mögliche Werte: max. 32 Zeichen

■ **Beschreibung**

In der Aktionstabelle werden die Firewall-Aktionen als beliebige Kombinationen aus Bedingungen, Limits, Paket-Aktionen und weiteren Maßnahmen zusammengestellt.

Bedingungen

Mit den Bedingungen schränkt man die Wirksamkeit einer Firewall-Regel ein.

Mögliche Werte für die Bedingungen:

- □ @c: Connect-Filter – Der Filter ist aktiv, wenn keine physikalische Verbindung zum Ziel des Pakets besteht.
- □ @d (plus DSCP): DiffServ-Filter – Der Filter ist aktiv, wenn das Paket den angegebenen Differentiated Services Code Point (DSCP) enthält.
- □ @i: Internet-Filter – Der Filter ist aktiv, wenn das Paket über die Defaultroute empfangen wurde oder gesendet werden soll.
- □ @v: VPN-Filter – Der Filter ist aktiv, wenn das Paket über eine VPN-Verbindung empfangen wurde oder gesendet werden soll.
- □ @b: Backup-Filter – Der Filter ist aktiv, wenn sich entweder die direkte Gegenstelle im Backup-Zustand befindet oder wenn in einem Protokollstapel (z.B. VPN über PPTP über DSL) eines der gestapelten Protokolle über eine Backupverbindung aufgebaut wurde. Wenn sich z. B. die Internetverbindung im Backup-Zustand befindet, dann gilt für die Firewall auch eine darüber aufgebaute VPN-Verbindung als Backupverbindung.

Besondere Werte für die Bedingungen:

- □ Wenn zum "Connect-" oder "Internet-" Filter keine weitere Aktion angegeben wird, dann wird implizit eine Kombination dieser Filter mit der "Reject" Aktion angenommen.

Limits

Das Limit (oder auch Trigger) bezeichnet einen quantifizierten Grenzwert, der auf der definierten Verbindung überschritten werden muss, bevor der Filter ein Datenpaket erfasst. Ein Limit setzt sich zusammen aus den Werten für die Einheit (kBit, kByte, Pakete, Anzahl Sessions oder % der Bandbreite), dem Betrag (Datenrate oder Anzahl) sowie der Bezugsgröße (pro Sekunde, pro Minute, pro Stunde oder absolut) und ggf. weiteren Parametern (z.B. Zeitraum und Größe).

Zusätzlich kann für das Limit vereinbart werden, ob es sich auf eine logische Session bzw. eine Station 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 Grenzwert durchbricht.

Bei absoluten Werten kann außerdem definiert werden, dass der zugehörige Zähler beim Überschreiten des Limits zurückgesetzt wird.

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.

Mögliche Werte für die Limits:

- %c: Connection – Das Limit bezieht sich auf die einzelne Verbindung.
- %u: User – Das Limit bezieht sich auf alle Verbindungen des Users (der Station, identifiziert über die IP-Adresse).
- %g: Global – Das Limit bezieht sich auf alle Verbindungen gemeinsam, die zu den für diese Firewall-Regel definierten Quellen und Zielen sowie Protokollen und Diensten passen.
- %d: Data – Anzahl von Kilobytes, nach denen die Aktion ausgeführt wird.
- %p: Packet – Anzahl von Paketen, nach denen die Aktion ausgeführt wird.
- %i: Interconnection – Anzahl von Verbindungen (Sessions), nach denen die Aktion ausgeführt wird.
- %b: Based – Prozentualer Anteil der Bandbreite, nach der die Aktion ausgeführt wird.
- %s, %m, %h: Second, Minute, Hour – Zeitraum in Sekunde, Minute, Stunde, nach denen die Aktion ausgeführt wird.
- %r: receive Option – Beschränkung des Limits auf die Empfangsrichtung.
- %t: transmit Option – Beschränkung des Limits auf die Senderichtung.
- Betrag – Anzahl der Daten, Pakete, Verbindungen bzw. prozentualer Anteil der Bandbreite, nach denen die Aktion ausgeführt wird.

Limit-Objekte werden dabei allgemein mit %L eingeleitet, gefolgt von einer Kombination der möglichen Limit-Parameter.

Besondere Werte für die Limits:

- Das Limit %i für die Anzahl der Verbindung macht nur Sinn bei User-bezogenen (%u) oder globalen Regeln (%g).

Wird eine Firewall-Regel ohne Limit angegeben, so wird implizit ein Paket-Limit angenommen, welches sofort beim ersten Paket überschritten wird.

Paket-Aktionen

Die Paket-Aktionen sind beliebig miteinander kombinierbar, wobei bei widersinnigen oder nicht eindeutigen Aktionen (z.B.: Accept + Drop) die sicherere, d.h. im Beispiel "Drop" genommen wird.

Mögliche Werte für die Paket-Aktionen:

- %a: Accept – Das Paket wird angenommen.
- %r: Reject – Das Paket wird mit einer passenden Fehlermeldung zurückgewiesen.
- %d: Drop – Das Paket wird stillschweigend verworfen.

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 Aufgaben "Protokollierung/Benachrichtigung" und "Verhindern weiterer Angriffe":

Mögliche Werte für sonstige Maßnahmen:

- %s: Syslog – Gibt eine detaillierte Meldung über Syslog aus.
- %m: Mail – Schickt eine E-Mail an den Administrator.
- %n: SNMP – Sendet einen SNMP-Trap.

- %p: Close-Port – Schließt den Zielport des Pakets für eine einstellbare Zeit.
- %h: Deny-Host – Sperrt die Absender-Adresse des Pakets für eine einstellbare Zeit.
- %t: Disconnect – Trennt die physikalische Verbindung zur Gegenstelle, über die das Paket empfangen wurde oder gesendet werden sollte.
- %z: Zero-Limit – Setzt den Limit-Counter bei überschreiten der Trigger-Schwelle wieder auf 0.
- %f: Fragmentierung – Erzwingt die Fragmentierung aller nicht auf die Regel passenden Pakete.

Besondere Werte für sonstige Maßnahmen:

- Wenn die "Close-Port"-Aktion ausgeführt wird, wird ein Eintrag in einer Sperrliste vorgenommen, durch den alle Pakete, die an den jeweiligen Rechner und Port gesendet werden, verworfen werden. Für das "Close-Port"-Objekt kann eine Sperrzeit in Sekunden, Minuten oder Stunden angegeben werden, die direkt hinter der Objekt-ID vermerkt wird. Diese Zeitangabe baut sich zusammen aus dem Bezeichner für die Zeiteinheit (h, m, s für Stunde, Minute und Sekunde) sowie der eigentlichen Zeitangabe. So sperrt z.B. %pm10 den Port für 10 Minuten. Wird keine Zeiteinheit angegeben, so wird "Minuten" als Einheit angenommen. (damit ist %p10 gleichbedeutend mit %pm10)
- Wird die "Deny-Host"-Aktion ausgeführt, so wird der Absender des Pakets in eine Sperrliste eingetragen. Ab diesem Moment werden alle Pakete, die von dem gesperrten Rechner empfangen werden verworfen. Auch das "Deny-Host"-Objekt kann mit einer Sperrzeit versehen werden, die wie bei der "Close-Port" Option beschrieben gebildet wird.

G Voice over IP

G.1 Konfiguration der VoIP-Parameter

Änderungen mit LCOS 7.6:

- Angabe des folgenden Parameters für SIP-, ISDN- und Analog-User:
  - CLIR
- Angabe der folgenden Parameter für SIP-Provider- und SIP-PBX-Lines:
  - Lokale-Portnummer
  - (Re-)Registrierung
  - Leitungsüberwachung
  - Überwachungsintervall
  - Vertrauenswürdig
  - Privacy-Methode
- Angabe der folgenden Parameter für Analog-Lines:
  - Caller-ID Signaling
  - Caller-ID Transmission Requirements

G.1.1 Konfiguration der Benutzer

Lokale Benutzer sind die am LANCOM VoIP Router angeschlossenen Endgeräte/Telefone. Es wird unterschieden zwischen:

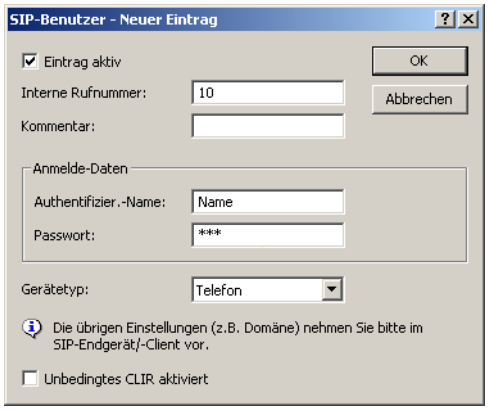
- SIP-Benutzer: Benutzer, die über ein SIP-Telefon an das LAN angeschlossen sind. Dabei ist es für die Konfiguration des Benutzers egal, ob das LAN direkt am LANCOM angeschlossen ist, oder über ein VPN (über das Internet) angeschlossen ist.
- ISDN-Benutzer: Benutzer, die über ISDN angeschlossen sind. Sie verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.
- Analog-Benutzer: Benutzer, die an die analogen Schnittstellen angeschlossen sind. Sie verwenden das SIP-Gateway, um über die VoIP-Funktion zu telefonieren.

SIP-Benutzer

Je nach Modell können unterschiedlich viele SIP-Benutzer angelegt werden. Mehr als die erlaubte Anzahl Benutzer können nicht angelegt werden, ebenso werden gleiche Namen oder gleiche Rufnummern nicht zugelassen.

Die vom SIP-Teilnehmer verwendete Domäne wird üblicherweise im Endgerät selbst eingestellt.

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ SIP-Benutzer



WEBconfig: Setup ▶ Voice-Call-Manager ▶ User ▶ SIP-User

Zur Definition eines SIP-Benutzers können die folgenden Parameter eingetragen werden:

- **Number/Name**

  Telefonnummer des SIP-Telefons oder Name des Benutzers (SIP-URI).

  Mögliche Werte:

□ Maximal 16 alphanumerische Zeichen.

Default:

□ Leer

■ **Auth-Name**

Name zur Authentifizierung am SIP-Proxy, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Der Name wird benötigt, wenn eine Anmeldung erforderlich ist (z.B. bei übergeordneter Anmeldung an einer SIP-TK-Anlage oder Setzen von "Lokale Authentifizierung erzwingen" für die SIP-Benutzer).

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Secret**

Passwort zum Anmelden des SIP-Benutzers, ggf. auch an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich Benutzer lokal am SIP-Proxy ohne Authentifizierung anmelden ("Lokale Authentifizierung erzwingen" für SIP-Benutzer ist deaktiviert) und ggf. an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen.

Default:

□ Leer

■ **Device-Type**

Typ des angeschlossenen Geräts.

Mögliche Werte:

□ Telefon

□ Fax

□ Telefon/Fax

Default:

□ Telefon

■ **CLIR**

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

Mögliche Werte:

□ Ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.

□ Nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

Default:

□ Nein

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag

Mögliche Werte:

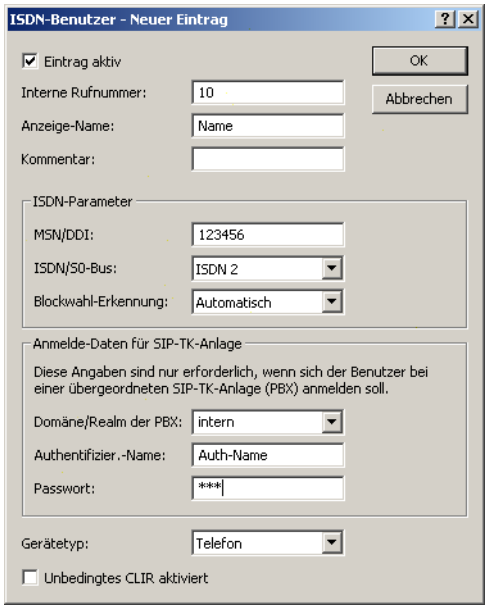
□ Maximal 64 alphanumerische Zeichen.

Default:

□ Leer

ISDN- Benutzer

LANconfig: VoIP- Call- Manager ▶ Benutzer ▶ ISDN- Benutzer



WEBconfig: Setup ▶ Voice- Call- Manager ▶ User ▶ ISDN- User

■ **Number/Name**

Interne Rufnummer des ISDN-Telefons oder Name des Benutzers (SIP- URI).

Mögliche Werte:

□ Maximal 16 alphanumerische Zeichen.

Default:

□ Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern an einem Anlagenanschluss in einem einzigen Eintrag erfaßt werden. Mit der Rufnummer '#' und der DDI '#' werden z.B. die Durchwahlnummern ohne Veränderung in interne Rufnummern umgesetzt. Mit der Rufnummer '3#' und der DDI '#' wird z.B. ein ankommender Ruf für die Durchwahl '55' an die interne Rufnummer '355' weitergeleitet, bei ausgehenden Rufen von der internen Rufnummer '377' wird die '77' als Durchwahl verwendet.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN- Benutzer notwendig.

■ **Ifc**

ISDN- Interface, das für den Verbindungsaufbau verwendet werden soll.

Mögliche Werte:

□ Ein oder mehrere der im Gerät verfügbaren S0- Busse

Default:

□ Leer

■ **MSN/DDI**

Interne MSN, die für diesen Benutzer auf dem internen ISDN- Bus verwendet wird.

□ MSN: Nummer des Telefonanschlusses, wenn es sich um einen Mehrgeräteanschluss handelt.

□ DDI (Direct Dialing in): Durchwahlnummer des Telefons, wenn der Anschluss als Anlagenanschluss konfiguriert ist.

Mögliche Werte:

□ Maximal 19 Zeichen (Ziffern und #-Zeichen).

Default:

□ Leer

Mit dem #-Zeichen als Platzhalter können ganze Gruppen von Rufnummern z.B. bei der Verwendung von Durchwahlnummern in einem einzigen Eintrag erfaßt werden.

Benutzereinträge mit #-Zeichen zur Abbildung von Benutzergruppen können nicht für eine Anmeldung an einer übergeordneten TK-Anlage verwendet werden. Für diese Anmeldung ist immer ein spezifischer Eintrag für den einzelnen ISDN-Benutzer notwendig.

■ **Auth-Name**

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen.

Default:

□ Leer

■ **Display-Name**

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Secret**

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des ISDN-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Domain**

Domäne einer übergeordneten SIP-TK-Anlage, wenn der ISDN-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

Mögliche Werte:

□ Maximal 63 alphanumerische Zeichen

Default:

□ Leer

■ **Device-Type**

Typ des angeschlossenen Gerätes.

Mögliche Werte:

□ Telefon

□ Fax

□ Telefon/Fax

Default:

□ Telefon

■ **DialCompl**

Blockwahlerkennung.

Mögliche Werte:

□ Auto: Blockwahl wird automatisch erkannt (z.B. bei Zielwahl oder Wahlwiederholung), und der Ruf damit schneller aufgebaut. Eine Nachwahl ist nicht möglich.

□ Manual: Keine Blockwahl, mit Eingabe des "#" kann die Nummer als vollständig gekennzeichnet werden und somit der Rufaufbau initiiert werden.

Default:

- □ Auto

■ **CLIR**

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

Mögliche Werte:

- □ Ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.
- □ Nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

Default:

- □ Nein

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

- □ Ja, Nein

Default:

- □ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag.

Mögliche Werte:

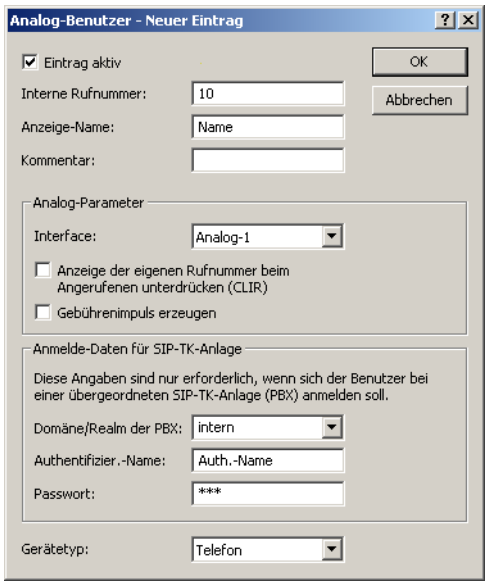
- □ Maximal 64 alphanumerische Zeichen

Default:

- □ Leer

Analog-Benutzer

LANconfig: VoIP-Call-Manager ▶ Benutzer ▶ Analog-Benutzer



WEBconfig: Setup ▶ Voice-Call-Manager ▶ User ▶ Analog-User

■ **Number/Name**

Interne Rufnummer des Analog-Telefons oder Name des Benutzers (SIP-URI).

Mögliche Werte:

- □ Maximal 16 alphanumerische Zeichen

Default:

- □ Leer

■ **Auth-Name**

Name zur Authentifizierung an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Display-Name**

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Secret**

Passwort zum Anmelden als SIP-Benutzer an einer übergeordneten SIP-TK-Anlage, wenn die Domäne des Analog-Benutzers mit der Domäne einer SIP-PBX-Line übereinstimmt. Es ist möglich, dass sich ISDN-Benutzer an einer übergeordneten SIP-TK-Anlage mit einem gemeinsamen Passwort ("Standard-Passwort" an der SIP-PBX-Line) anmelden.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Ifc**

Analoges-Interface, das für den Verbindungsaufbau verwendet werden soll.

Mögliche Werte:

□ Eine der im Gerät verfügbaren analogen Schnittstellen.

Default:

□ Analog-1

■ **CLIR**

Schaltet die Übermittlung der Absenderinformationen ein oder aus.

Mögliche Werte:

□ Ja: Die Übermittlung der Absenderinformationen wird auf jeden Fall unterdrückt, unabhängig von den Einstellungen am Endgerät des Benutzers.

□ Nein: Die Übermittlung der Absenderinformationen wird nicht im Gerät unterdrückt, die Einstellungen am Endgerät des Benutzers entscheiden über Übermittlung der Absenderinformationen.

Default:

□ Nein

■ **Gebührenimpuls**

Mit dem Gebührenimpuls (GBI) werden in analogen Telefonnetzen Informationen über die während einer Verbindung anfallenden Kosten zum Anrufer übermittelt. In dessen Endgerät (Telefon mit Gebührenanzeige, Gebührenanzeiger) wird der Gebührenimpuls aus dem übertragenen Gesamtsignal heraus gefiltert und in eine entsprechende Gebührenanzeige umgewandelt.

Mit dieser Option wird die Übertragung des Gebührenimpulses an den analogen Benutzer/das Endgerät ermöglicht. Dabei kann eine Gebühreninformation beispielsweise aus dem ISDN-Telefonnetz an eine ISDN-Leitung übermittelt und in einen analogen Gebührenimpuls umgesetzt werden.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Domain**

Domäne einer übergeordneten SIP-TK-Anlage, wenn der Analog-Benutzer als SIP-Benutzer angemeldet werden soll. Die Domäne muss bei einer SIP-PBX-Line konfiguriert sein, damit eine übergeordnete Anmeldung erfolgt.

Mögliche Werte:

□ Maximal 63 alphanumerische Zeichen

Default:

□ Leer

■ **Device-Type**

Typ des angeschlossenen Geräts.

Mögliche Werte:

□ Telefon

□ Fax

□ Telefon/Fax

Default:

□ Telefon

Der Typ entscheidet, ob ggf. eine Umwandlung einer analogen Fax-Verbindung in SIP T.38 erfolgt. Bei Auswahl des Typs "Fax" oder "Telefon/Fax" wird eine Erkennung von Fax-Signalen aktiviert, die u.U. bei einem Telefon zu Beeinträchtigungen der Verbindungsqualität führen kann. Bitte wählen Sie daher den Typ entsprechend des angeschlossenen Gerätes, um die optimale Qualität zu erzielen.

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen.

Default:

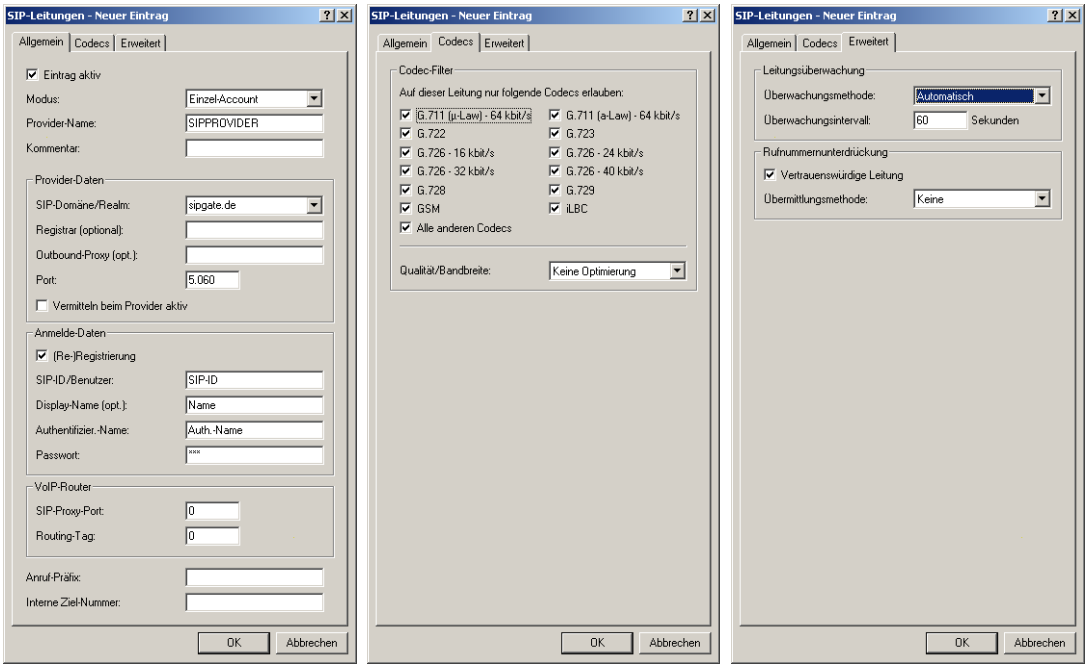
□ Leer

G.1.2 Konfiguration der Leitungen

SIP-Provider-Line

Über diese Leitungen meldet das Gerät sich bei anderen SIP-Gegenstellen (in der Regel SIP-Provider oder als Remote Gateway bei SIP-TK-Anlagen) an. Die Verbindung erfolgt entweder über das Internet oder einen VPN-Tunnel. Es können bis zu 16 SIP-Leitungen eingetragen werden.

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ SIP-Leitungen



WEBconfig: Setup ▶ Voice-Call-Manager ▶ Line ▶ SIP-Provider

■ **Name**

Der Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

Mögliche Werte:

□ Maximal 16 alphanumerische Zeichen

Default:

□ Leer

■ **Mode**

Mit dieser Auswahl bestimmen Sie die Betriebsart der SIP-Leitung.

Mögliche Werte:

□ Einzel-Account-Modus: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer. Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer ersetzt (maskiert). Eingehende Rufe werden der konfigurierten internen Ziel-Nummer zugestellt. Die maximale Anzahl von gleichzeitigen Verbindungen wird entweder vom Provider vorgegeben oder von der vorhandenen Bandbreite und den verwendeten Codecs bestimmt.

Tabelle für die Rufnummernumsetzung:

Einzel-Account	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Beim Provider registrierte Nummer (User-ID)
Eingehender Ruf	"To:"	User-ID

□ Trunk-Modus: Verhält sich nach außen wie ein erweiterter SIP-Account mit einer Stamm- und mehreren Durchwahlnummern. Die SIP-ID wird als Stammnummer beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen fungiert die Stammnummer als Präfix, das jeder rufenden Nummer (Absender; SIP: "From:") vorangestellt wird. Bei eingehenden Rufen wird das Präfix aus der Ziel-Nummer entfernt (SIP: "To:"). Die verbleibende Nummer wird als interne Durchwahl verwendet. Im Fehlerfall (Präfix nicht auffindbar, Ziel gleich

Präfix) wird der Ruf an die konfigurierte interne Ziel-Nummer geleitet. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

Trunk	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Stammnummer (User-ID) + "From:"
Eingehender Ruf	Stammnummer (User-ID) + "To:"	"To:" als interne Durchwahl

□ Gateway-Modus: Sie verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer, der SIP-ID. Die Nummer (SIP-ID) wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender) durch die registrierte Nummer (SIP-ID in SIP: "From:") ersetzt (maskiert) und in einem separaten Feld (SIP: "Contact:") übertragen. Bei eingehenden Rufen wird die gerufene Nummer (Ziel) nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

Gateway	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	Beim Provider registrierte Nummer (User-ID)
	"From:"	"Contact:"
Eingehender Ruf	"To:"	"To:"

□ Link-Modus: Verhält sich nach außen wie ein üblicher SIP-Account mit einer einzigen öffentlichen Nummer (SIP-ID). Die Nummer wird beim Serviceprovider registriert und die Registrierung regelmäßig aufgefrischt (wenn eine (Re-)Registrierung für diese SIP-Provider-Line aktiviert ist). Bei ausgehenden Rufen wird die Nummer des Rufenden (Absender; SIP: "From:") nicht modifiziert. Bei eingehenden Rufen wird die gerufene Nummer (Ziel; SIP: "To:") nicht modifiziert. Die maximale Anzahl der Verbindungen zu einem bestimmten Zeitpunkt ist nur durch die zur Verfügung stehende Bandbreite begrenzt.

Tabelle für die Rufnummernumsetzung:

Link	An der Leitung anliegende SIP-Nummer	Von der Leitung abgesetzte SIP-Nummer
Ausgehender Ruf	"From:"	"From:"
Eingehender Ruf	"To:"	"To:"

Default:

□ Einzel-Account

■ **Domain**

SIP-Domäne/Realm der übergeordneten Gegenstelle. Sofern die Gegenstelle DNS-Service Records für SIP unterstützt, genügt diese Angabe, um Proxy, Outbound-Proxy, Port, Registrar automatisch zu ermitteln - das ist bei typischen SIP-Provider-Angeboten i.d.R. der Fall.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Rtg-Tag**

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu diesem SIP-Provider.

Mögliche Werte:

□ Maximal 64 Ziffern

Default:

□ 0

■ **Port**

TCP/UDP-Port beim SIP-Provider, an den die SIP-Pakete gesendet werden.

Mögliche Werte:

□ Beliebieger freier TCP/IP-Port

Default:

□ 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

■ **User-id**

Telefonnummer des SIP-Accounts oder Name des Benutzers (SIP-URI).

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Bei einem SIP-Trunking-Account wird hier die Stammnummer eingetragen. Bei ankommenden Rufen werden alle über diese Stammnummer hinausgehenden Zeichen als Durchwahl (DDI) erkannt und nur diese an den Call Router übergeben. Bei abgehenden Rufen wird die vom Call Router empfangene DDI um die Stammnummer ergänzt.
Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Auth-Name**

Name zur Authentifizierung an der übergeordneten SIP-Gegenstelle (Provider/SIP-TK-Anlage).

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Display-Name**

Name, der auf dem angerufenen Telefondisplay erscheinen soll.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Dieser Wert sollte im Normalfall nicht gesetzt werden, da bei eingehenden Rufen der SIP-Provider den Display-Namen setzt und bei ausgehenden Rufen der lokale Client bzw. die Rufquelle (ggf. überschrieben mit den Einstellungen zum Display-Namen des jeweiligen Benutzers). Oftmals werden hier zusätzliche Informationen übermittelt (z.B. Originalrufnummer bei einer Umleitung etc.), die für den Angerufenen hilfreich sein können.
Im Fall von SIP-Einzel-Accounts verlangen manche Provider allerdings auch den in den Anmeldedaten vorgegebenen Display-Namen bzw. einen zur SIP-ID identischen Eintrag (z.B. T-Online).
Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Secret**

Das Passwort zur Authentifizierung beim SIP-Registrar und SIP-Proxy des Providers. Bei Leitungen ohne (Re-)Registrierung kann das Passwort unter Umständen entfallen.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Mit den Zugangsdaten wird die Leitung (Einzel-Account, Trunk, Link, Gateway) angemeldet, nicht jedoch einzelne lokale Benutzer mit ihren individuellen Anmeldedaten. Wenn einzelne Benutzer (SIP, ISDN, Analog) mit den dort bzw. auf dem Endgerät hinterlegten Daten bei einer übergeordneten Instanz registriert werden sollen, muss der Leitungstyp SIP-PBX-Leitung gewählt werden.

■ **Registrar**

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account beim SIP-Provider entgegen nimmt.

Mögliche Werte:

□ Maximal 63 alphanumerische Zeichen

Default:

□ Leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Registrar wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

■ **Outb-proxy**

Der Outbound-Proxy des SIP-Providers nimmt alle vom LANCOM ausgehenden SIP-Signalisierungen einer Verbindung zu diesem Provider für die Dauer der Verbindung entgegen.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Dieses Feld kann frei bleiben, sofern der SIP-Provider keine speziellen Angaben macht. Der Outbound-Proxy wird dann über DNS-SRV-Anfragen zur konfigurierten SIP-Domäne/Realm ermittelt (bei SIP-Services im Firmennetz/VPN ist dies oftmals nicht der Fall, d.h. der Wert muss explizit gesetzt werden).

■ **Cln-Prefix**

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:") aller ankommenden Anrufe auf dieser SIP-Provider-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

Mögliche Werte:

□ Maximal 9 Ziffern

Default:

□ Leer

■ **Number/Name**

Die Wirkung dieses Feldes hängt von der Einstellung des Modus der Leitung ab:

□ Wenn der Modus der Leitung „Einzel-Account" ist, werden alle über die Leitung eingehenden Rufe mit dieser Nummer als Ruf-Ziel (SIP: „To:") an den Call-Router übergeben.

□ Wenn der Modus „Trunk" ist, wird die Ziel-Nummer durch Entfernen der für den Trunk definierten Stammnummer ermittelt – falls dabei ein Fehler auftritt, wird der Ruf mit der in diesem Feld eingetragenen Nummer versehen (SIP: „To:") an den Call-Router übergeben.

□ Wenn der Modus auf „Gateway" oder „Link" eingestellt ist, hat der Eintrag in diesem Feld keine Wirkung.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Codecs**

Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendet werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

Mögliche Werte:

□ Auswahl aus der Liste der verfügbaren Codecs.

Default:

□ Alle

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

■ **Codec-Order**

Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

Mögliche Werte:

□ Keine Optimierung: Läßt die Reihenfolge der Codecs unverändert.

□ Beste Qualität: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst hohe Sprachqualität erreicht wird.

□ Minimale Bandbreite: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst geringe Bandbreite benötigt wird.

Default:

□ Keine Optimierung

■ **Refer-weiterleiten**

Bei der Rufvermittlung (Verbindung) von zwei entfernten Gesprächsteilnehmern kann die Vermittlung im Gerät selbst gehalten (Media-Proxy) oder an die Vermittlungsstelle beim Provider übergeben werden, wenn beide zu vebindende Gesprächsteilnehmer über diese SIP-Provider-Leitung erreicht werden (andernfalls übernimmt der Media-Proxy im LANCOM die Vermittlung der Medienströme, z.B. beim Verbinden zwischen zwei SIP-Provider-Leitungen).

Mögliche Werte:

□ Ja: Vermittlung wird an den Provider weitergeleitet.

□ Nein: Die Verbindungen werden im Gerät selbst gehalten.

Default:

□ Nein

Eine Übersicht über die wichtigsten SIP-Provider, die diese Funktion unterstützen, finden Sie im Support-Bereich auf der Internet-Seite.

■ **Lokale-Portnummer**

Dies ist der Port des LANCOM-Proxies zur Kommunikation mit dem Provider.

Mögliche Werte:

□ 1 bis 65536

Default:

□ 0

Besondere Werte:

□ 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch auf der Providerseite eingetragen werden (z.B. bei Nutzung eines regsitrierungslosen Trunks im Firmen-VPN), damit sich beide Seiten SIP-Signalisierungen senden können.

■ **(Re-)Registrierung**

Hiermit wird die (wiederholte) Registrierung der SIP-Provider-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar des Providers ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

■ **Leitungsüberwachung**

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-Provider-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

Mögliche Werte:

□ Auto: Die Methode wird automatisch ermittelt.

□ Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.

□ Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.

□ Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Default:

□ Auto

■ **Überwachungsintervall**

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

Mögliche Werte:

□ Max. 5 Ziffern.

Default:

□ 60

Besondere Werte:

□ Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

■ **Vertrauenswürdig**

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

Mögliche Werte:

□ Ja: Vertrauenswürdig

□ Nein: Nicht vertrauenswürdig

Default:

□ Ja

Bitte beachten sie, dass diese Funktion nicht von allen Providern unterstützt wird.

■ **Privacy-Methode**

Spezifiziert die verwendete Methode zur Übermittlung der Caller ID im separaten SIP-Header-Feld.

Mögliche Werte:

□ Keine

□ RFC3325: mittels P-Preferred-Id/P-Asserted-Id

□ IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

Default:

□ Keine

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

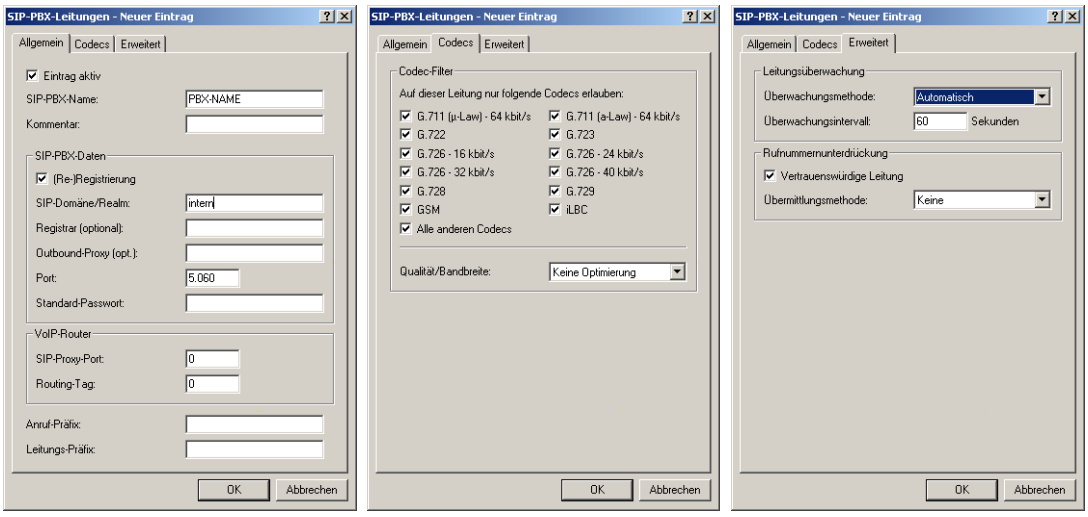
Default:

□ Leer

SIP-PBX-Line

Über diese Leitungen werden Verbindungen zu übergeordneten SIP-TK-Anlagen konfiguriert, die in der Regel über VPN angebunden sind.

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ SIP-PBX-Leitungen



WEBconfig: Setup ▶ Voice-Call-Manager ▶ Line ▶ SIP-PBX

■ **Name**

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

Mögliche Werte:

□ Maximal 16 alphanumerische Zeichen

Default:

□ Leer

■ **Domain**

SIP-Domäne/Realm der übergeordneten SIP-TK-Anlage.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Rtg-Tag**

Routing-Tag zur Auswahl einer bestimmten Route über die Routing-Tabelle für Verbindungen zu dieser SIP-TK-Anlage.

Mögliche Werte:

□ Maximal 64 Ziffern

Default:

□ 0

■ **Port**

TCP/UDP-Port der übergeordneten SIP-TK-Anlage, an den die SIP-Pakete vom LANCOM aus gesendet werden.

Mögliche Werte:

□ Beliebieger freier TCP/IP-Port.

Default:

□ 5060

In der Firewall muss dieser Port freigeschaltet sein, damit die Verbindung funktionieren kann.

■ **Secret**

Gemeinsames Passwort zum Anmelden an der SIP-TK-Anlage. Dieses Passwort wird nur benötigt, wenn sich SIP-Teilnehmer an der TK-Anlage anmelden sollen, die nicht als SIP-Benutzer mit eigenen Zugangsdaten in der Liste der SIP-Benutzer angelegt sind, oder keine lokale Authentifizierung erzwungen wird, so dass sich SIP-Benutzer ohne Passwort am LANCOM anmelden können, aber mit einem gemeinsamen Passwort bei der übergeordneten SIP-TK-Anlage angemeldet werden, wenn die Domäne der SIP-Benutzer mit der Domäne der SIP-PBX-Line übereinstimmt.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Registrar**

Der SIP-Registrar ist die Stelle, welche die Anmeldung mit den konfigurierten Authentifizierungsdaten für diesen Account in der SIP-TK-Anlage entgegen nimmt.

Mögliche Werte:

□ Maximal 63 alphanumerische Zeichen

Default:

□ Leer

■ **Cln-Prefix**

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser SIP-PBX-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

Mögliche Werte:

□ Maximal 9 Ziffern

Default:

□ Leer

■ **Line-Prefix**

Bei ausgehenden Anrufen über diese Leitung wird der angerufenen Rufnummer dieses Präfix vorangestellt, um eine vollständige für diese Leitung gültige Rufnummer zu erzeugen. Bei ankommenden Rufen wird dieses Präfix entfernt, falls vorhanden.

Mögliche Werte:

□ Maximal 19 Ziffern

Default:

□ Leer

■ **Codecs**

Die beteiligten Endgeräte handeln beim Verbindungsaufbau aus, welche Codecs für die Komprimierung der Sprachdaten verwendeten werden sollen. Mit dem Codec-Filter können Sie die erlaubten Codecs einschränken und nur bestimmte Codecs zulassen.

Mögliche Werte:

□ Auswahl aus der Liste der verfügbaren Codecs.

Default:

□ Alle

Falls die Schnittmenge an verfügbaren Codecs der beteiligten Endgeräte hier ausgeschaltet wird, kommt keine Verbindung zustande.

■ **Codec-Order**

Mit diesem Parameter beeinflussen Sie die Reihenfolge, in der die möglichen Codecs beim Verbindungsaufbau angeboten werden.

Mögliche Werte:

□ Keine Optimierung: Läßt die Reihenfolge der Codecs unverändert.

□ Beste Qualität: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst hohe Sprachqualität erreicht wird.

□ Minimale Bandbreite: Verändert die Reihenfolge der angebotenen Codecs so, dass eine möglichst geringe Bandbreite benötigt wird.

Default:

□ Keine Optimierung

■ **Lokale-Portnummer**

Dies ist der Port des LANCOM-Proxies zur Kommunikation mit der übergeordneten SIP-TK-Anlage.

Mögliche Werte:

□ 1 bis 65536

Default:

□ 0

Besondere Werte:

□ 0: Dynamische Portauswahl, der Port wird automatisch aus dem Pool der freien Portnummern gewählt.

Wenn die (Re-)Registrierung der Leitung deaktiviert ist, muss der lokale Port fest vorgegeben und als Zielport auch in der SIP-TK-Anlage eingetragen werden, damit sich beide Seiten SIP-Signalisierungen senden können.

■ **(Re-)Registrierung**

Hiermit wird die (wiederholte) Registrierung der SIP-PBX-Leitung aktiviert. Die Registrierung kann auch zur Leitungsüberwachung herangezogen werden.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

Für die Nutzung der (Re-)Registrierung muss die Methode der Leitungsüberwachung entsprechend auf "Registrierung" oder "Automatisch" gestellt werden. Die Registrierung wird jeweils nach Ablauf des Überwachungsintervalls wiederholt. Wenn der SIP-Registrar der SIP-TK-Anlage ein anderes Intervall vorschlägt, wird dieses automatisch übernommen.

■ **Leitungsüberwachung**

Spezifiziert die Methode der Leitungsüberwachung. Die Leitungsüberwachung prüft die Verfügbarkeit einer SIP-PBX-Leitung. Der Status der Überwachung kann im Call Router zum Wechsel auf eine Backup-Leitung herangezogen werden. Die Überwachungsmethode legt fest, wie der Status geprüft wird.

Mögliche Werte:

- □ Auto: Die Methode wird automatisch ermittelt.
- □ Deaktiviert: Keine Überwachung, die Leitung wird stets als verfügbar gemeldet. In dieser Einstellung kann die tatsächliche Verfügbarkeit der Leitung nicht überwacht werden.
- □ Register: Überwachung mittels Register-Requests während des Registrierungsvorgangs. Für die Nutzung dieser Einstellung muss für diese Leitung ebenfalls die "(Re-)Registrierung" aktiviert sein.
- □ Options: Überwachung mittels Options-Requests. Dabei wird wie bei einem Polling regelmäßig eine Anfrage an die Gegenstelle verschickt, je nach Antwort wird die Leitung als verfügbar oder nicht verfügbar angesehen. Diese Einstellung eignet sich z. B. für registrierungslose Leitungen.

Default:

- □ Auto

■ **Überwachungsintervall**

Das Intervall der Leitungsüberwachung in Sekunden. Dieser Wert wirkt sich sowohl auf die Leitungsüberwachung mit Register-Request als auch mit Option-Request aus. Das Überwachungsintervall muss mindestens 60 Sekunden betragen und legt fest, nach welcher Zeit die Überwachungsmethode erneut angewendet wird. Wenn die (Re-)Registrierung aktiviert ist, wird das Überwachungsintervall auch als Zeitraum bis zur nächsten Registrierung verwendet.

Mögliche Werte:

- □ Max. 5 Ziffern.

Default:

- □ 60

Besondere Werte:

- □ Werte kleiner als 60 Sekunden werden automatisch als 60 Sekunden angenommen.

Falls die Gegenstelle in der Antwort auf einen Option-Request einen anderen Wert für das Überwachungsintervall vorschlägt, so wird dieser akzeptiert und in der Folgezeit verwendet.

■ **Vertrauenswürdig**

Spezifiziert die Zugehörigkeit der Gegenstelle dieser Leitung (Provider) zur "Trusted-Area". In dieser vertrauenswürdigen Zone wird die Caller ID als Information über den Gesprächsteilnehmer nicht entfernt, selbst wenn das durch Einstellungen in der Leitung (CLIR) oder durch das Endgerät gewünscht ist. Bei einer Verbindung über eine vertrauenswürdige Leitung wird die Caller ID entsprechend der ausgewählten Privacy-Methode übertragen und erst in der letzten Vermittlungsstelle vor dem entfernten Gesprächsteilnehmer entfernt. Innerhalb der vertrauenswürdigen Zone kann so z. B. die Caller ID für Abrechnungszwecke ausgewertet werden. Diese Funktion ist u. a. für Provider interessant, die mit einem VoIP-Router direkt beim Kunden das von ihnen selbst verwaltete Netzwerk bis zum Anschluss der VoIP-Endgeräte ausdehnen.

Mögliche Werte:

- □ Ja: Vertrauenswürdig
- □ Nein: Nicht vertrauenswürdig

Default:

- □ Ja

Bitte beachten sie, dass diese Funktion nicht von allen Providern unterstützt wird.

■ **Privacy-Methode**

Spezifiziert die verwendete Methode zur Übermittlung der Absenderinformationen im separaten SIP-Feld.

Mögliche Werte:

- □ Keine
- □ RFC3325: mittels P-Preferred-Id/P-Asserted-Id
- □ IETF-Draft-Sip-Privacy-04: mittels RPID (Remote Party ID)

Default:

- □ Keine

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag.

Mögliche Werte:

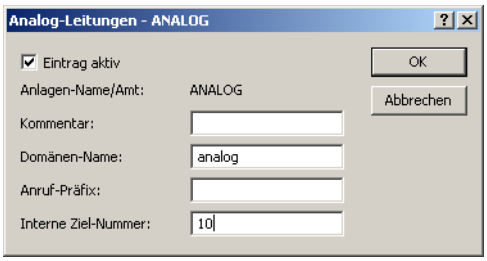
□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Analog-Line

LANconfig: VoIP-Call-Manager ▶ Leitungen ▶ Analog-Leitungen



WEBconfig: Setup ▶ Voice-Call-Manager ▶ Line ▶ Analog

■ **Name**

Name der Leitung, darf nicht identisch sein mit einer anderen in dem Gerät konfigurierten Leitung.

Mögliche Werte:

□ Maximal 16 alphanumerische Zeichen

Default:

□ Leer

■ **Domain**

Domänen-Name der Analog-Leitung, der für die Adressierung in SIP verwendet wird.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ analog

■ **Cln-Prefix**

Das Anruf-Präfix ist eine Nummer, die den Anrufer-Nummern (CLI; SIP „From:“) aller ankommenden Anrufe auf dieser Analog-Leitung vorangestellt wird, um eindeutige Rückruf-Nummern zu erzeugen.

Beispielsweise kann hier eine Nummer ergänzt werden, die im Call-Router bei abgehenden Rufen (dem Rückruf) zur Leitungsauswahl ausgewertet und wieder entfernt wird.

Mögliche Werte:

□ Maximal 9 Ziffern

Default:

□ Leer

■ **Number/Name**

Interne Rufnummer/SIP-URI, den jeder Anruf auf diese Analog-Leitung als Rufziel erhält. Diese Rufnummer kann sich von der tatsächlichen Rufnummer des Telefonie-Anbieters für den analogen Leitungs-Anschluss unterscheiden (Mapping).

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

Tragen Sie hier z.B. die Rufnummer einer Gruppe ein, die jeden eingehenden Anruf erhält und steuern Sie darüber flexibel, welche Telefone bei Rufen klingeln oder leiten Sie den Ruf nach einer Zeit auf eine Mobilnummer oder den Anrufbeantworter um.

■ **Active**

Aktiviert oder deaktiviert den Eintrag.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **Kommentar**

Kommentar zu diesem Eintrag.

Mögliche Werte:

□ Maximal 64 alphanumerische Zeichen

Default:

□ Leer

■ **Caller-ID Signaling**

Die Anbieter von analogen Telefonanschlüssen unterstützen unterschiedliche Dienstmerkmale, zu denen auch die Übertragung der Caller ID, also die Anzeige des anrufenden Teilnehmers auf dem Display des gerufenen Endgerätes gehört. Dieser Dienst ist auch als Calling Line Identification Presentation (CLIP) bekannt. Die Caller ID wird je nach Land und Anbieter durch zwei verschiedene Modulationsverfahren über die analoge Verbindung übertragen (FSK oder DTMF).

Mögliche Werte:

□ Default: In dieser Einstellung werden die Standardwerte für das Land verwendet, in dem das Gerät eingesetzt wird.

□ FSK: Übertragung der Caller ID mit dem FSK-Verfahren (Frequency Shift Keying)

□ DTMF: Übertragung der Caller ID mit dem DMTF-Verfahren (Dual Tone Multi Frequency)

Default:

Länderspezifische Default-Werte:

□ Niederlande: DTMF

□ Alle anderen Länder: V.23 (FSK)

■ **Caller-ID Transmission Requirements**

Neben der Auswahl des Modulationsverfahrens ist bei der Übertragung der Caller ID auch die zeitliche Steuerung der Signalisierung auf analogen Leitungen je nach Land und Anbieter unterschiedlich geregelt. Damit das gerufene Endgerät die Caller ID zum richtigen Zeitpunkt erwartet, wird das vom Anbieter genutzte Verfahren entsprechend eingestellt.

Mögliche Werte:

□ Default: In dieser Einstellung werden die Standardwerte für das Land verwendet, in dem das Gerät eingesetzt wird.

□ During-Ringing: Die Caller ID wird während des Klingel-Vorgangs übertragen, und zwar zwischen dem ersten und zweiten Klingelton.

□ RP-AS: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden, sondern wird durch ein spezielles "Alarmsignal" angekündigt. Dieses Alarmsignal wird durch Klingelimpulse dargestellt (Ringing Pulse Alerting Signal, RP-AS). Nach dem Klingelimpuls kann die Caller ID übertragen werden.

□ Line-Reversal: Die Übertragung der Caller ID ist zeitlich nicht mit dem Klingeln verbunden, sondern wird durch ein spezielles "Alarmsignal" angekündigt. Das Alarmsignal wird durch das kurzzeitige Vertauschen der Polarität auf der Leitung dargestellt (Line Reversal). Nach dem Line Reversal kann die Caller ID übertragen werden.

Default:

Länderspezifische Default-Werte:

□ Österreich: During-Ringing

□ Belgien: Ringing Pulse Alerting Signal, RP-AS

□ Frankreich: During-Ringing

- □ Italien: During-Ringing
- □ Schweiz: During-Ringing
- □ Niederlande: Line-Reversal
- □ Spanien: Ringing Pulse Alerting Signal, RP-AS
- □ United Kingdom: Line-Reversal
- □ Deutschland: During-Ringing

H WLAN

H.1 Konfiguration der WLAN-Parameter

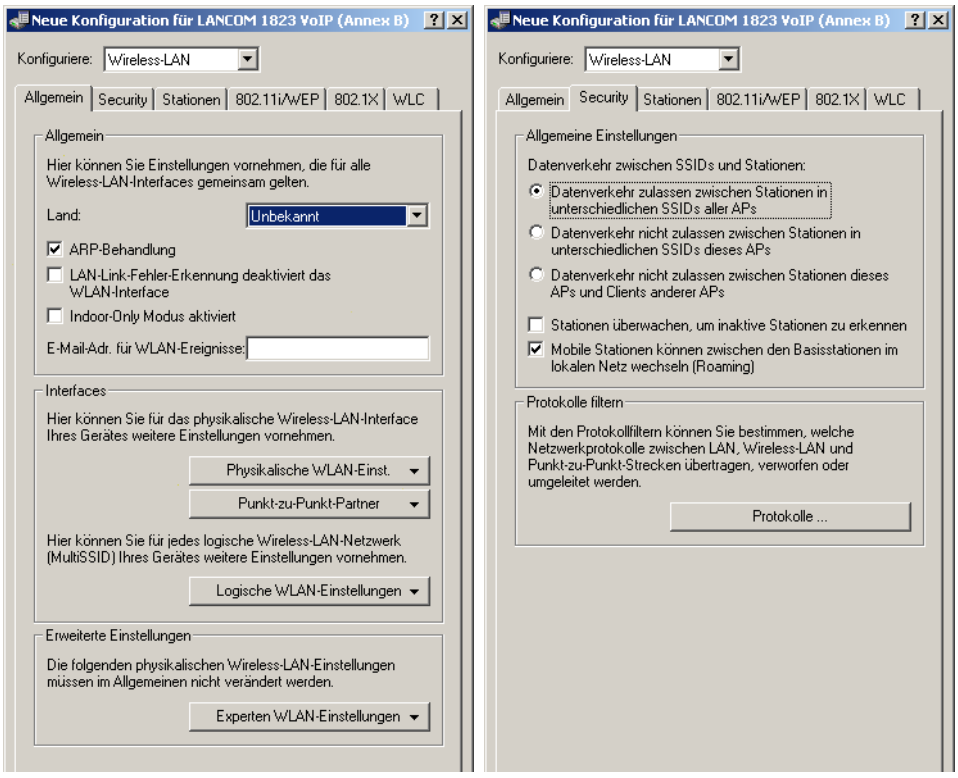
H.1.1 Allgemeine WLAN-Einstellungen

Änderungen mit LCOS 7.6:

- Inter-SSID-Verkehr für das gesamte WLAN einstellbar.

LANconfig: Wireless-LAN ▶ Allgemein

LANconfig: Wireless-LAN ▶ Security



WEBconfig: Setup ▶ WLAN

- **Link-Fehler-Erkennung**

  Das WLAN-Interface wird deaktiviert, wenn die LAN-Verbindung (Link) verloren geht. (Broken-Link-Detection)

  Mögliche Werte:

  □ Ja, Nein

  Default:

  □ Nein

Bei WLAN-Geräten mit mehreren LAN-Schnittstellen bezieht sich dieser Parameter immer auf die erste LAN-Schnittstelle LAN-1.

- **Heap-Reserve**

  Die Heap-Reserve gibt an, wie viele Blöcke des LAN-Heaps für die direkte Kommunikation (Telnet) mit dem Gerät reserviert werden. Wenn die Anzahl der Blöcke im Heap unter den angegebenen Wert fällt, dann werden empfangene Pakete sofort verworfen (außer bei TCP-Paketen, die direkt an das Gerät gerichtet sind).

  Mögliche Werte:

  □ Max. drei Ziffern

  Default:

  □ 10

- **IAPP-Protokoll**

  Über das Inter Access Point Protocol (IAPP) tauschen die Access Points untereinander Informationen über die eingebuchten Clients aus. Diese Informationen werden beim Roaming von Clients zwischen verschiedenen

Access Points verwendet. Der neue Access Point informiert den bisherigen Access Point über den Roaming-Vorgang, damit der bisherige Access Point den Client aus seiner Stationstabelle löschen kann.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

■ **IAPP-Announce-Interval**

In diesem Intervall (in Sekunden) geben die Access Points ihre SSIDs bekannt.

Mögliche Werte:

□ Max. 10 Ziffern.

Default:

□ 120

■ **IAPP-Handover-Timeout**

Bei einem erfolgreichen Roaming-Vorgang (Handover) informiert der neue Access Point den bisherigen Access Point darüber, dass ein bestimmter Client jetzt bei einem anderen Access Point angemeldet ist. Mit dieser Information kann der alte Access Point den Client aus seiner Stationstabelle austragen und leitet nicht mehr (unnötigerweise) Pakete für diesen Client in seine Funkzelle weiter. Für diesen Zeitraum (in Millisekunden) wartet der neue Access Point, bis er versucht, den bisherigen Access Point noch einmal zu kontaktieren. Nach fünf Versuchen gibt der neue Access Point diese Versuche auf.

Mögliche Werte:

□ Max. 10 Ziffern

Default:

□ 1000

■ **Land**

Damit das WLAN mit den zulässigen Parametern betrieben werden kann, muss das Gerät seinen nationalen Standort kennen.

□ Auswahl aus der Liste der angebotenen Länder.

Default:

□ Leer

■ **Nur-Indoor-Betrieb**

Bei aktiviertem Indoor-Only Modus werden im 5 GHz Band in ETSI-Ländern die Kanäle auf den Bereich 5,15 bis 5,25 GHz (Kanäle 36-48) beschränkt. Die Radarerkennung (DFS) wird ausgeschaltet und es entfällt die Zwangsunterbrechung alle 24 Stunden. In dieser Betriebsart ist daher das Risiko von Unterbrechungen durch (falsche) Radarerkennungen reduziert. Im 2,4 GHz Band in Frankreich werden die Kanäle 8 bis 13 freigegeben, wodurch mehr Kanäle zur Verfügung stehen.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

Die Aktivierung des Indoor-Only-Modus ist nur erlaubt, wenn die Basisstation und alle Stationen in einem geschlossenen Raum betrieben werden.

■ **Mail-Adresse**

An diese E-Mail-Adresse werden Informationen über die Ereignisse im WLAN versendet.

Mögliche Werte:

□ Gültige E-Mail-Adresse

Default:

□ Leer

Zur Nutzung der E-Mail-Benachrichtigung muss ein SMTP-Konto eingerichtet sein.

■ **Karten-Reinit-Zyklus**

In diesem Intervall (in Sekunden) werden die internen WLAN-Karten bei älteren Access Points re-initialisiert, um Point-to-Point-Verbindungen aufrecht zu erhalten. Diese Funktion wird bei aktuelleren Modellen über den "Alive-Test" ersetzt.

Mögliche Werte:

□ Max. 10 Ziffern.

Default:

□ 0

Besondere Werte:

□ 0: Deaktiviert diese Funktion.

■ **Rausch-Messzyklus**

In diesem Intervall (in Sekunden) wird bei WLAN-Karten mit Atheros-Chipsatz der Rauschpegel auf dem Medium gemessen.

Mögliche Werte:

□ Max. 10 Ziffern

Default:

□ 10

Besondere Werte:

□ 0: Deaktiviert diese Funktion.

Bitte beachten Sie, dass die Hardware der WLAN-Karte bei deaktiviertem Rausch-Messzyklus nicht mehr auf veränderte Rauschpegel reagieren kann! Bei der Verwendung von DFS ist diese Messung verpflichtend (automatisch im Intervall von 10 Sekunden). In diesen Fällen kann hier nur ein kürzeres Intervall eingestellt werden, die Funktion darf jedoch nicht deaktiviert werden.

■ **Therm.-Rekal.-Messzyklus**

In diesem Intervall (in Sekunden) wird bei älteren WLAN-Karten mit Atheros-Chipsatz die Sendeleistung korrigiert, um thermische Schwankungen auszugleichen.

Mögliche Werte:

□ Max. 10 Ziffern

Default:

□ 20

Besondere Werte:

□ 0: Deaktiviert diese Funktion.

Bitte beachten Sie, dass die Hardware der WLAN-Karte bei deaktiviertem Therm.-Rekal.-Messzyklus nicht mehr auf thermische Schwankungen reagieren kann!

■ **Trace-MAC**

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Client eingestellt werden, dessen WLAN-MAC-Adresse hier eingetragen wird.

Mögliche Werte:

□ Max. 12 hexadezimale Zeichen

Default:

□ 000000000000

Besondere Werte:

□ 000000000000: Deaktiviert diese Funktion und gibt die Tracemeldungen von allen Clients aus.

■ **Trace-Stufe**

Für den WLAN-Data-Trace kann die Ausgabe von Tracemeldungen auf einen bestimmten Inhalt beschränkt werden. Die Meldungen werden dazu in Form einer Bit-Maske eingetragen.

Mögliche Werte:

□ 0 bis 255.

□ 0: nur die Meldung, dass ein Paket überhaupt empfangen/gesendet wurde

- □ 1: zusätzlich die physikalischen Parameter der Pakete /Datenrate, Signalstärke...)
- □ 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

Default:

- □ 255

■ **Idle-Timeout**

Zeit der Inaktivität (in Minuten), nach der ein Client vom Access Point getrennt wird. Die vom Client empfangenen Pakete setzen diese Zeit zurück (nicht die zum Client gesendeten Pakete).

Mögliche Werte:

- □ 0 bis 65535 (5 Zeichen)

Default:

- □ 60

Besondere Werte:

- □ 0: Schaltet den Timeout aus

■ **Ueberwachung-Stationen**

Besonders bei öffentlichen WLAN-Zugriffspunkten (Public Spots) ist es für die Abrechnung der Nutzungsgebühren erforderlich, nicht mehr aktive Stationen zu erkennen. Dazu kann der Access Point 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.

Mögliche Werte:

- □ Ja, Nein

Default:

- □ Nein

■ **ARP-Behandlung**

Will eine Station im LAN eine Verbindung zu einer Station im WLAN aufbauen, die im Stromspar-Modus ist, so klappt dies häufig entweder gar nicht oder nur mit großen Verzögerungen. Der Grund ist, dass die Auslieferung von Broadcasts, z.B. ARP-Anfragen, an im Powersave befindliche Stationen von der Basisstation nicht garantiert werden kann.

Wenn Sie die ARP-Behandlung einschalten, beantwortet die Basisstation ARP-Anfragen für bei ihr eingebuchte Stationen selber und damit in solchen Fällen zuverlässiger.

Mögliche Werte:

- □ Ja, Nein

Default:

- □ Ja

■ **Zugriffsmodus**

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

Mögliche Werte:

- □ Positiv: Daten von den aufgeführten Stationen ausfiltern, alle anderen Stationen übertragen
- □ Negativ: Daten von den aufgeführten Stationen übertragen, alle anderen über RADIUS authentifizieren oder ausfiltern.

■ **Inter-SSID-Verkehr**

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point 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.

Mögliche Werte:

- □ Ja, Nein

Default:

- □ Ja

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.

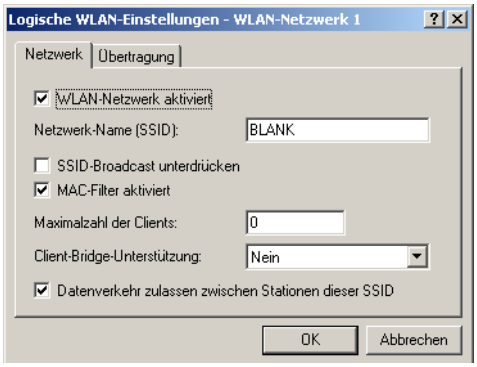
H.1.2 WLAN-Netzwerke

Änderungen mit LCOS 7.6:

- Inter-Stations-Verkehr für jedes logische WLAN separat einstellbar.

Jede physikalische WLAN-Schnittstelle kann bis zu acht verschiedene logische Funknetzwerke aufspannen (Multi-SSID). Für jedes dieser Funknetze können bestimmte Parameter speziell definiert werden, ohne dass zusätzliche Access Points benötigt werden.

LANconfig: Wireless-LAN ▶ Allgemein ▶ Logische WLAN-Einstellungen



WEBconfig: Setup ▶ Schnittstellen ▶ WLAN ▶ Netzwerk

- **Ifc**

  Auswahl aus den logischen WLAN-Schnittstellen.

  Mögliche Werte:

  □ WLAN-1 bis WLAN-1-8, WLAN-2 bis WLAN-2-8

- **Aktiv**

  Schaltet das logische WLAN separat ein- oder aus.

  Mögliche Werte:

  □ Ja, Nein

  Default:

  □ Ja

- **Netzwerkname**

  Stellen Sie für jedes benötigte logische WLAN eine eindeutige SSID (den Netzwerknamen) ein. Nur solche Netzwerkkarten, die über die gleiche SSID verfügen, können sich in diesem Funknetzwerk anmelden.

  Mögliche Werte:

  □ Max. 32 Zeichen

  Default:

  □ Leer

- **MAC-Filter**

  In der MAC-Filterliste werden die MAC-Adressen der Clients hinterlegt, die sich bei einem WLAN einbuchen dürfen. Mit dem Schalter 'MAC-Filter' kann die Verwendung der MAC-Filterliste gezielt für einzelne logische Netzwerke ausgeschaltet werden.

  Die Verwendung der MAC-Filterliste ist auf jeden Fall erforderlich für logische Netzwerke, in denen sich die Clients mit einer individuellen Passphrase uber LEPS anmelden. Die bei LEPS verwendete Passphrase wird ebenfalls in der MAC-Filterliste eingetragen. Für die Anmeldung mit einer individuellen Passphrase wird daher immer die MAC-Filterliste beachtet, auch wenn diese Option hier deaktiviert ist.

  Mögliche Werte:

  □ Ja, Nein

  Default:

□ Nein

■ **RADIUS-Accounting**

Aktiviert das Accounting über RADIUS für dieses logische WLAN, z. B. um IP-Adressen und Datenvolumen der eingebuchten Clients zu erfassen. Die RADIUS-Pakete für das Accounting werden an den Server verschickt, der für das RADIUS-Accounting eingetragen ist.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Closed-Network**

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' in Ihrem Funknetzwerk anmelden.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Maximum-Stationen**

Legen Sie hier die maximale Anzahl der Clients fest, die sich bei diesem Access Point einbuchen dürfen. Weitere Clients, die sich über diese Anzahl hinaus anmelden wollen, werden abgelehnt.

Mögliche Werte:

□ Max. 10 Zeichen

Default:

□ 0

Besondere Werte:

□ 0: Keine Beschränkung für die maximale Anzahl der eingebuchten Clients.

■ **Cl.-Brg.-Support**

Während mit der Adress-Anpassung im Client-Modus nur die MAC-Adresse eines einzigen angeschlossenen Gerätes für den Access Point sichtbar gemacht werden kann, werden über die Client-Bridge-Unterstützung alle MAC-Adressen der Stationen im LAN hinter der Clientstationen transparent an den Access Point übertragen.

Aktivieren Sie diese Option für das logische WLAN, wenn den Clients diese Betriebsart angeboten werden soll.

Mögliche Werte:

□ Ja, Nein, Exclusiv

Default:

□ Nein

Besondere Werte:

□ Exclusiv: In dieser Einstellung werden nur solche Clients akzeptiert, die diese Betriebsart unterstützen.

Der Client-Bridge-Modus kann ausschließlich zwischen zwei LANCOM-Geräten verwendet werden.

■ **Inter-Stations-Verkehr**

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Für jedes logische WLAN kann separat eingestellt werden, ob die Clients in dieser SSID untereinander Daten austauschen können.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

Die Kommunikation der Clients in unterschiedlichen logischen WLANs wird zentral bei den allgemeinen WLAN-Einstellungen gesteuert (Inter-SSID-Verkehr).

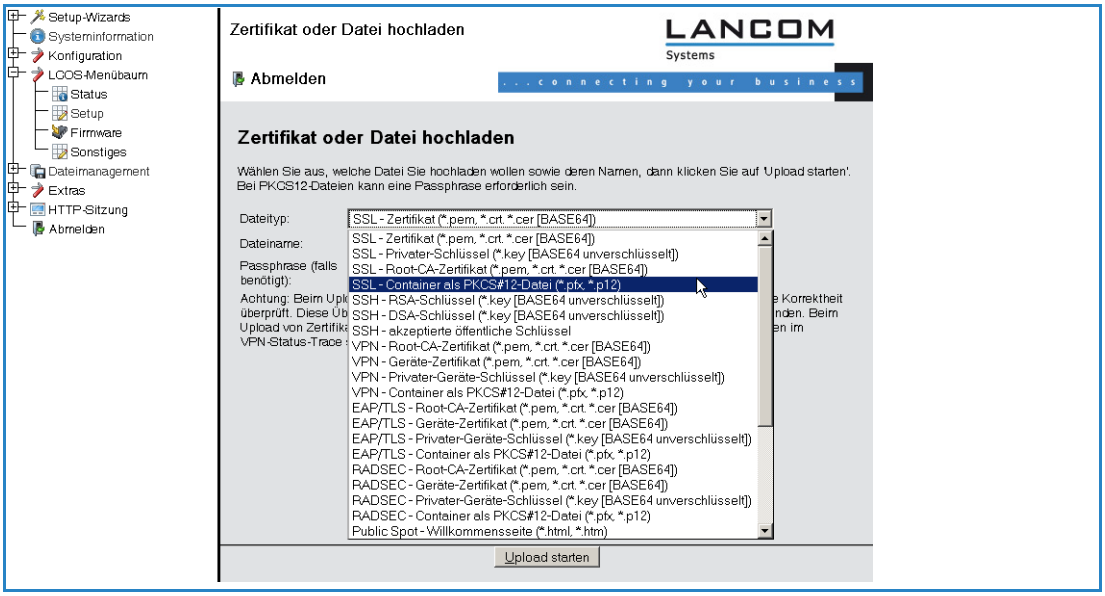
H.2 Mehrstufige Zertifikate für PublicSpots

Neu mit LCOS 7.6:

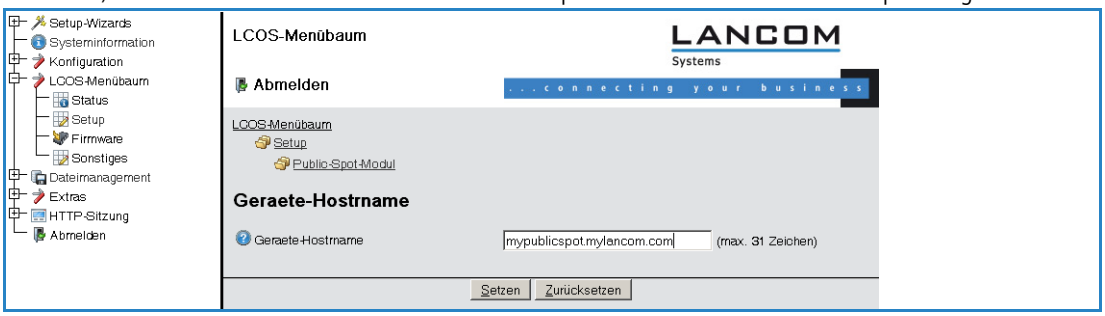
- Mehrstufige Zertifikate für PublicSpots

SSL-Zertifikatsketten können in Form eines PKCS#12-Containers in das LANCOM geladen werden. Diese Zertifikatsketten können für die PublicSpot-Authentifizierungsseiten über den im LCOS implementierten HTTPS-Server verwendet werden. Zertifikate von allgemein anerkannten Trust-Centern sind üblicherweise mehrstufig. Offiziell signierte Zertifikate im PublicSpot sind notwendig, um Zertifikatsfehlermeldungen des Browsers bei PublicSpot-Authentifizierungen zu vermeiden.

Das Zertifikat laden Sie z.B. unter WEBconfig 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 PublicSpot anstelle einer internen IP-Adresse den DNS-Namen des Zertifikats als Ziel angeben (LCOS Menübaum/Setup/Public-Spot-Modul/Geraete-Hostname). Dieser Name muss im DNS-Server auf die entsprechende IP-Adresse des PublicSpots aufgelöst werden.



H.3 DFS 2: Freilassen von Kanälen für Wetter-Radar

Beim für 5 GHz WLANs geforderten DFS-Verfahren (Dynamic Frequency Selection) wird automatisch eine freie Frequenz gewählt, z. B. um das Stören von Radaranlagen zu verhindern und um die WLAN-Geräte möglichst gleichmäßig über das ganze Frequenzband zu verteilen. Die Signale von Wetter-Radarstationen können jedoch manchmal nicht sicher erkannt werden.

Die europäische Kommission fordert daher in Ergänzung zu den Standards ETSI EN 301 893 V1.3.1 und ETSI EN 310 893 V1.4.1, im Unterband 2 des 5 GHz-Bandes drei Kanäle (120, 124 und 128) auszusparen und nicht für die automatische Kanalwahl zu verwenden. Verfahren zur Erkennung der Wetter-Radar-Signaturen befinden sich in Entwicklung.

H.4 Zentrales Firmware- und Skript-Management

Neu mit LCOS 7.6:

- Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

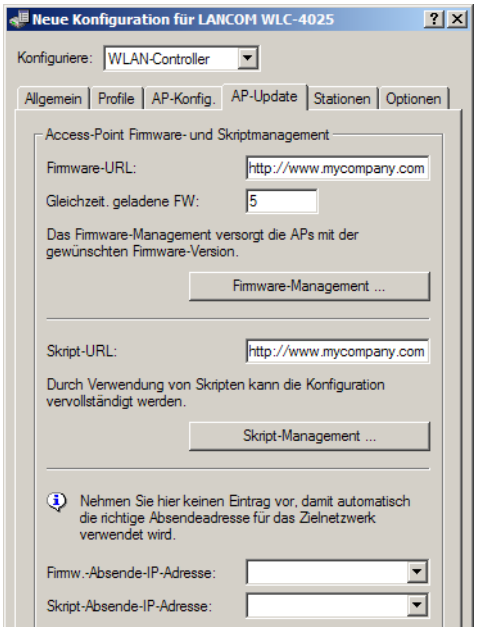
Mit einem LANCOM WLAN Controller kann die Konfiguration von mehreren LANCOM Wireless Routern und LANCOM Access Points von einer Stelle aus komfortabel und konsistent verwaltet werden. Mit dem zentralen Firmware- und Skript-Management können auch Firmware- und Skript-Uploads auf allen verwalteten WLAN-Geräten automatisch ausgeführt werden.

Dazu werden die Firmware- und Skript-Dateien auf einem Web-Server abgelegt (Firmware als *.UPX, Skripte als *.LCS). Der WLAN-Controller 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 Access Point läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points 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 Access Point automatisch neu.
- Wenn der Access Point schon verbunden ist, startet das Gerät danach **nicht** automatisch neu. In diesem Fall wird der Access Point manuell über die Menüaktion "/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs" oder zeitgesteuert per Cron-Job neu gestartet.
- Mit der Aktion "/Setup/WLAN-Management/Central-Firmware-Management/Update-Firmware-and-Script-Information" können Skript- und Firmwareverzeichnisse aktualisiert werden.



Sie finden die Parameter zur Konfiguration auf folgenden Pfaden:

LANconfig: **WAN-Controller ▶ AP-Update**

WEBconfig: **Setup ▶ WLAN-Management ▶ Zentrales-Firmware-Management**

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 WLAN-Controllers vorgehaltenen Firmware-Versionen.

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' fur die IP-Adresse im ersten Netzwerk mit der Einstellung 'DMZ'.
- □ Name einer Loopback-Adresse.
- □ Beliebige andere IP-Adresse.

Default:

- □ leer

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

Tabelle mit Gerätetyp, MAC-Adresse und Firmware-Version zur gezielten Steuerung der verwendeten Firmware-Dateien.

■ **Gerätetypen**

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- □ Mögliche Werte: Alle bzw. 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

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

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

Tabelle mit Skript-Dateiname und WLAN-Profil zur Zuordnung der Skripte zu einem WLAN-Profil.

Die Konfiguration eines Wireless Routers und Access Points 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 Wireless Router und Access Points 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 Wireless Router oder Access Point wird allerdings eine MD5-Prüfsumme der Skript-Datei gespeichert. Über diese Prüfsumme kann der WLAN-Controller 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

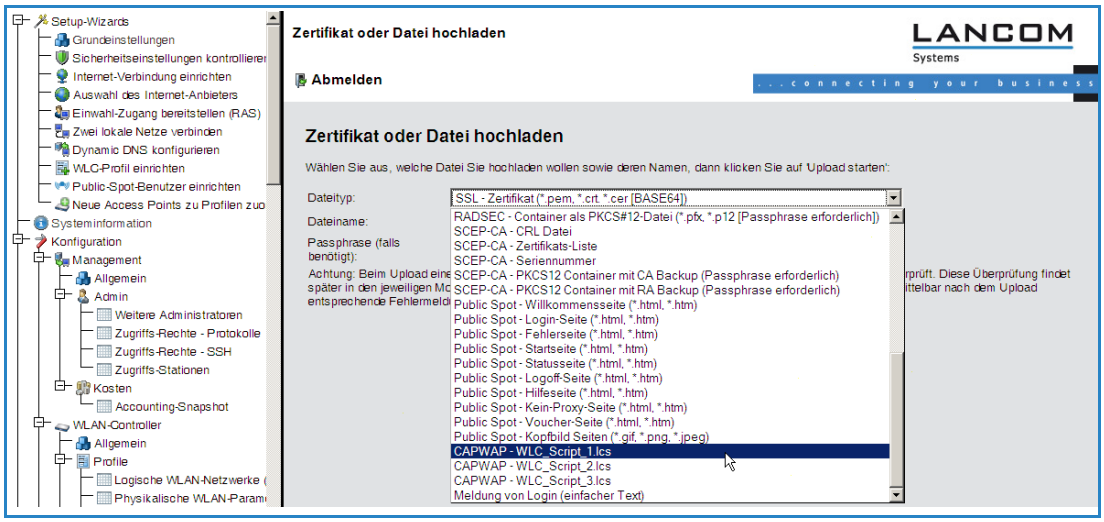
Interner Skript-Speicher (Skript-Management ohne HTTP-Server)

Skripte haben im Gegensatz zu Firmware-Dateien oft nur ein geringes Datenvolumen. Im internen Skript-Speicher der WLAN-Controller 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).

Bitte beachten Sie bei der Angabe der Script-Namen die Groß- und Kleinschreibung!



I Meldungen

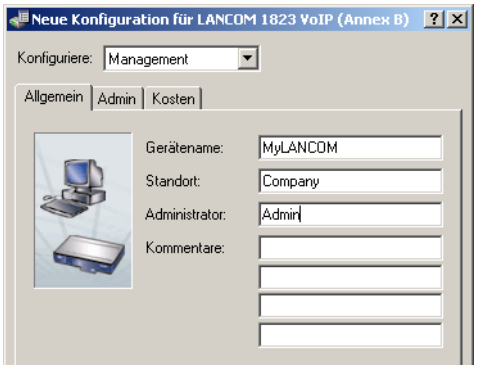
I.1 SNMP-Traps

Neu in LCOS 7.60:

- SNMP-Traps: Trapversion konfigurierbar

I.1.1 Allgemeine SNMP-Einstellungen

LANconfig: Management ▶ Allgemein



WEBconfig: Setup ▶ SNMP

- **Traps-senden**

  Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der IP-Trap-Tabelle die IP-Adressen der Computer ein, auf denen diese SNMP-Manager installiert sind.

  Mögliche Werte:

  □ Ja, Nein

  Default:

  □ Nein

- **Administrator**

  Name des Geräte-Administrators. Wird nur zu Anzeigezwecken verwendet.

  Mögliche Werte:

  □ Max. 255 Zeichen

  Default:

  □ Leer

- **Standort**

  Standortangabe zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

  Mögliche Werte:

  □ Max. 255 Zeichen

  Default:

  □ Leer

- **Register-Monitor**

  Mit dieser Aktion können sich SNMP-Agenten bei einem Gerät anmelden, um anschließend SNMP-Traps zu erhalten. Zu dem Kommando werden dazu die IP-Adresse, der Port und die MAC-Adresse des SNMP-Agenten angegeben. Beide Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

  Mögliche Werte:

  □ <IP-Adresse|*>:<Port|*> <MAC-Adresse|*> <W>

  Besondere Werte:

  □ <W> am Ende des Kommandos ist für eine Registrierung über eine WAN-Verbindung erforderlich.

Ein LANmonitor muss nicht explizit am Gerät angemeldet werden. Der LANmonitor überträgt bei der Suche nach neuen Geräten automatisch die Anmeldeinformationen an das Gerät.

■ **Loesche-Monitor**

Mit dieser Aktion können angemeldete SNMP-Agenten aus der Monitor-Liste entfernt werden. Zu dem Kommando werden dazu die IP-Adresse und der Port des SNMP-Agenten angegeben. Alle drei Werte können durch den Platzhalter * ersetzt werden, in diesem Fall ermittelt das Gerät die Werte aus den vom SNMP-Agenten empfangenen Paketen.

Mögliche Werte:

□ <IP-Adresse|*>:<Port|*>

■ **Passw.Zwang-fuer-SNMP-Lesezugriff**

Mit dieser Option können Sie entscheiden, dass zum Lesen von SNMP-Meldungen über einen SNMP-Agenten (z. B. LANmonitor) ein Passwort benötigt wird. Ist diese Option aktiviert, so muss zwingend das Gerätepasswort (oder Username:Passwort) als Community verwendet werden.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Kommentar-1**

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Mögliche Werte:

□ Max. 255 Zeichen

Default:

□ Leer

■ **Kommentar-2**

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Mögliche Werte:

□ Max. 255 Zeichen

Default:

□ Leer

■ **Kommentar-3**

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Mögliche Werte:

□ Max. 255 Zeichen

Default:

□ Leer

■ **Kommentar-4**

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Mögliche Werte:

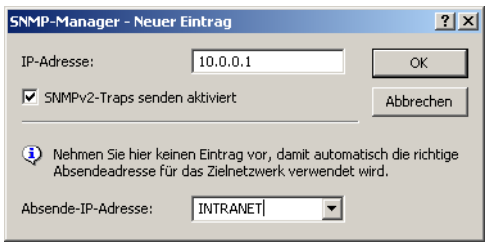
□ Max. 255 Zeichen

Default:

□ Leer

I.1.2 Die IP-Trap-Tabelle

LANconfig: Meldungen ▶ SNMP ▶ SNMP-Manager



WEBconfig: Setup ▶ SNMP ▶ IP-Traps

- **Trap-IP**
  Geben Sie hier die IP-Adresse des Computers ein, auf dem ein SNMP-Manager installiert ist.
  Mögliche Werte:
  - □ Gültige IP-Adresse

  Default:
  - □ Leer
- **Loopback-Addr.**
  Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten 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

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.

- **Version**
  Gibt die SNMP-Version an, die für die Traps an diesen Empfänger verwendet werden soll.
  Mögliche Werte:
  - □ SNMPv1, SNMPv2

  Default:
  - □ SNMPv2

I.1.3 Die Monitor-Tabelle

Die Monitor-Tabelle zeigt alle am Gerät angemeldeten SNMP-Agenten.

- **Gegenstelle**
  Name der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.
- **IP-Adresse**
  IP-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.
- **Loopback-Addr.**
  Loopback-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.
- **MAC-Adresse**
  MAC-Adresse der Gegenstelle, von der ein SNMP-Agent auf das Gerät zugreift.
- **Port**
  Port, über den die Gegenstelle mit einem SNMP-Agenten auf das Gerät zugreift.
- **Timeout**
  Timeout in Minuten, bis die Gegenstelle aus der Monitor-Tabelle entfernt wird.
- **VLAN-ID**
  VLAN-ID, über den die Gegenstelle mit einem SNMP-Agenten auf das Gerät zugreift.
- **Ethernet-Port**
  Ethernet-Port, über den die Gegenstelle mit einem SNMP-Agenten auf das Gerät zugreift.
- **LAN-Ifc**
  LAN-Ifc, über den die Gegenstelle mit einem SNMP-Agenten auf das Gerät zugreift.

J Server- Dienste

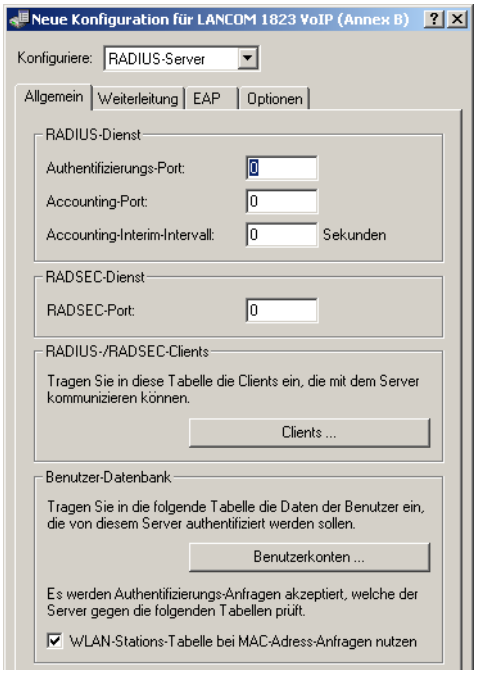
J.1 RADIUS- Server

Neu in LCOS 7.60:

- VLAN- ID in der Tabelle der RADIUS- Benutzer
- Maskierung auf rufende Stationen und/oder gerufene RADIUS Clients (z.B. Access Points) in der Tabelle der RADIUS- Benutzer

J.1.1 Globale Einstellungen für den RADIUS- Server

LANconfig: RADIUS- Server ▶ Allgemein



WEBconfig: Setup ▶ RADIUS ▶ Server

- **Authentifizierungs- Port**

  Geben Sie hier den Port an, über den der RADIUS- Client mit dem RADIUS- Server im Gerät kommunizieren. Üblicherweise wird der Port '1812' verwendet.

  Mögliche Werte:

  □ Max. 4 Ziffern

  Default:

  □ 0

  Besondere Werte:

  □ 0: Schaltet den RADIUS- Server aus.

- **Accounting- Interim- Intervall**

  Geben Sie hier an, welchen Wert der RADIUS- Server bei erfolgreicher Authentifizierung als "Accounting- Interim- Interval" ausgeben soll. Sofern das anfragende Gerät dieses Attribut unterstützt, wird damit gesteuert, in welchem Intervall (in Sekunden) ein Update der Accounting- Daten an den Accounting- RADIUS- Server geschickt wird.

  Mögliche Werte:

  □ Max. 4 Ziffern

  Default:

  □ 0

  Besondere Werte:

  □ 0: Schaltet die Verwendung dieser Funktion aus.

■ **Accounting- Port**

Geben Sie hier den Port an, über den der RADIUS-Server Accounting-Informationen entgegennimmt. Üblicherweise wird der Port 1813 verwendet.

Mögliche Werte:

□ Max. 4 Ziffern

Default:

□ 1813

Besondere Werte:

□ 0: Schaltet die Verwendung dieser Funktion 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.

Mögliche Werte:

□ Max. 24 Zeichen

Default:

□ Leer

■ **Empty- Realm**

Dieser Realm wird verwendet, wenn der übermittelte Benutzername keinen Realm enthält.

Mögliche Werte:

□ Max. 24 Zeichen

Default:

□ Leer

■ **RADSEC- Port**

Geben Sie hier an, über welchen (TCP-)Port der Server über RADSEC verschlüsselte Accounting- oder Authentifizierungs-Anfragen annimmt. Üblicherweise wird Port 2083 verwendet.

Mögliche Werte:

□ Max. 4 Ziffern

Default:

□ 2083

Besondere Werte:

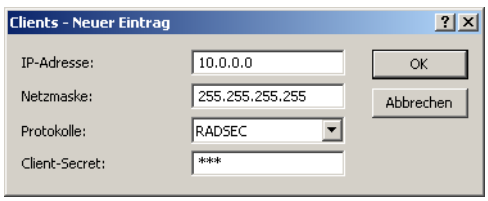
□ 0: Deaktiviert RADSEC im RADIUS-Server.

J.1.2 Tabelle der RADIUS- Clients

In der Clients-Tabelle werden die Clients eingetragen, die mit dem RADIUS-Server kommunizieren können.

Die von einem WLAN-Controller angelegten managed Access Points werden nicht explizit in die Liste der RADIUS-Clients aufgenommen. Die manuelle Angabe ist hier nicht notwendig.

LANconfig: RADIUS-Server ▶ Allgemein ▶ RADIUS-Clients



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Clients

■ **IP- Netz**

IP-Netz (Bereich von IP-Adressen) der RADIUS-Clients, für die das in diesem Eintrag definierte Kennwort gilt.

Mögliche Werte:

□ Gültige IP-Netzadresse

Default:

□ Leer

■ **IP- Netzmaske**

IP- Netzmaske des RADIUS- Clients.

Mögliche Werte:

□ Gültige IP- Netzmaske

Default:

□ Leer

■ **Protocols**

Protokoll für die Kommunikation zwischen dem internen RADIUS- Server und den Clients.

Mögliche Werte:

□ RADSEC, RADIUS, alle

Default:

□ RADIUS

■ **Secret**

Kennwort, das der Client für den Zugang zum internen RADIUS- Server benötigt.

Mögliche Werte:

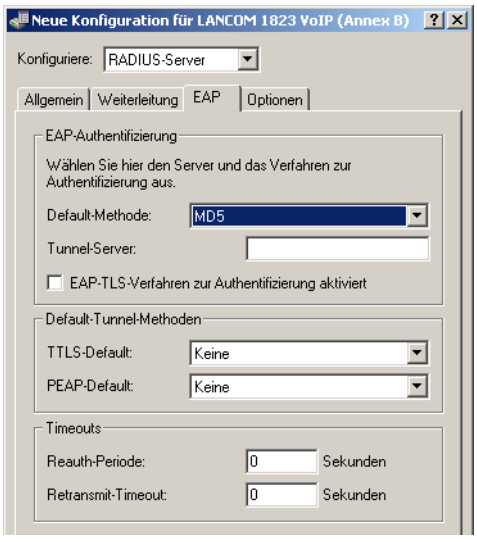
□ Max. 32 Zeichen

Default:

□ Leer

J.1.3 EAP- Einstellungen

LANconfig: RADIUS- Server ▶ EAP



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ EAP

■ **PEAP- Vorgabe- Tunnel- Methode**

Bei der Verwendung von PEAP werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer TLS-Tunnel ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder ablehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem Verfahren, welches er gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

Mögliche Werte:

□ Keine, MD5, GTC, MSCHAPv2

Default:

□ MSCHAPv2

■ **Reauth- Periode**

Wenn der interne RADIUS- Server auf die Anfrage eines Clients mit einem ACCEPT antwortet (Verhandlung des Authentifizierungsverfahrens ist erfolgreich abgeschlossen), kann der RADIUS- Server dem Authenticator mitteilen, nach welcher Zeit (in Sekunden) er eine erneute Authentifizierung des Clients auslösen soll.

Mögliche Werte:

□ Max. 10 Ziffern

Default:

□ 0

Besondere Werte:

□ 0: Es wird kein Timeout an den RADIUS- Client übermittelt.

Diese Funktion wird nicht von jedem RADIUS- Client unterstützt.

■ **Retransmit- Timeout**

Wenn der interne RADIUS- Server auf die Anfrage eines Clients mit einem CHALLENGE antwortet (Verhandlung des Authentifizierungsverfahrens ist noch nicht abgeschlossen), kann der RADIUS- Server dem Authenticator mitteilen, wie lange (in Sekunden) er auf eine Antwort des Clients warten soll, bevor der CHALLENGE erneut zugestellt wird.

Mögliche Werte:

□ Max. 10 Ziffern.

Default:

□ 0

Besondere Werte:

□ 0: Es wird kein Timeout an den RADIUS- Client übermittelt.

Diese Funktion wird nicht von jedem RADIUS- Client unterstützt.

■ **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.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **TTLS- Vorgabe- Tunnel- Methode**

Bei der Verwendung von TTLS werden zwei Authentifizierungmethoden ausgehandelt. Zunächst wird über EAP ein sicherer TLS-Tunnel ausgehandelt. In diesem Tunnel wird dann wiederum ein zweites Authentifizierungverfahren ausgehandelt. Bei diesen Verhandlungen bietet der Server jeweils ein Verfahren an, welches der Client annehmen (ACK) oder ablehnen (NAK) kann. Lehnt der Client ab, schickt er dem Server einen Vorschlag mit einem Verfahren, welches er gerne nutzen würde. Ist das vom Client vorgeschlagene Verfahren im Server erlaubt, so wird es verwendet, ansonsten bricht der Server die Verhandlung ab.

Mit diesem Parameter wird das Verfahren festgelegt, das der Server den Clients als Authentifizierungverfahren im TLS-Tunnel anbieten soll. Durch diese Vorgabe können abgelehnte Vorschläge bei der Verhandlung vermieden und so die Verhandlung beschleunigt werden.

Mögliche Werte:

□ Keine, MD5, GTC, MSCHAPv2

Default:

□ MD5

■ **Tunnel- Server**

Realm als Verweis auf den Eintrag in der Tabelle der Weiterleitungs- Server, der für getunnelte TTLS bzw. PEAP Anfragen verwendet werden soll.

Mögliche Werte:

□ Max. 24 Zeichen

Default:

□ Leer

Wenn das Feld leer bleibt, übernimmt der lokale RADIUS-Server die Anfrage selbst. Das bedeutet, die innere und äußere EAP-Authentifizierung wird vom lokalen RADIUS-Server durchgeführt.

■ **Default-Methode**

Gibt an, welche Methode der RADIUS-Server dem Client außerhalb eines eventuellen TTLS/PEAP-Tunnels anbieten soll.

Mögliche Werte:

□ Keine, MD5, GTC, MSCHAPv2, TLS, TTLS, PEAP

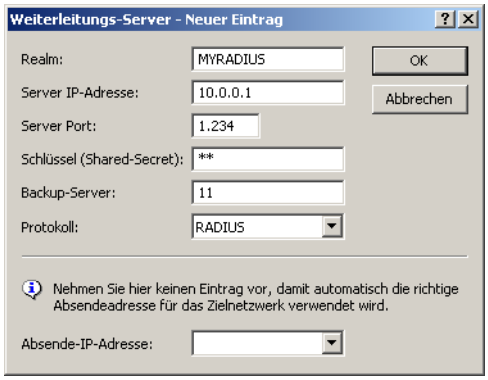
Default:

□ MD5

J.1.4 Tabelle der Weiterleitungs-Server

In der Tabelle der Weiterleitungs-Server werden bis zu 16 Realms mit den zugehörigen Weiterleitungs-Zielen eingetragen.

LANconfig: RADIUS-Server ▶ Weiterleitung ▶ Weiterleitungs-Server



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Weiterleit-Server

■ **Realm**

Zeichenkette, mit der das Weiterleitungs-Ziel identifiziert wird.

Mögliche Werte:

□ Max. 24 Zeichen

Default:

□ Leer

■ **IP-Adresse**

IP-Adresse des RADIUS-Servers, an den die Anfrage weitergeleitet werden soll.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ Leer

■ **Port**

Offener Port, über den mit dem Weiterleitungs-Server kommuniziert werden kann.

Mögliche Werte:

□ Max. 4 Ziffern

Default:

□ 0

■ **Secret**

Kennwort, das für den Zugang zum Weiterleitungs-Server benötigt wird.

Mögliche Werte:

□ Max. 32 Zeichen

Default:

□ Leer

■ **Loopback-Addr.**

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten 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

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.

■ **Protokoll**

Protokoll für die Kommunikation zwischen dem internen RADIUS-Server und dem Weiterleitungs-Server.

Mögliche Werte:

□ RADSEC, RADIUS, alle

Default:

□ RADIUS

■ **Backup**

Alternativer Weiterleitungs-Server, an den Anfragen weitergeleitet werden, wenn der erste Weiterleitungs-Server nicht erreichbar ist.

Mögliche Werte:

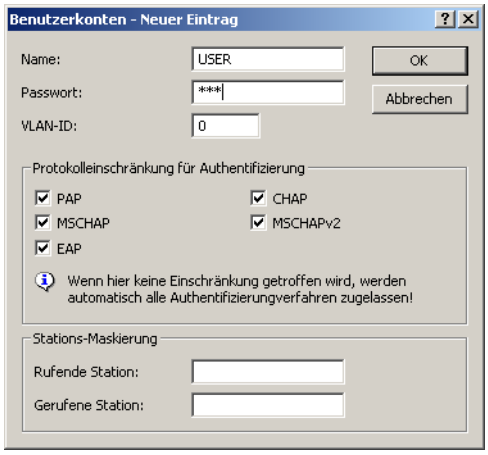
□ Max. 24 Zeichen

Default:

□ Leer

J.1.5 Tabelle der RADIUS-Benutzer

LANconfig: RADIUS-Server ▶ Allgemein ▶ RADIUS-Benutzerkonten



WEBconfig: Setup ▶ RADIUS ▶ Server ▶ Benutzer

■ **Benutzername**

Name des Benutzers.

Mögliche Werte:

□ Max. 48 Zeichen

Default:

- □ Leer

■ **Rufende-Station-Id-Maske**

Mit dieser Maske wird die Gültigkeit des Eintrags auf bestimmte IDs eingeschränkt, die von der rufenden Station (WLAN-Client) übermittelt wird. Bei der Authentifizierung über 802.1x wird die MAC-Adresse des rufenden Access Points im ASCII-Format (nur Großbuchstaben) übertragen, dabei werden Zeichenpaare durch einen Bindestrich getrennt (z. B. "00-10-A4-23-19-C0")

Mögliche Werte:

- □ Max. 48 Zeichen

Default:

- □ Leer

Besondere Zeichen:

- □ Mit dem * als Platzhalter können ganze Gruppen von IDs erfasst und als Maske definiert werden.

■ **Gerufene-Station-Id-Maske**

Mit dieser Maske wird die Gültigkeit des Eintrags auf bestimmte IDs eingeschränkt, die von der gerufenen Station (BSSID und SSID des Access Point) übermittelt wird. Bei der Authentifizierung über 802.11x werden MAC-Adressen (BSSID) des gerufenen Access Points 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")

Mögliche Werte:

- □ Max. 48 Zeichen

Default:

- □ Leer

Besondere Werte:

- □ Mit dem * als Platzhalter können ganze Gruppen von IDs erfasst und als Maske definiert werden. Mit der Maske "*:OFFICE1" wird z. B. ein Eintrag definiert, der für einen Client in der Funkzelle mit dem Namen "OFFICE1" gilt, egal über welchen Access Point der Client sich eingebucht hat. Auf diese Weise kann der Client von einem Access Point zum nächsten wechseln (Roaming) und jeweils mit den gleichen Authentifizierungsdaten arbeiten.

■ **Limitiere-Auth-Methoden**

Mit dieser Option können die für den Benutzer erlaubten Authentifizierungsverfahren eingeschränkt werden.

Mögliche Werte:

- □ PAP, CHAP, MS-CHAP, MS-CHAPv2, alle

Default:

- □ Leer

■ **Passwort**

Passwort des Benutzers.

Mögliche Werte:

- □ Max. 32 Zeichen

Default:

- □ Leer

■ **VLAN-Id**

Mit dieser Option kann dem Benutzer bei erfolgreicher Authentifizierung eine bestimmte VLAN-ID zugewiesen werden.

Mögliche Werte:

- □ 0 bis 4094

Default:

- □ 0

Besondere Werte:

- □ 0: sofern der SSID eine VLAN ID global zugewiesen wurde, wird diese verwendet.
- □ alle anderen Werte: Die benutzerspezifische VLAN ID überschreibt auch eine global definierte VLAN ID einer SSID.

J.2 Automatische IP-Adressverwaltung mit DHCP

Neu in LCOS 7.60:

- BOOTP: Zuweisung von festen IP-Adressen oder Boot-Images an bestimmte Stationen in Abhängigkeit vom IP-Netzwerk (ARF)

J.2.1 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, allen Rechnern im Netz „von Hand" diese Adressen 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 LANCOM-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

Der DHCP-Server entnimmt die IP-Adressen entweder aus einem frei definierten Adress-Pool oder ermittelt die Adressen selbstständig aus der eigenen IP-Adresse. Ein völlig unkonfiguriertes Gerät kann sogar im DHCP-Automodus die IP-Adressen für sich selbst und für die Rechner im Netz selbstständig festlegen. Im einfachsten Fall müssen Sie daher 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.

Die DHCP-Einstellungen können für jedes Netzwerk unterschiedlich sein. Im Zusammenhang mit dem Advanced Routing and Forwarding (ARF) können in den LANCOM-Geräten 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 das Gerät alternativ im DHCP-Client-Modus selbst die benötigten Adress-Informationen von dem anderen DHCP-Server beziehen.

Darüber hinaus kann ein LANCOM sowohl als DHCP-Relay-Agent als auch als DHCP-Relay-Server arbeiten.

- Als DHCP-Relay-Agent leitet ein LANCOM DHCP-Anfragen an einen weiteren DHCP-Server weiter.
- Als DHCP-Relay-Server kann ein LANCOM von DHCP-Relay-Agents weitergeleitete DHCP-Anfragen bearbeiten.

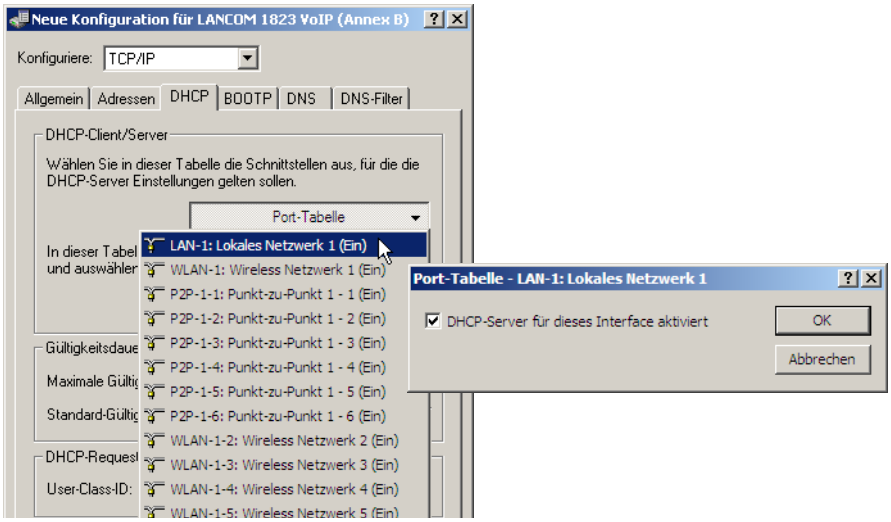
BOOTP

Über das Bootstrap-Protokoll (BOOTP) kann 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.

J.2.2 Konfiguration der DHCP-Parameter mit LANconfig

DHCP-Server für bestimmte logische Interfaces aktivieren oder deaktivieren

Der DHCP-Server kann für jedes logische Interface (z. B. LAN-1, WLAN-1, P2P-1-1 etc.) separat aktiviert oder deaktiviert werden. Wählen Sie dazu in der Port-Liste das entsprechende logische Interface und schalten Sie den DHCP-Server für dieses Interface ein oder aus. Die Parameter zur Aktivierung der Ports finden Sie in LANconfig im Konfigurationsbereich "TCP/IP" auf der Registerkarte "DHCP".



DHCP- Netzwerke konfigurieren

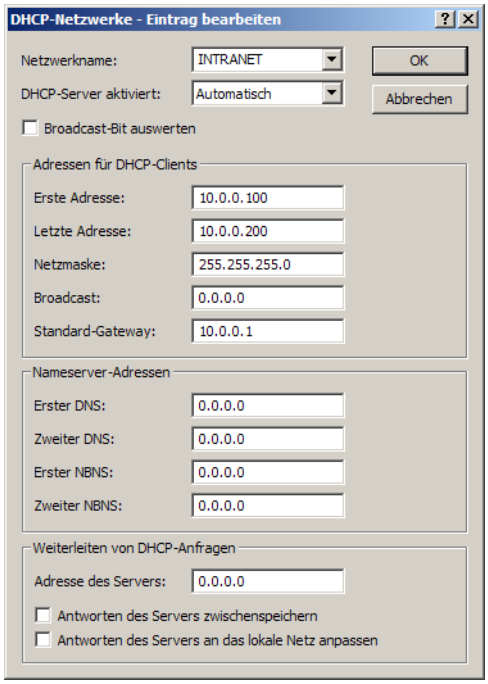
Für jedes im Gerät definierte IP- Netzwerk können die zugehörigen DHCP- Einstellungen separat festgelegt werden. Die Parameter zur Definition der DHCP- Netzwerke finden Sie in LANconfig im Konfigurationsbereich “TCP/IP” auf der Registerkarte “DHCP”.

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.

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.

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.



■ Auswahl des IP- Netzwerks

Wählen Sie aus, für welches IP- Netzwerk die folgenden DHCP- Einstellungen gelten sollen. Die Einstellungen für die IP- Netzwerke finden Sie in LANconfig im Konfigurationsbereich “TCP/IP” auf der Registerkarte “Allgemein”.

■ Betriebsmodus des DHCP- Servers einstellen

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'.

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.
- 'Auto': In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP- Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN- Rx/Tx- LED.
  - □ Wird mindestens ein anderer DHCP- Server gefunden, schaltet das Gerät seinen eigenen DHCP- Server aus. Ist für den LANCOM Router noch keine IP- Adresse konfiguriert, dann wechselt er in den DHCP- Client- Modus und bezieht eine IP- Adresse vom DHCP- Server. Damit wird u.a. verhindert, dass ein unkonfiguriertes 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 LANCOM Router deaktiviert.
- 'Client': Der DHCP- Server ist ausgeschaltet, das Gerät verhält sich als DHCP- Client und bezieht seine Adress- Informationen von einem anderen DHCP- Server im LAN.

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.

- 'Weiterleiten': Der DHCP- Server ist eingeschaltet, 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.

Ob der DHCP- Server letztendlich ein- oder ausgeschaltet ist, kann den DHCP- Statistiken entnommen werden.

Die Default- Einstellung für den Zustand ist 'Auto'.

■ Zuweisung von IP-Adressen

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.

■ Zuweisung der Netzmaske

Die Zuweisung der Netzmaske erfolgt analog zur Adresszuweisung. Wenn in DHCP-Einstellungen eine Netzmaske eingetragen ist, wird diese bei der Zuweisung verwendet. Ansonsten wird die Netzmaske aus dem IP-Netzwerk verwendet.

■ Zuweisung der Broadcast-Adresse

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 wird die zu verwendende Broadcast-Adresse in den DHCP-Einstellugnen eingetragen.

Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

■ Zuweisung des Standard-Gateways

Das LANCOM weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse in diesem Netzwerk als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway übertragen werden.

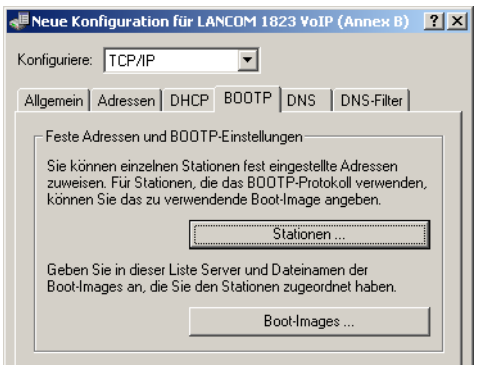
■ Zuweisung von DNS- und NBNS-Server

IP-Adressen der DNS- und NBNS-Nameserver, an den DNS- und NBNS-Anfragen weitergeleitet werden sollen.

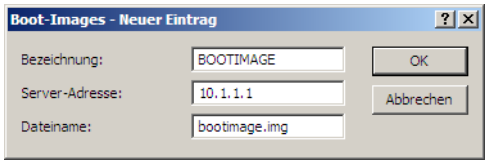
Ist bei den entsprechenden Feldern kein Server angegeben, so gibt der Router seine eigene IP-Adresse in diesem Netzwerk als DNS- bzw. NBNS-Adresse weiter, wenn der DNS-Server für dieses Netzwerk aktiviert ist. Ist der DNS-Server für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als DNS-Server übermittelt.

Zuweisung von festen IP-Adressen an bestimmte Stationen konfigurieren

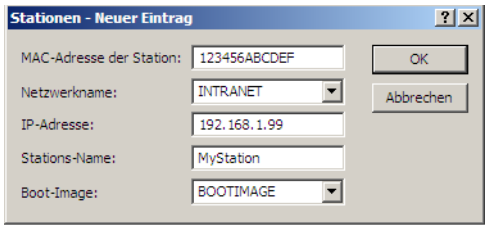
Die Parameter zur Konfiguration von BOOTP finden Sie in LANconfig im Konfigurationsbereich “TCP/IP” auf der Registerkarte “BOOTP”.



Optional: Definieren Sie in der Liste der Boot-Images ein Boot-Image, dass Sie einer Station zuweisen möchten.



Definieren Sie in der Liste der Stationen die MAC-Adresse einer Station, der Sie eine bestimmte IP-Adresse zuweisen möchten. Wählen Sie optional ein Boot-Image aus, das dieser Station zugewiesen werden soll. Wenn diese Adress-Zuweisung nur dann verwendet werden soll, wenn sich die Station in einem bestimmten IP-Netzwerk befindet, geben Sie zusätzlich das entsprechende IP-Netzwerk an.



J.2.3 Konfiguration der DHCP-Parameter mit Telnet oder WEBconfig

Allgemeine DHCP-Einstellungen

- **User-Class-Identifer**
  - □ Pfad: Setup/DHCP

  Der DHCP-Client im LANCOM 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, z.B. 'LANCOM L-54ag'. Die Vendor-Class-ID wird immer übertragen. Der User-Class-Identifier (DHCP-Option 77) gibt einen benutzerdefinierten String an. Die User-Class-ID wird nur übertragen, wenn der Benutzer einen Wert konfiguriert hat.

  Mögliche Werte:

  - □ Max. 63 Zeichen

  Default:

  - □ Leer
- **Default-Gueltigkeit-Minuten**
  - □ Pfad: Setup/DHCP

  Wenn ein Client eine IP-Adresse anfordert, ohne eine Gültigkeitsdauer für diese Adresse zu fordern, wird dieser Adresse als Gültigkeistdauer der hier eingestellte Wert zugewiesen.

  Mögliche Werte:

  - □ Max. 5 Zeichen

  Default:

  - □ 500
- **Max.-Gueltigkeit-Minuten**
  - □ Pfad: Setup/DHCP

  Wenn ein Client eine IP-Adresse bei einem DHCP-Server anfordert, kann er eine Gültigkeitsdauer für diese Adresse anfordern. Dieser Wert kontrolliert die maximale Gültigkeitsdauer, die ein Client anfordern darf.

  Mögliche Werte:

  - □ Max. 5 Zeichen

  Default:

  - □ 6000

Alias-Liste

In der Alias-Liste werden die Bezeichnungen für die Boot-Images definiert, über welche die Images in der Host-Tabelle referenziert werden können.

- □ Pfad: Setup/DHCP/Alias-Liste

- **Image-Alias**
  Geben Sie eine beliebige Bezeichnung für dieses Boot-Image ein. Diese Bezeichnung wird verwendet, wenn Sie in der Stations-Liste ein Boot-Image einer bestimmten Station zuordnen.
  Mögliche Werte:
  - □ Max. 16 Zeichen

  Default:
  - □ Leer
- **Image-Server**
  Geben Sie die IP-Adresse des Servers ein, der das Boot-Image zur Verfügung stellt.
  Mögliche Werte:
  - □ Gültige IP-Adresse.

  Default:
  - □ 0.0.0.0
- **Image-File**
  Geben Sie den Namen der Datei auf dem Server an, die das Boot-Image enthält.
  Mögliche Werte:
  - □ Max. 60 Zeichen

  Default:
  - □ Leer

DHCP-Tabelle

Die DHCP-Tabelle gibt eine Übersicht über die in den IP-Netzwerken verwendeten IP-Adressen. Bei der DHCP-Tabelle handelt es sich um eine reine Status-Tabelle, in der keine Parameter konfiguriert werden können.

- □ Pfad: Setup/DHCP/DHCP-Tabelle

- **IP-Adresse**
  IP-Adresse, die von der Station verwendet wird.
- **MAC-Adresse**
  MAC-Adresse der Station.
- **Timeout**
  Gültigkeitsdauer der Adresszuweisung in Minuten.
- **Rechnername**
  Name der Station, sofern dieser ermittelt werden konnte.
- **Typ**
  Im Feld 'Typ' wird angegeben, wie die Adresse zugewiesen wurde. Das Feld kann die folgenden Werte annehmen:
  - □ neu: Der Rechner hat zum ersten Mal angefragt. Der DHCP-Server überprüft die Eindeutigkeit der Adresse, die dem Rechner zugewiesen werden soll.
  - □ unbek.: 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.
  - □ stat.: 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.
  - □ dyn.: Der DHCP-Server hat dem Rechner eine Adresse zugewiesen.
- **LAN-Ifc**
  Logische Interface, über das die Station mit dem Gerät verbunden ist.
- **Ethernet-Port**
  Physikalisches Interface, über das die Station mit dem Gerät verbunden ist.
- **VLAN-ID**
  Die von dieser Station verwendete VLAN-ID.
- **Netzwerkname**
  Name des IP-Netzwerks, in dem sich die Station befindet.

Host-Tabelle

Über das Bootstrap-Protokoll (BOOTP) kann einer Station beim Starten eine IP-Adresse und weitere Parameter übermittelt werden. Dazu wird die MAC-Adresse der Station in die Host-Tabelle eingetragen.

□ Pfad: Setup/DHCP/Hosts

■ **MAC-Adresse**

Geben Sie hier die MAC-Adresse der Station ein, der eine IP-Adresse zugewiesen werden soll.

Mögliche Werte:

□ Gültige MAC-Adresse.

Default:

□ Leer

■ **Netzwerkname**

Hier wird der Name eines konfigurierten IP-Netzwerks eingetragen. Nur wenn sich die anfragende Station in diesem IP-Netzwerk befindet, wird der Station die für die MAC-Adresse definierte IP-Adresse zugewiesen.

Mögliche Werte:

□ Max. 16 Zeichen

Default:

□ Leer

Besondere Werte:

□ Leer: Passt die in diesem Eintrag definierte IP-Adresse zu dem Adresskreis des IP-Netzwerks, in dem sich die anfragende Station befindet, dann wird die IP-Adresse zugewiesen.

Befindet sich die anfragende Station in einem IP-Netzwerk, zu dem es keinen passenden Eintrag in der Host-Tabelle gibt, so wird der Station dynamisch eine IP-Adresse aus dem IP-Adress-Pool des jeweiligen IP-Netzwerks zugewiesen.

■ **IP-Adresse**

Geben Sie hier die IP-Adresse der Station ein, die der Station zugewiesen werden soll.

Mögliche Werte:

□ Gültige IP-Adresse.

Default:

□ 0.0.0.0

■ **Rechnername**

Geben Sie hier einen Namen ein, mit dem die Station identifiziert werden soll. Wenn eine Station ihren Namen nicht übermittelt, verwendet das Gerät den hier eingetragenen Namen.

Mögliche Werte:

□ Max. 30 Zeichen

Default:

□ Leer

■ **Image-Alias**

Wenn die Station das BOOTP-Protokoll verwendet, dann können Sie ein Boot-Image auswählen, über das die Station ihr Betriebssystem laden soll.

Mögliche Werte:

□ Max. 16 Zeichen

Default:

□ Leer

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.

Netzliste

In dieser Tabelle werden die DHCP-Einstellungen zu den IP-Netzwerken definiert.

□ Pfad: Setup/DHCP/Netzliste

■ **Netzwerkname**

Name des Netzwerks, für das die Einstellungen des DCHP-Servers gelten sollen.

Mögliche Werte:

□ Name eines definierten IP-Netzwerks, max. 16 Zeichen

Default:

□ Leer

■ **DHCP-Server aktiviert**

Betriebsart des DHCP-Servers für dieses Netzwerk. Je nach Betriebsart kann sich der DHCP-Server selbst aktivieren bzw. deaktivieren. Ob der DHCP-Server aktiv ist, kann den DHCP-Statistiken entnommen werden.

Mögliche Werte:

□ Nein: Der DHCP-Server ist dauerhaft abgeschaltet.

□ Automatisch: In diesem Zustand sucht das Gerät regelmäßig im lokalen Netz nach anderen DHCP-Servern. Diese Suche ist erkennbar durch ein kurzes Aufleuchten der LAN-Rx/Tx-LED.

Wird mindestens ein anderer DHCP-Server gefunden, schaltet das Gerät seinen eigenen DHCP-Server aus. Ist für den LANCOM Router noch keine IP-Adresse konfiguriert, dann wechselt er in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server. Damit wird u.a. verhindert, dass ein unkonfiguriertes 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 LANCOM Router deaktiviert.

□ 'Ja': 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 für das Netzwerk 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.

□ 'Anfragen Weiterleiten': Der DHCP-Server ist eingeschaltet, 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 (Betriebsart DHCP-Relay-Agent).

Default:

□ Automatisch

Verwenden Sie die Einstellung "Ja" nur dann, wenn sichergestellt ist, dass kein anderer DHCP-Server im LAN aktiv ist.

Verwenden Sie die Einstellung "Client-Modus" nur dann, wenn sichergestellt ist, das ein anderer DHCP-Server im LAN aktiv ist und die Zuweisung der IP-Adress-Informationen übernimmt.

■ **Broadcast-Bit auswerten**

Wählen Sie hier, ob das von den Clients gemeldete Broadcast-Bit ausgewertet wird oder nicht. Wenn das Bit nicht ausgewertet wird, werden alle DHCP-Nachrichten als Broadcast versendet.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Erste Adresse**

Erste IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die erste freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

■ **Letzte Adresse**

Letzte IP-Adresse des Adressbereiches, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die letzte freie IP-Adresse aus diesem Netzwerk (wird bestimmt aus Netzadresse und Netzmaske).

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

■ **Netzmaske**

Zugehörige Netzmaske für den Adressbereich, der den Clients zur Verfügung steht. Wenn hier keine Adresse eingetragen ist, dann verwendet der DHCP-Server die Netzmaske aus dem zugehörigen Netzwerk.

Mögliche Werte:

□ Gültige IP-Netzmaske

Default:

□ 0.0.0.0

■ **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 wird die zu verwendende Broadcast-Adresse im DHCP-Modul eingetragen.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Broadcast-Adresse wird automatisch ermittelt.

Die Änderung der Voreinstellung für die Broadcast-Adresse wird nur für erfahrene Netzwerk-Spezialisten empfohlen. Eine Fehlkonfiguration in diesem Bereich kann zu unerwünschten, kostenpflichtigen Verbindungsaufbauvorgängen führen!

■ **Standard-Gateway**

Der LANCOM weist dem anfragenden Rechner standardmäßig seine eigene IP-Adresse als Gateway-Adresse zu. Falls erforderlich, kann durch den Eintrag einer entsprechende IP-Adresse auch ein anderes Gateway übertragen werden.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Die IP-Adresse des LANCOMs in diesem Netzwerk wird als Gateway übermittelt.

■ **Erster DNS**

IP-Adresse des DNS-Nameservers, an den DNS-Anfragen weitergeleitet werden sollen.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Die IP-Adresse des LANCOMs in diesem Netzwerk wird als DNS-Server übermittelt, wenn der DNS-Server für dieses Netzwerk aktiviert ist. Ist der DNS-Server für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als DNS-Server übermittelt.

■ **Zweiter DNS**

IP-Adresse des Backup-DNS-Nameservers, an den DNS-Anfragen weitergeleitet werden sollen, wenn der erste Nameserver ausfällt.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Die IP-Adresse aus den globalen TCP/IP-Einstellungen wird als Backup-DNS-Server übermittelt.

■ **Erster NBNS**

IP-Adresse des NetBIOS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Die IP-Adresse des LANCOMs in diesem Netzwerk wird als NBNS-Server übermittelt, wenn der NetBIOS-Proxy für dieses Netzwerk aktiviert ist. Ist der NetBIOS-Proxy für dieses Netzwerk nicht aktiv, so wird die IP-Adresse aus den globalen TCP/IP-Einstellungen als NBNS-Server übermittelt.

■ **Zweiter NBNS**

IP-Adresse des Backup-NBNS-Nameservers, an den NBNS-Anfragen weitergeleitet werden sollen, wenn der erste Nameserver ausfällt.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

Besondere Werte:

□ 0.0.0.0: Die IP-Adresse aus den globalen TCP/IP-Einstellungen wird als Backup-NBNS-Server übermittelt.

■ **Adresse des Servers**

Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

Mögliche Werte:

□ Gültige IP-Adresse

Default:

□ 0.0.0.0

■ **Antworten des Servers zwischenspeichern**

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers im LANCOM Router gespeichert werden. Spätere Anfragen können dann vom LANCOM Router selbst beantwortet werden. Diese Option ist nützlich, wenn der übergeordnete DHCP-Server nur über eine kostenpflichtige Verbindung erreicht werden kann.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

■ **Antworten des Servers an das lokale Netz anpassen**

Mit dieser Option können die Antworten des übergeordneten DHCP-Servers an das lokale Netzwerk angepasst werden. Bei aktivierter Anpassung ersetzt ein LANCOM in den Antworten des übergeordneten DHCP-Servers folgende Einträge durch seine eigene Adresse (bzw. lokal konfigurierte Adressen):

□ Gateway

□ Netzmaske

□ Broadcast-Adresse

□ DNS-Server

□ NBNS-Server

□ Server-ID

Diese Option ist sinnvoll, wenn der übergeordnete DHCP-Server keine getrennte Konfiguration für DHCP-Clients in einem anderen Netzwerk zulässt.

Mögliche Werte:

□ Ja, Nein

Default:

□ Nein

Port-Tabelle

In der Port-Tabelle wird der DHCP-Server für die jeweiligen logischen Interfaces des Geräts freigegeben.

□ Pfad: Setup/DHCP/Ports

■ **Port**

Auswahl des logischen Interfaces, für das der DHCP-Server aktiviert bzw. deaktiviert werden soll.

Mögliche Werte:

□ Auswahl aus der Liste der logischen Interfaces in diesem Gerät, z. B. LAN-1, WLAN-1, P2P-1-1 etc.

Default:

□ N/A

■ **DHCP-freigeben**

Aktiviert bzw. deaktiviert den DHCP-Server für das gewählte logische Interface.

Mögliche Werte:

□ Ja, Nein

Default:

□ Ja

Zusaetzliche-Optionen

Mit den DHCP-Optionen können zusätzliche Konfigurationsparameter an die Stationen übertragen werden. Der Vendor-Class-Identifier (DHCP-Option 60) zeigt so z. B. den Gerätetyp an. In dieser Tabelle werden zusätzliche Optionen für den DHCP-Betrieb definiert.

□ Pfad: Setup/DHCP/Zusaetzliche-Optionen

■ **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. Eine vollständige Liste aller DHCP-Optionen finden Sie im RFC 2132 – DHCP Options and BOOTP Vendor Extensions der Internet Engineering Task Force (IETF).

Mögliche Werte:

□ Max. 3 Zeichen

Default:

□ Leer

■ **Netzwerkname**

Name des IP-Netzwerks, in dem diese DHCP-Option verwendet werden soll.

Mögliche Werte:

□ Auswahl aus der Liste der definierten IPNetzwerke, max. 16 Zeichen.

Default:

□ Leer

Besondere Werte:

□ Leer: Wird kein Netzwekname angegeben, so wird die in diesem Eintrag definierte DHCP-Option in allen IP--Netzwerken verwendet.

■ **Options-Wert**

In diesem Feld wird der Inhalt der DHCP-Option definiert. Für die Option "17" wird hier z. B. der Pfad zu einem Boot-Image eingetragen, über welches ein PC ohne eigene Festplatte über BOOTP sein Betriebssystem beziehen kann.

Mögliche Werte:

□ String aus max. 128 Zeichen

Default:

□ Leer

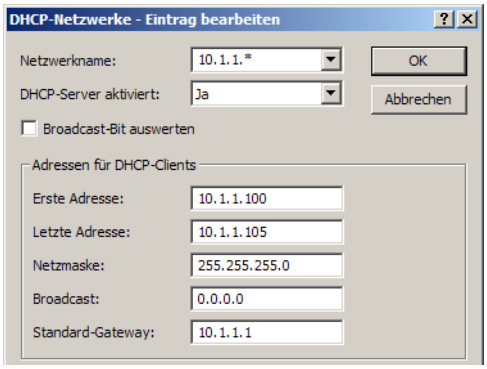
Die mögliche Länge des Optionswertes hängt von der gewählten Optionsnummer ab. Der RFC 2132 listet für jede Option ein zulässige Länge auf.

10.2.4 DHCP- Relay- Server

Ein LANCOM kann nicht nur DHCP-Anfragen an einen übergeordneten DHCP-Server weiterleiten, es kann auch selbst als zentraler DHCP-Server fungieren (DHCP-Relay-Server).

Um einen LANCOM 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 den LANCOM als übergeordneten DHCP-Server verwenden, dann kann die Zuweisung von IP-Adressen und Standard-Gateway an die Clients so erfolgen:



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.

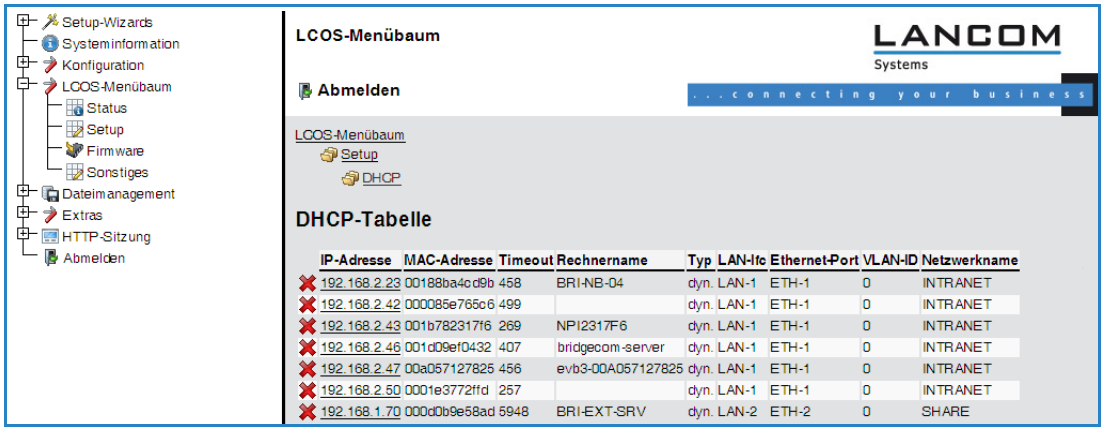
J.2.5 Konfiguration der Stationen

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.

J.2.6 IP-Adressen im LAN überprüfen

Eine Übersicht über die IP-Adressen im LAN gibt die DHCP-Tabelle (WEBconfig: Setup/DHCP/Tabelle-DHCP). Sie zeigt die zugewiesene bzw. verwendete IP-Adresse, die MAC-Adresse, die Gültigkeitsdauer, den Namen des Rechners (falls vorhanden) sowie den Typ der Adresszuweisung.



K Sonstige Änderungen

K.1 Zugangslisten mit Routing-Tags

K.1.1 Einleitung

Die LANCOM-Geräte verwenden verschiedene Zugangslisten, um den Zugriff auf bestimmte Funktionen gezielt auf einen definierten Kreis von Workstations oder Netzwerken zu beschränken. Diese Zugangslosten werden für folgende Module verwendet:

- TCP/IP: Konfigurationszugang zum Gerät über TCP/IP
- LANCAPI: Nutzung der LANCAPI-Funktion
- Drucker: Nutzung des am Gerät angeschlossenen Druckers

In der jeweiligen Zugangsliste wird mit einer IP-Adresse und einer Netzmaske der Bereich der zugelassenen Workstations definiert.

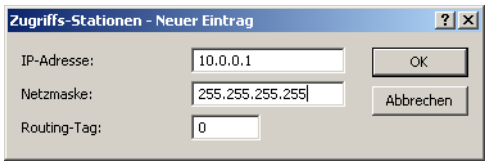
Zusätzlich kann optional ein Routing-Tag angegeben werden, mit dem nur die Stationen aus dem entsprechenden IP-Netzwerk (siehe Advanced Routing and Forwarding) Zugriff auf die Funktion erhalten. Die Angabe von Routing-Tags in der Zugangsliste ist z.B. dann sinnvoll, wenn in einer Netzstruktur mehrere IP-Netzwerke mit dem gleichen IP-Adresskreis arbeiten, die über Routing-Tags getrennt werden.

K.1.2 Konfiguration der Zugangslisten

LANconfig: Management ▶ Admin ▶ Zugriffs-Stationen

LANconfig: CAPI ▶ Optionen ▶ Zugangsliste

LANconfig: Drucker ▶ Allgemein ▶ Zugangsliste



WEBconfig: Setup ▶ TCP-IP ▶ Zugangs-Liste

WEBconfig: Setup ▶ LANCAPI ▶ Zugangs-Liste

WEBconfig: Setup ▶ Drucker ▶ Zugangs-Liste

- **IP-Adresse**

  Geben Sie hier die IP-Adresse der Station ein, die Zugriff auf die Funktion erhalten soll.

  Mögliche Werte:

  □ Gültige IP-Adresse.

  Default:

  □ 0.0.0.0

- **IP-Netzmaske**

  Geben Sie hier die IP-Netzmaske des Netzwerks ein, das Zugriff auf die Funktion erhalten soll. Wenn Sie nur eine einzelne Station mit der angegebenen IP-Adresse freischalten wollen, geben Sie 255.255.255.255 ein. Wenn Sie ein ganzes IP-Netz freigeben wollen, geben Sie die zugehörige Netzmaske ein.

  Mögliche Werte:

  □ Gültige IP-Netzmaske.

  Default:

  □ 0.0.0.0

- **Routing-Tag**

  Geben Sie hier das Routing-Tag des Netzwerks ein, das Zugriff auf die Funktion erhalten soll.

  Mögliche Werte:

  □ 0 bis 65535

  Default:

  □ 0

  Besondere Werte:

- □ 0: Erlaubt den Zugriff auf diese Funktion für alle Routing-Tags, die Zugriffsprüfung erfolgt nur anhand der IP-Adresse.