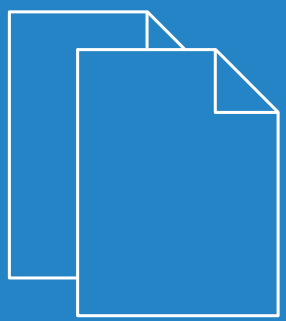
SICHER. **VERNETZT.**

LCOS 10.12

Addendum



LANCOM Systems

Inhalt

1 Addendum zur LCOS-Version 10.12

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.12 gegenüber der vorherigen Version.

2 WLAN-Management

2.1 RADIUS

2.1.1 Erreichbarkeitsprüfung für externe RADIUS-Server

Ab LCOS-Version 10.12 können Sie mit diesem Feature überwachen, ob ein RADIUS-Server erreichbar ist. Hierzu werden regelmäßig RADIUS-Requests gesendet, es wird also geprüft, ob der RADIUS-Dienst funktional ist.

Die Überprüfung kann folgendermaßen geschehen:

- durch das Senden von Status-Server-Requests (DEFAULT). Diese dienen speziell der Erreichbarkeitsüberprüfung von RADIUS-Diensten. Sie werden aber nicht von allen RADIUS-Servern unterstützt (ein Positivbeispiel ist FreeRADIUS).
- durch das Senden von Access-Requests ("Dummy-Requests"). Diese Methode sollte nur verwendet werden, wenn der Server keine Status-Server-Requests unterstützt.

Unter **Setup** > **RADIUS** > **Supervision-Servers** > **Profiles** können Sie Supervisionsprofile anlegen. Diese beinhalten, nach welcher Methode die Erreichbarkeitsprüfung erfolgt, in welchem Intervall (in Sekunden) die Prüfung erfolgt und welche Attribute einem Access-Request angefügt werden (es muss mindestens ein Benutzername für den Dummy-Request enthalten sein; für Status-Server-Requests hingegen ist kein zusätzliches Attribut erforderlich). Im Default ist folgendes Profil bereits enthalten:

```
root@LCS_L452_Office:/Setup/RADIUS/Supervision-Servers/Profiles/DEFAULT
> ls -a
[1.3.6.1.4.1.2356.11][2.25.21.1.1][column][7.68.69.70.65.85.76.84]

[  1] Name              INFO:       DEFAULT
[  2] Type              VALUE:      Status-Server
[  3] Attributes        VALUE:
[  4] Request-Interval  VALUE:      60
```

Es folgt ein Beispiel-Profil, um Access-Requests zu verwenden:

```
root@LCS_L452_Office:/Setup/RADIUS/Supervision-Servers/Profiles/DUMMY
> ls -a
[1.3.6.1.4.1.2356.11][2.25.21.1.1][column][5.68.85.77.77.89]

[  1] Name              INFO:       DUMMY
[  2] Type              VALUE:      Dummy-Request
[  3] Attributes        VALUE:      User-name=dummyuser
[  4] Request-Interval  VALUE:      60
```

Hier ist auch zu sehen, dass der User-Name als Attribut gesetzt wurde. Bitte achten Sie darauf, einen Benutzernamen zu verwenden, der dem RADIUS-Server nicht bekannt ist - dies vermeidet, dass eine reguläre Anmeldung am RADIUS-Server durchgeführt wird. Die "Anmeldeversuche" durch die Überwachung werden so nur als fehlgeschlagene Logins gezählt.

Nun kann auf ein in dieser Tabelle enthaltenes Profil referenziert werden. Dies ist für die für 802.1X verwendeten RADIUS-Server möglich, hier ein Beispieleintrag in der entsprechenden Tabelle:

```
root@LCS_L452_Office:/Setup/IEEE802.1x/RADIUS-Server/FREERADIUS
> ls -a
[1.3.6.1.4.1.2356.11][2.30.3.1][column][10.70.82.69.69.82.65.68.73.85.83]

[  1] Name              INFO:       FREERADIUS
[  8] Host-Name         VALUE:      192.168.1.2
[  3] Port              VALUE:      1812
[  4] Secret            VALUE:      *
```

```
[  6] Loopback-Addr.    VALUE:
[  7] Protocol          VALUE:      RADIUS
[  9] Attribute-Values  VALUE:
[ 10] Sup.-Profile      VALUE:      DEFAULT
[  5] Backup            VALUE:
```

Der hier angegebene RADIUS-Server wird mittels des Supervision-Profiles "DEFAULT" überwacht. Erfolgt für "Sup.-Profile" ein Eintrag, der keine Entsprechung in den Supervision-Profiles hat, wird automatisch das DEFAULT-Profil verwendet. Ist "Sup.-Profile" leer, wird keine Überwachung durchgeführt.

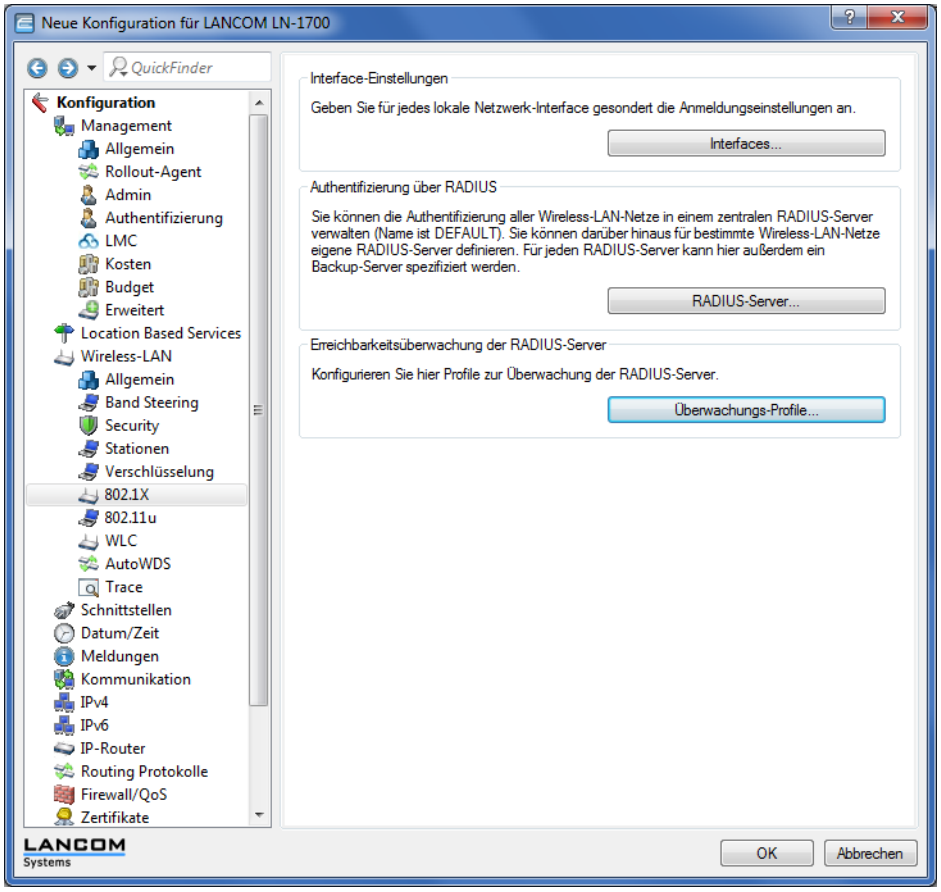
Die so überwachten RADIUS-Server sowie deren Status können Sie in folgender Tabelle einsehen:

```
root@LCS_L452_Office:/Status/TCP-IP/RADIUS-Supervision-Servers/Servers
> ls -a
[1.3.6.1.4.1.2356.11][1.9.14.1]

Index      Server-Hostname        Port  Loopback-Address  Protocol  State
[1]        [2]                    [3]    [4]              [5]        [6]
==========-----------------------------------------------------------------
1          192.168.1.2            1812                    RADIUS      Up
2          192.168.1.254          1812                    RADIUS      Timeout
```

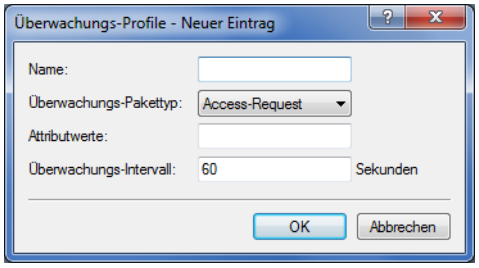
Die Statustabelle ist auch unter folgendem Pfad zu erreichen: **Status** > **SLA-Monitor** > **RADIUS** > **Servers**.

Überwachungsprofile in LANconfig

Navigieren Sie zu **Wireless-LAN** > **802.1X** > **Erreichbarkeitsüberwachung der RADIUS-Server**.



Die Tabelle **Überwachungsprofile** bietet Ihnen folgende Konfigurationsmöglichkeiten:



Name

Enthält den Namen des Überwachungs-Profils

Überwachungs-Pakettyp

Hier haben sie die Wahl zwischen folgenden Typen:

Access-Request (Default)

Dieser Typ sollte nur verwendet werden, wenn der Server keine Status-Server-Requests unterstützt.

Status-Server

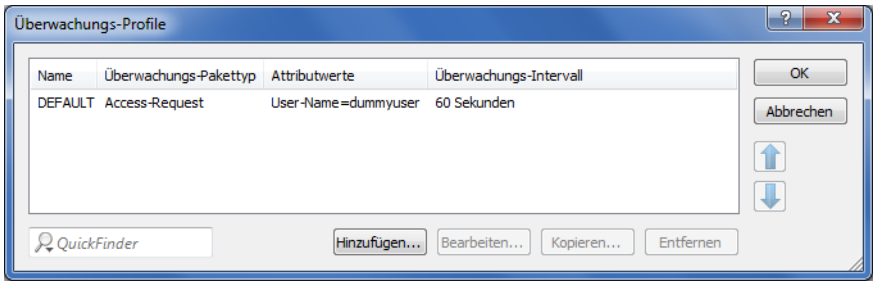
Dieser Typ dient speziell der Erreichbarkeitsüberprüfung von RADIUS-Diensten, wird aber nicht von allen RADIUS-Servern unterstützt.

Attributwerte

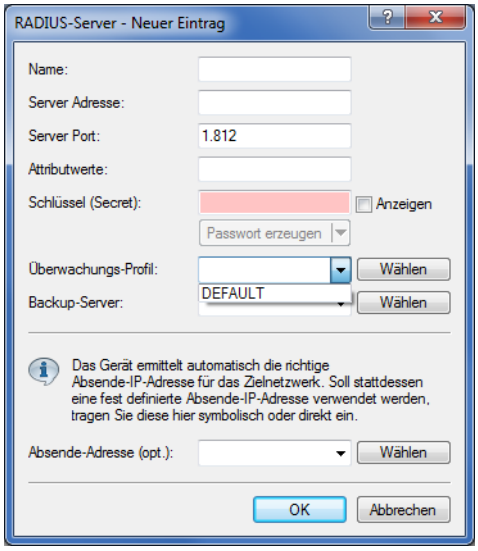
Ein Attribut ist nur für Access-Requests erforderlich. Für Status-Server-Requests ist es entbehrlich.

Überwachungs-Intervall

Das Überwachungs-Intervall in Sekunden (Default: 60)



Das neu angelegte Überwachungsprofil (hier: DEFAULT) steht ab sofort auch der Tabelle **RADIUS-Server** zur Verfügung:



Ergänzungen im Status-Menü

Servers

Dieser Eintrag enthält die Statuswerte für Servers.

SNMP-ID:

1.36.2.1

Pfad Telnet:

Status > **SLA-Monitor** > **RADIUS**

Mögliche Werte:

0

Unknown

Der Status des Servers ist nicht bekannt, weil entweder noch keine Anfrage an ihn abgeschickt wurde oder aber keine valide Antwort erhalten wurde.

1

Up

Der Server hat auf eine Anfrage mit einer validen RADIUS-Antwort reagiert und wird daher als operational angenommen.

2

DNS-Error

Das Gerät kann den Namen des DNS-Servers nicht auflösen.

3

Authenticator-Mismatch

Das Gerät hat zwar eine Antwort vom Server erhalten, allerdings mit einer fehlerhaften Authentifizierung. Dies verweist auf ein nicht übereinstimmendes Shared Secret. Beachten Sie, dass dieser Status nur dann auftreten kann, wenn zu Testzwecken unmittelbar nach einer solchen Nicht-Übereinstimmung Zugriffsanfragen an den Server gesendet werden, da Status-Server-Pakete ein

Message-Authenticator-Attribut enthalten und im Falle einer Nicht-Übereinstimmung still verworfen werden. Nichtsdestotrotz stellt eine Nicht-Übereinstimmung eines Shared Secrets keinesfalls eine zeitweise Nicht-Erreichbarkeit, sondern eine andauernde Fehlkonfiguration dar.

4

Host-Unreachable

Der Server ist nicht via IP erreichbar.

5

Port-Unreachable

Der Server ist zwar via IP erreichbar, jedoch verwendet kein RADIUS-Server den eingestellten Port.

6

Timeout

Es ist nicht möglich, die IP-Adresse des Servers zu routen.

Ergänzungen im Setup-Menü

Erreichbarkeitsprüfung

In diesem Verzeichnis konfigurieren Sie die Erreichbarkeitsprüfung.

Die Überwachung erfolgt durch Senden von Status-Server-Requests oder alternativ Access-Requests.

SNMP-ID:

2.25.21

Pfad Telnet:

Setup > **RADIUS**

Profile

Hier erstellen Sie Überwachungsprofile für die Erreichbarkeit von RADIUS-Servern.

SNMP-ID:

2.25.21.1

Pfad Telnet:

Setup > **RADIUS** > **Erreichbarkeitsprüfung**

Name

Hier können Sie einen benutzerdefinierten Namen für das Überwachungsprofil vergeben.

SNMP-ID:

2.25.21.1.1

Pfad Telnet:

Setup > **RADIUS** > **Erreichbarkeitsprüfung** > **Profile**

Mögliche Werte:

Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

DEFAULT

Typ

Hier legen Sie fest, ob zur Erreichbarkeitsprüfung Status-Server- oder Access-Requests an den RADIUS-Server gesendet werden.

SNMP-ID:

2.25.21.1.2

Pfad Telnet:

Setup > **RADIUS** > **Erreichbarkeitsprüfung** > **Profile**

Mögliche Werte:

Access-Request
Status-Server

Default-Wert:

Access-Request

Attribute

Wird die Erreichbarkeitsprüfung mittels Access-Requests durchgeführt, so können hier die Attribute des Access-Requests mittels einer kommaseparierten Liste im Format **Attribut1=Wert1,Attribut2=Wert2,...** übergeben werden. Für die Erreichbarkeitsprüfung mittels Access-Request ist mindestens die Angabe des Attributs "User-Name" erforderlich, z. B. **User-Name=dummyuser**.

Für Status-Server-Requests ist kein Attribut erforderlich.

SNMP-ID:

2.25.21.1.3

Pfad Telnet:

Setup > **RADIUS** > **Erreichbarkeitsprüfung** > **Profile**

Mögliche Werte:

Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Anfrage-Intervall

Hier legen Sie das Intervall in Sekunden fest, innerhalb dessen die Erreichbarkeit des RADIUS-Servers überprüft wird.

SNMP-ID:

2.25.21.1.4

Pfad Telnet:

Setup > **RADIUS** > **Erreichbarkeitsprüfung** > **Profile**

Mögliche Werte:

`[0-9]`

Default-Wert:

60

2.2 Koordinierte Kanalwahl Wireless ePaper

Ab LCOS-Version 10.12 steht Ihnen die koordinierte Kanalwahl für Wireless ePaper zur Verfügung.

Dieses Feature benötigen Sie insbesondere dann, wenn Sie mit mehreren Wireless ePaper Access Points innerhalb eines Standorts arbeiten.

Da jeder AP einen eigenen ePaper-Kanal benötigt, darf es nicht zu Kollisionen / Mehrfachbelegungen kommen.

Daher ermitteln die ePaper-APs innerhalb einer Broadcast-Domain automatisch über ein TCP-basiertes Protokoll, welches in einer Multicast-Gruppe übertragen wird, benachbarte ePaper-APs. Aus diesen APs wird automatisch ein Master-AP bestimmt. Die übrigen APs werden zu Slave-APs. Fällt der Master-AP aus, wird automatisch einer der Slave-APs zum Master-AP ernannt.

Die Slave-APs übermitteln dem Master-AP regelmäßig eine Beurteilung des aktuellen ePaper-Kanals. Der Master entscheidet daraufhin unter Berücksichtigung der Beurteilungen sämtlicher Slaves, ob ein Kanalwechsel des Slaves stattfinden muss oder nicht.

Der ePaper-AP erstellt eine Beurteilung aller ePaper-Kanäle. Dabei wird sowohl der lokal verwendete WLAN-Kanal (den der ePaper-Kanal nicht überlappen sollte) berücksichtigt als auch, ob es sich bei dem ePaper-Kanal um einen bevorzugten Kanal handelt.

Bevorzugte Kanäle sind: 3,5,8,9 und 10.

Anhand der erhaltenen Kanalbeurteilungen wird eine Optimierung der ePaper-Kanäle folgendermaßen erreicht:

Der Master-AP wählt aus den noch nicht vergebenen Kanälen denjenigen mit der besten Bewertung aus und weist ihn dem ePaper-AP mit der niedrigsten ePaper-AP-ID zu (der Master weist sich selbst ebenfalls einen Kanal zu). Dies wird sukzessive für alle ePaper-APs fortgeführt.

Bei einer Neuverteilung wird ein Kanal nur gewechselt, wenn die Bewertung des konkurrierenden Kanals um einen konfigurierbaren Threshold besser ist. Auf diese Weise werden unnötige Kanalwechsel vermieden.

Gibt es im Netzwerk ePaper-APs mit statisch zugewiesenem ePaper-Kanal, so kann die koordinierte Kanalwahl trotzdem durchgeführt werden. Ist diese auch auf dem AP mit statischem Kanal eingeschaltet, wird der Master bei der Kanalzuweisung beachten, dass dieser Kanal bereits vergeben ist und ihn keinem anderen AP zuweisen.

Das Status-Menü des Features Wireless ePaper wurde um eine Peer-Tabelle erweitert. In dieser werden die über die Kanal-Koordinierung erfassten APs aufgelistet.

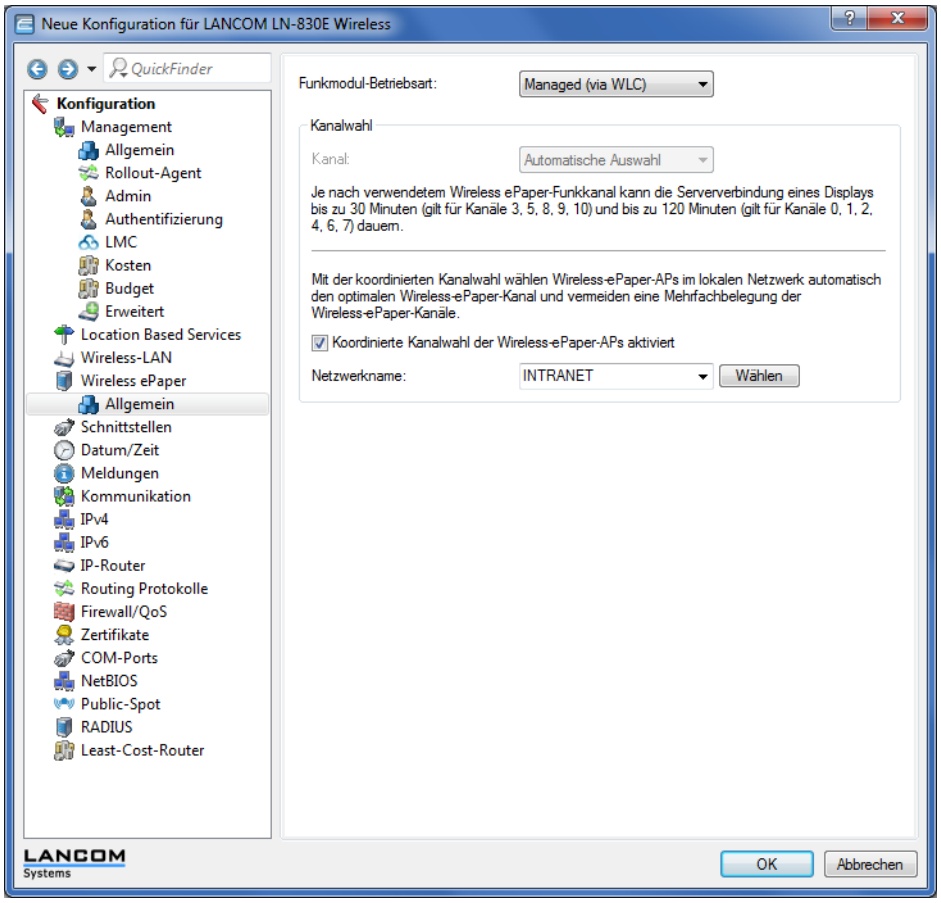
Die Peer-Tabelle enthält die ePaper-AP-ID, die Rolle des AP (Slave oder Master), die Kanalbeurteilung sowie den zugewiesenen ePaper-Kanal.

Die Kanalbeurteilung ist als Liste der ePaper-Kanäle 0 bis 10 dargestellt, dahinter jeweils die Beurteilung. Der Wertebereich beträgt 0 bis 255, wobei ein höherer Wert einer besseren Bewertung entspricht.

```
root@LN-830E PM:/Status/Wireless-ePaper
> ls -a Channel-Coordination/Peer-Table/

ID    State    IP-Address    Rtg-Tag  Connected  Assessment  Assignment
==============-------------------------------------------------------
66122  SLAVE  172.16.26.7      1        Yes       0:108|1:096|2:073|3:196
66123  MASTER 172.16.26.6      1        No                  3
66124  SLAVE  172.16.26.8      1        Yes       0:127|1:127|2:127:3:255
```

2.2.1 Aktivierung und Konfiguration in LANconfig

Sie aktivieren und konfigurieren das Feature unter **Wireless ePaper** > **Allgemein**.



1. Aktivieren Sie die koordinierte Kanalwahl über das Auswahlkästchen **Koordinierte Kanalwahl der Wireless ePaper-APs aktiviert**.

Falls die koordinierte Kanalwahl nicht aktiviert ist, so erscheint der Parameter **Netzwerkname** ausgegraut.

2. Wählen Sie aus der Auswahlliste **Netzwerkname** das Netzwerk aus, in dem die Access Points miteinander kommunizieren sollen.
3. Übernehmen Sie Ihre vorgenommenen Einstellungen durch einen Klick auf die Schaltfläche **OK**.

2.2.2 Ergänzungen im Status-Menü

Kanal-Koordination

Dieses Menü enthält die Einstellungen für die koordinierte Kanalzuweisung.

SNMP-ID:

1.88.9

Pfad Telnet:

Status > **Wireless-ePaper**

2.2.3 Ergänzungen im Setup-Menü

Koordinierte-Kanalwahl

Vemeidet Mehrfachbelegung von ePaper-Kanälen durch zueinander in Reichweite befindliche APs.

SNMP-ID:

2.88.4

Pfad Telnet:

Setup > **Wireless-ePaper**

Aktiv

Hier wird die koordinierte Kanalwahl aktiviert bzw. deaktiviert.

SNMP-ID:

2.88.4.1

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0

Nein

1

Ja

Default-Wert:

1

Netzwerk

Hier legen Sie das Netzwerk fest, in dem die Access Points miteinander kommunizieren sollen.

SNMP-ID:

2.88.4.2

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

16 Zeichen aus nachfolgendem Zeichensatz `[A-Z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

Announce-Adresse

Hier legen Sie die Ankündigungs-Adresse fest.

SNMP-ID:

2.88.4.3

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

39 Zeichen aus nachfolgendem Zeichensatz: `[0-9 A-F a-f :.]`

Announce-Port

Hier legen Sie den Ankündigungs-Port fest.

SNMP-ID:

2.88.4.4

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Intervall

Hier legen Sie das Ankündigungs-Intervall fest.

SNMP-ID:

2.88.4.5

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Timeout-Faktor

Hier legen Sie den Ankündigungs-Timeout-Faktor fest.

SNMP-ID:

2.88.4.6

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Timeout-Intervall

Hier legen Sie das Akündigungs-Timeout-Intervall fest.

SNMP-ID:

2.88.4.7

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Announce-Master-Backoff-Intervall

Hier legen Sie das Ankündigungs-Master-Backoff-Intervall fest.

SNMP-ID:

2.88.4.8

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

3 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Port

Hier legen Sie die Port-Koordination fest.

SNMP-ID:

2.88.4.9

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

5 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Keep-Alive-Intervall

Hier legen Sie die Koordination des Keep-Alive-Intervalls fest.

SNMP-ID:

2.88.4.10

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Koordination-Reconnect-Intervall

Hier legen Sie die Koordination des Reconnect-Intervalls fest.

SNMP-ID:

2.88.4.11

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

10 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Zuweisung-Wechsel-Grenzwert

Hier legen Sie den Grenzwert für den Zuweisungswechsel fest.

SNMP-ID:

2.88.4.12

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

3 Zeichen aus nachfolgendem Zeichensatz: `[0-9]`

Distanz-Bewertung

Hier legen Sie die Bewertung für die Entfernung zum WLAN fest.

Ein höherer Wert bedeutet eine bessere Bewertung.

SNMP-ID:

2.88.4.13

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0 … 255

Kanal-Bewertung

Hier legen Sie die Bewertung für einen ausgesuchten Kanal fest.

Ein höherer Wert bedeutet eine bessere Bewertung.

SNMP-ID:

2.88.4.14

Pfad Telnet:

Setup > **Wireless-ePaper** > **Koordinierte-Kanalwahl**

Mögliche Werte:

0 … 255

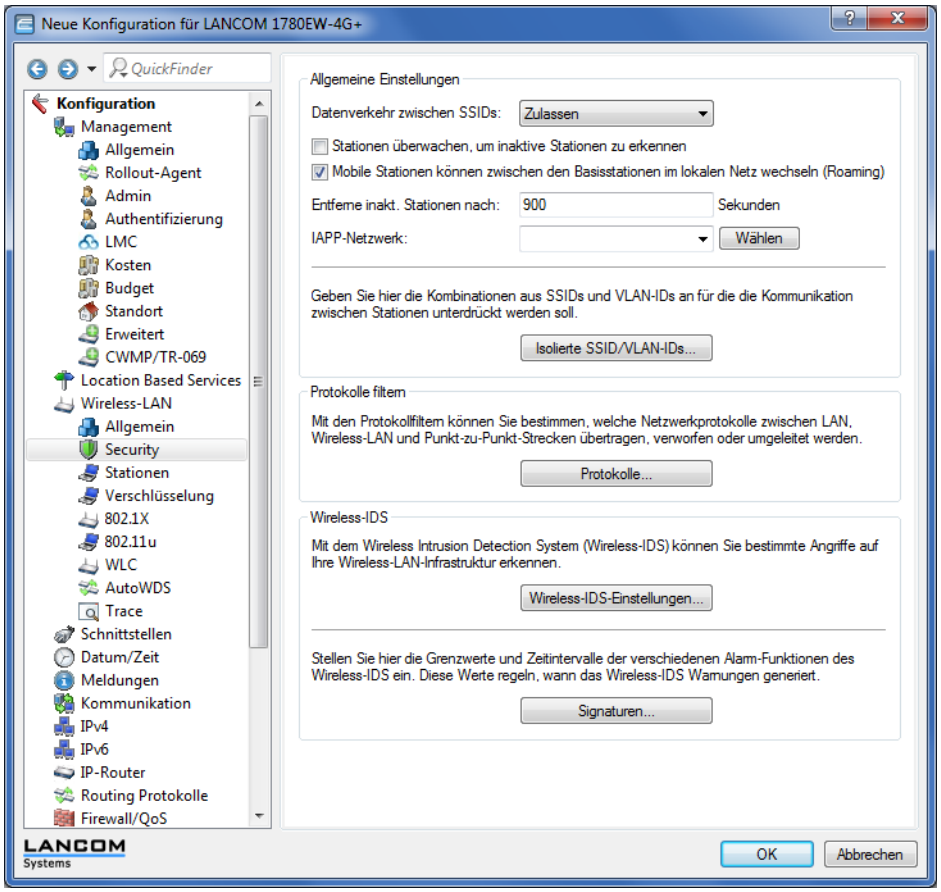
3 Wireless LAN – WLAN

3.1 Inter-Station-Traffic selektiv für Clients desselben VLANs erlauben

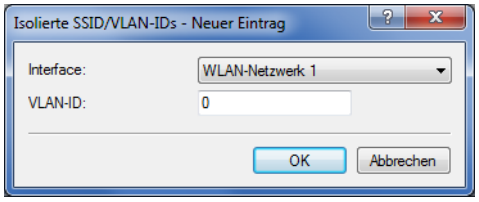
Ab LCOS-Version 10.12 bietet Ihnen dieses Feature die Möglichkeit, ein "Sammel-VLAN" abzubilden, in dem WLAN-Clients nicht untereinander kommunizieren dürfen, sondern eine Kommunikation nur zwischen WLAN-Client und AP möglich ist (Hotspot-Szenario). Außerhalb dieses "Sammel-VLANs" kann eine Kommunikation der Clients untereinander erlaubt werden. Dies funktioniert vollkommen transparent innerhalb derselben SSID, in der den Clients unterschiedliche VLANs zugewiesen werden.

3.1.1 Konfiguration in LANconfig

Navigieren Sie zu **Wireless-LAN** > **Security**.



In dem Menü **Isolierte SSID/VLAN-IDs** können Sie nun einen neuen Eintrag hinzufügen:



Hier definieren Sie, für welche Kombinationen aus SSIDs und VLANs der Datenverkehr zwischen den Clients verboten wird. Diese Tabelle funktioniert also als Blacklist, da man üblicherweise nur wenige VLANs definieren will, in denen die Kommunikation verboten wird, aber mehrere, in denen sie erlaubt wird.

Dieser Mechanismus funktioniert auch dann, wenn die Clients an verschiedenen APs eingebucht sind (wobei auf übereinstimmende Konfiguration der Tabelle geachtet werden sollte). Voraussetzung dafür ist, dass die APs via IAPP kommunizieren können.

Die Tabelle enthält folgende Parameter:

Interface

Die Liste der verfügbaren WLAN-Netzwerke.

VLAN-ID

Die Identifikationsnummer des VLANs.

Im Menü **Datenverkehr zwischen SSIDs** muss **Zulassen** ausgewählt sein, damit er mit diesem Feature wieder beschränkt werden kann.

3.1.2 Ergänzungen im Setup-Menü

VLAN-kein-Interstation-Verkehr

Diese Tabelle enthält Kombinationen aus SSIDs und VLANs, bei denen der Datenverkehr zwischen Clients verboten ist.

SNMP-ID:

2.12.71

Pfad Telnet:

Setup > **WLAN**

Netzwerk

Wählen Sie aus der Liste der vorhandenen SSIDs das Netzwerk aus, für den der Datenaustausch zwischen Clients verboten werden soll.

SNMP-ID:

2.12.71.1

Pfad Telnet:

Setup > **WLAN** > **VLAN-kein-Interstation-Verkehr**

VLAN-Id

Geben Sie hier die VLAN-ID an, für die der Datenaustausch zwischen Clients verboten werden soll.

SNMP-ID:

2.12.71.2

Pfad Telnet:

Setup > **WLAN** > **VLAN-kein-Interstation-Verkehr**

Mögliche Werte:

1 … 4094

Default-Wert:

0

3.2 Umgebungsscan zu einer konfigurierbaren Zeit starten

Die Umgebung Ihres WLAN kann regelmäßig nach Rogue APs abgesucht werden.

Ab LCOS-Version 10.12 können Sie Zeiten konfigurieren, zu denen täglich automatisiert ein Umgebungsscan nach Rogue APs durchgeführt wird.

Um den normalen Betrieb nicht unnötig zu stören, sollte ein solcher Umgebungsscan zu bestimmten Zeiten geschehen.

Daher bietet Ihnen dieses Feature die Option, täglich zu einer vordefinierten Zeit das konfigurierte Frequenzband scannen zu lassen.

Scannen bedeutet hier:

- aktives Scannen mittels Probe Requests.
- passives Scannen durch Empfang der fremden Beacons.

Unter gewissen Umständen ist nur passives Scannen möglich, z. B. wenn ein 5 GHz-Kanal momentan nicht als DFS-frei markiert ist. In diesem Fall darf nicht gesendet werden.

Zur Konfiguration über die Kommandozeile gibt es folgende Menüpunkte, hier beispielhaft mit Default-Werten:

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Environment-Scan
> ls -a

[1.3.6.1.4.1.2356.11][2.23.20.27]
Ifc      Operating  Hour    Minute  Channel-List
[1]      [2]         [3]    [4]     [5]
=========-------------------------------------------------------------------
WLAN-1    No          3      0
WLAN-2    No          3      0
```

Mittels "Hour" und "Minute" wird eingestellt, zu welchen Zeiten der Environment Scan täglich ausgeführt wird. In diesen Feldern ist auch die Cron-Syntax erlaubt. Mit der Channel-List können die zu scannenden Kanäle eingeschränkt werden (Angabe als kommaseparierte Liste). Erfolgt hier keine Angabe, werden alle Kanäle des Frequenzbandes, auf dem das Modul gerade arbeitet, gescannt.

Während des Scans verweilt das WLAN-Modul ca. drei Sekunden auf jedem Kanal. Anschließend wird der nächste Kanal gescannt. Wurden alle konfigurierten Kanäle gescannt, wechselt das Modul wieder in den regulären Betriebsmodus.

Während des Scans ist kein regulärer WLAN-Betrieb auf dem Modul möglich, anders als z.B. beim Background-Scan. Es ist aber sichergestellt, dass immer nur eines der beiden Module zur gleichen Zeit den Environment Scan durchführt, so dass auf dem jeweils anderen Modul noch der Regelbetrieb möglich ist.

Zusätzlich zur zeitgesteuerten Aktivierung des Environment Scan ist auch eine permanente Aktivierung möglich. Dazu kann das WLAN-Modul in den neu geschaffenen Betriebsmodus "Scanner" versetzt werden (siehe Operation-Mode 7):

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> l

Ifc       Operating     Operation-Mode  Link-LED-Function     Broken-Link-Detection
==========------------------------------------------------------------------------
WLAN-1    Yes           Scanner         Normal                No
WLAN-2    Yes           managed-AP      Normal                No

root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> set ?

Possible input for columns in table 'Operational':
[  1] Ifc                  : WLAN-1 (1), WLAN-2 (2)
[  2] Operating            : Yes (0), No (1)
[  3] Operation-Mode       : Access-Point (1), managed-AP (4), Station (0),
                             Probe (5), Scanner (7)
[  4] Link-LED-Function    : Normal (0), Client-Mode-Strength (1), P2P-1-Strength (8))
[  5] Broken-Link-Detection : No (0), LAN-1 (1), LAN-2 (2)
```

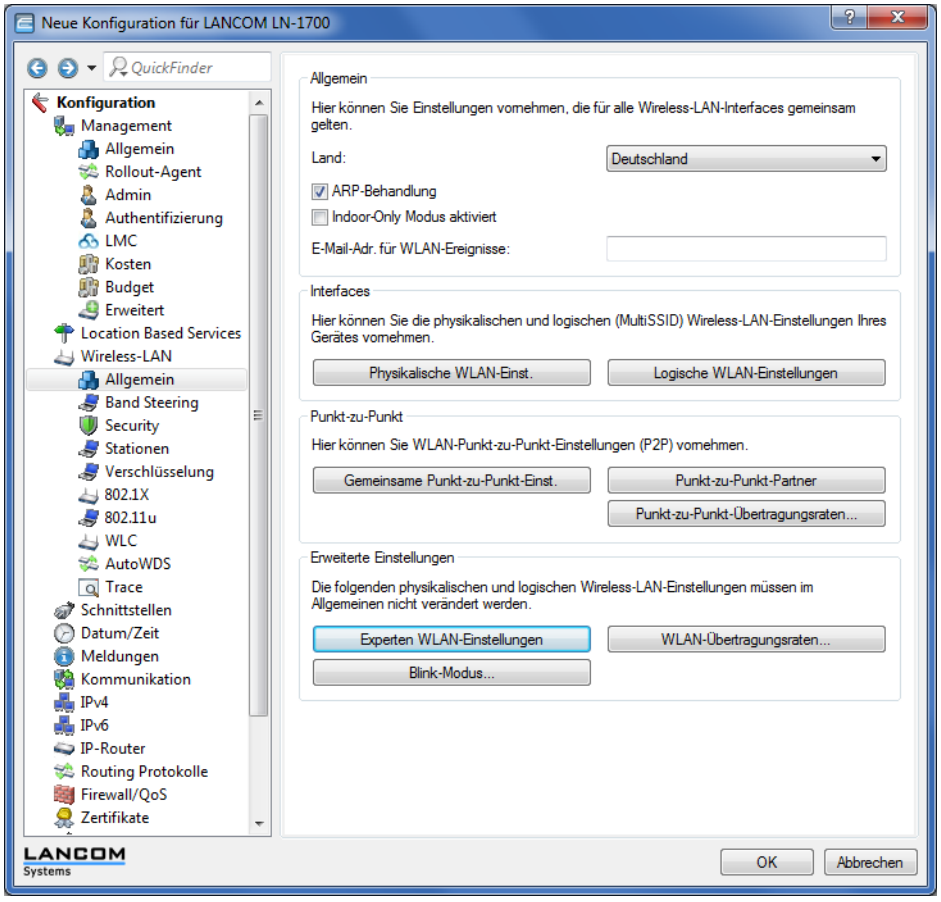
Der Umgebungsscan wird hierdurch wie oben beschrieben durchgeführt; nach dem Scannen der konfigurierten Kanäle wird der Scan nicht beendet, sondern wieder von vorne begonnen.

Diese Betriebsart kann verwendet werden, um einen AP dediziert als "Scanner"-AP zu verwenden.

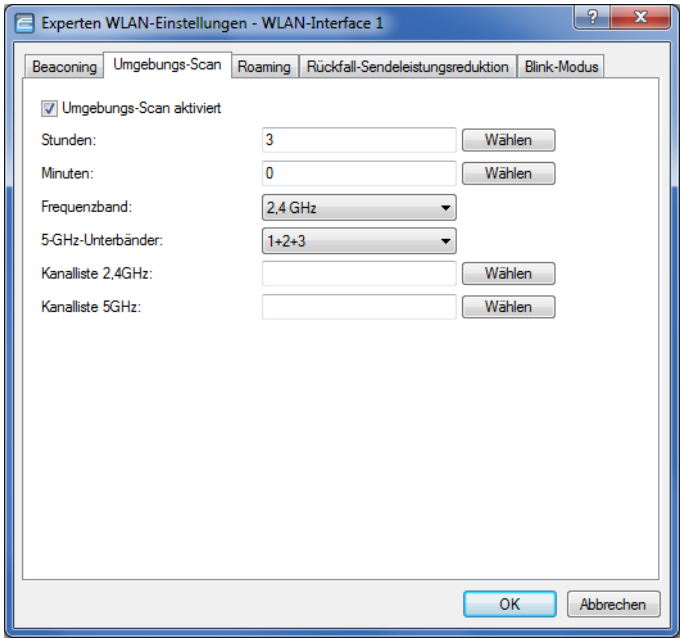
Das Ergebnis des Umgebungsscans kann in der Tabelle **Status** > **WLAN** > **Environment-Scan-Results** eingesehen werden.

3.2.1 Konfiguration in LANconfig

Navigieren Sie zu **Wireless-LAN** > **Allgemein** > **Erweiterte Einstellungen**.



Die Parameter für den Umgebungsscan werden definiert in der Tabelle **Experten WLAN-Einstellungen** im Reiter **Umgebungs-Scan**.



Umgebungs-Scan aktiviert

Aktiviert/deaktiviert den Umgebungs-Scan.

Die nachfolgenden Parameter sind ausgegraut, falls der Umgebungs-Scan deaktiviert ist.

Stunden

Enthält den Stundenwert der Uhrzeit für den Umgebungs-Scan.

Minuten

Enthält den Minutenwert der Uhrzeit für den Umgebungs-Scan.

Frequenzband

Enthält die Frequenzbänder für den Umgebungs-Scan.

Mögliche Werte:

2,4 GHz

Das 2,4 GHz-Frequenzband wird gescannt.

5 GHz

Das 5 GHz-Frequenzband wird gescannt.

2,4/5 GHz

Das 2,4 GHz- und das 5 GHz-Frequenzband werden gescannt.

5-GHz-Unterbänder

Enthält die Unterbänder des 5 GHz-Frequenzbandes.

Mögliche Werte:

1

2

3

1+2

1+3

2+3

1+2+3

Kanalliste 2,4GHz

Legt fest, für welche 2,4 GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 2,4 GHz-Frequenzbandes durchgeführt.

Mögliche Werte (Mehrfachauswahl erlaubt):

1 bis 13

In Schritten von 1.

Kanalliste 5GHz

Legt fest, für welche 5 GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 5 GHz-Frequenzbandes durchgeführt.

Mögliche Werte (Mehrfachauswahl erlaubt):

36 bis 64

In Schritten von 4.

100 bis 140

In Schritten von 4.

3.2.2 Ergänzungen im Setup-Menü

Umgebungsscan zu einer konfigurierbaren Zeit starten

Mithilfe dieser Tabelle legen Sie fest, zu welcher Uhrzeit täglich das der jeweiligen Schnittstelle zugewiesene Frequenzband nach Rogue-APs durchsucht wird. Sie dürfen hierzu auch die *CRON-Syntax verwenden*. Das Durchsuchen umfasst sowohl aktives Scannen mittels Probe Requests, als auch passives Scannen durch Empfang der fremden Beacons.

Aktives Scannen ist nicht immer möglich, z. B. wenn ein 5 GHz-Kanal nicht DFS-frei ist.

SNMP-ID:

2.23.20.27

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN**

Ifc

Diese Tabelle enthält die verfügbaren WLAN-Schnittstellen.

SNMP-ID:

2.23.20.27.1

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

1

WLAN-1

2

WLAN-2

Aktiv

Hier aktivieren/deaktivieren Sie den Umgebungs-Scan.

SNMP-ID:

2.23.20.27.2

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

0

nicht aktiv

1

aktiv

Default-Wert:

0

Stunden

Hier legen Sie den Stundenwert für die Uhrzeit des Umgebungs-Scans fest.

SNMP-ID:

2.23.20.27.6

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

0 … 23

Default-Wert:

3

Minuten

Hier legen Sie den Minutenwert für die Uhrzeit des Umgebungs-Scans fest.

SNMP-ID:

2.23.20.27.7

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

0 … 59

Default-Wert:

0

Frequenzband

Hier stellen Sie das Radio-Band ein, für das Ihr WLAN-Modul einen Umgebungsscan durchführt.

SNMP-ID:

2.23.20.27.8

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

2,4 GHz
Das 2,4 GHz-Frequenzband wird gescannt.

5 GHz
Das 5 GHz-Frequenzband wird gescannt.

2,4/5 GHz
Das 2,4 GHz- und das 5 GHz-Frequenzband werden gescannt.

Default-Wert:

2,4 GHz

Unterbänder-5 GHz

Hier konfigurieren Sie die Unterbänder Ihres 5 GHz-Frequenzbandes.

SNMP-ID:

2.23.20.27.9

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

1+2+3
1+2
1+3
2+3
1
2
3

Default-Wert:

1+2+3

Kanalliste-2,4 GHz

Hier grenzen Sie ein, für welche 2,4 GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 2,4 GHz-Frequenzbandes durchgeführt.

SNMP-ID:

2.23.20.27.10

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

leer

Der Umgebungsscan wird für sämtliche Kanäle des 2,4 GHz-Frequenzbandes durchgeführt.

1

Der Umgebungsscan wird für Kanal 1 des 2,4 GHz-Frequenzbandes durchgeführt.

2

Der Umgebungsscan wird für Kanal 2 des 2,4 GHz-Frequenzbandes durchgeführt.

3

Der Umgebungsscan wird für Kanal 3 des 2,4 GHz-Frequenzbandes durchgeführt.

4

Der Umgebungsscan wird für Kanal 4 des 2,4 GHz-Frequenzbandes durchgeführt.

5

Der Umgebungsscan wird für Kanal 5 des 2,4 GHz-Frequenzbandes durchgeführt.

6

Der Umgebungsscan wird für Kanal 6 des 2,4 GHz-Frequenzbandes durchgeführt.

7

Der Umgebungsscan wird für Kanal 7 des 2,4 GHz-Frequenzbandes durchgeführt.

8

Der Umgebungsscan wird für Kanal 8 des 2,4 GHz-Frequenzbandes durchgeführt.

9

Der Umgebungsscan wird für Kanal 9 des 2,4 GHz-Frequenzbandes durchgeführt.

10

Der Umgebungsscan wird für Kanal 10 des 2,4 GHz-Frequenzbandes durchgeführt.

11

Der Umgebungsscan wird für Kanal 11 des 2,4 GHz-Frequenzbandes durchgeführt.

12

Der Umgebungsscan wird für Kanal 12 des 2,4 GHz-Frequenzbandes durchgeführt.

13

Der Umgebungsscan wird für Kanal 13 des 2,4 GHz-Frequenzbandes durchgeführt.

Kanalliste-5 GHz

Hier grenzen Sie ein, für welche 5 GHz-Kanäle der Umgebungs-Scan durchgeführt werden soll.

Falls Sie hier keine Eintragungen vornehmen, wird der Umgebungsscan für sämtliche Kanäle des 5 GHz-Frequenzbandes durchgeführt.

SNMP-ID:

2.23.20.27.11

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Umgebungs-Scan**

Mögliche Werte:

leer

Der Umgebungsscan wird für sämtliche Kanäle des 5 GHz-Frequenzbandes durchgeführt.

36

Der Umgebungsscan wird für Kanal 36 des 5 GHz-Frequenzbandes durchgeführt.

40

Der Umgebungsscan wird für Kanal 40 des 5 GHz-Frequenzbandes durchgeführt.

44

Der Umgebungsscan wird für Kanal 44 des 5 GHz-Frequenzbandes durchgeführt.

48

Der Umgebungsscan wird für Kanal 48 des 5 GHz-Frequenzbandes durchgeführt.

52

Der Umgebungsscan wird für Kanal 52 des 5 GHz-Frequenzbandes durchgeführt.

56

Der Umgebungsscan wird für Kanal 56 des 5 GHz-Frequenzbandes durchgeführt.

60

Der Umgebungsscan wird für Kanal 60 des 5 GHz-Frequenzbandes durchgeführt.

64

Der Umgebungsscan wird für Kanal 64 des 5 GHz-Frequenzbandes durchgeführt.

100

Der Umgebungsscan wird für Kanal 100 des 5 GHz-Frequenzbandes durchgeführt.

104

Der Umgebungsscan wird für Kanal 104 des 5 GHz-Frequenzbandes durchgeführt.

108

Der Umgebungsscan wird für Kanal 108 des 5 GHz-Frequenzbandes durchgeführt.

112

Der Umgebungsscan wird für Kanal 112 des 5 GHz-Frequenzbandes durchgeführt.

116

Der Umgebungsscan wird für Kanal 116 des 5 GHz-Frequenzbandes durchgeführt.

120

Der Umgebungsscan wird für Kanal 120 des 5 GHz-Frequenzbandes durchgeführt.

124

Der Umgebungsscan wird für Kanal 124 des 5 GHz-Frequenzbandes durchgeführt.

128

Der Umgebungsscan wird für Kanal 128 des 5 GHz-Frequenzbandes durchgeführt.

132

Der Umgebungsscan wird für Kanal 132 des 5 GHz-Frequenzbandes durchgeführt.

136

Der Umgebungsscan wird für Kanal 136 des 5 GHz-Frequenzbandes durchgeführt.

140

Der Umgebungsscan wird für Kanal 140 des 5 GHz-Frequenzbandes durchgeführt.

3.3 Umwandlung von Multicast- in Unicast-Datenströme

Ab LCOS-Version 10.12 können Sie auch Multicast- in Unicast-Datenströme umwandeln.

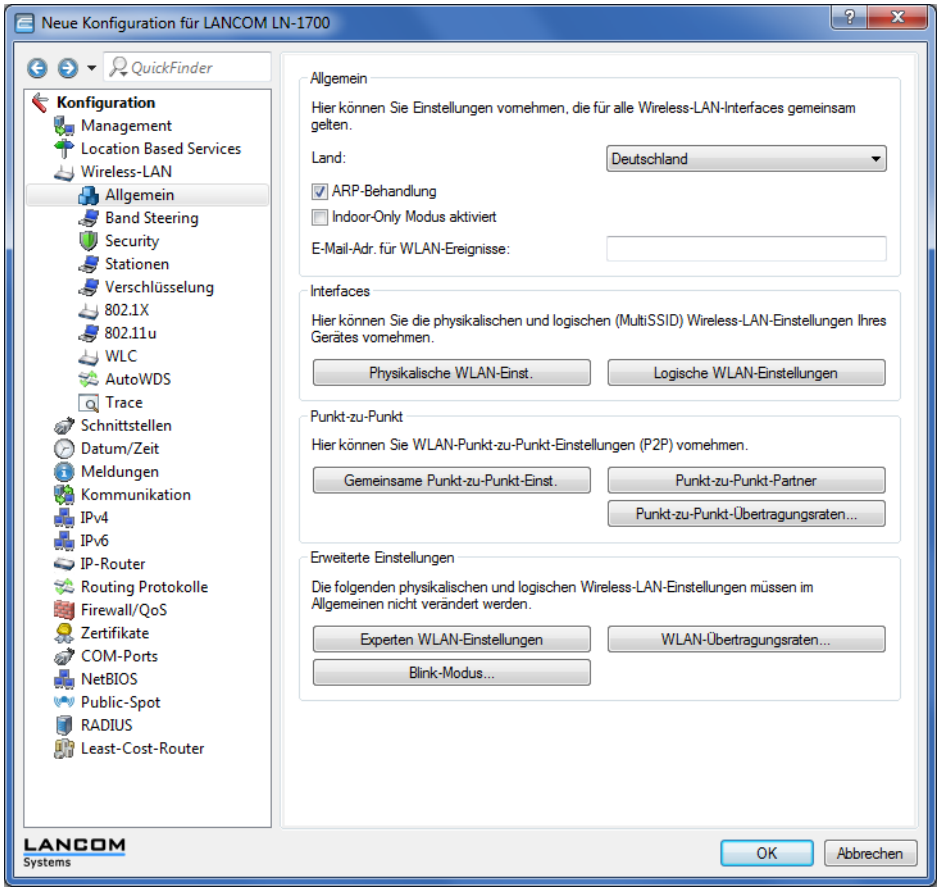
Die automatische Umwandlungsmöglichkeit von Multicast- in Unicast-Datenströme ermöglicht mehreren WLAN-Clients ruckelfreies Streaming hochauflösender Videoanwendungen. Bei Anwendungen, wie z.B. IPTV-Diensten, profitieren Sie so von gesteigerter Performance und einer deutlich spürbaren Qualitätsverbesserung.

Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert. Die Pakete werden zwar je Client dupliziert, können aber, da sie sich nun um Unicasts handeln, mit der für diesen Client höchstmöglichen Datenrate übertragen werden. Auch wenn die Pakete nun dupliziert werden, wird durch die viel schnellere Übertragung in den meisten Szenarien insgesamt deutlich weniger Airtime verbraucht, die dann für andere Übertragungen zur Verfügung steht.

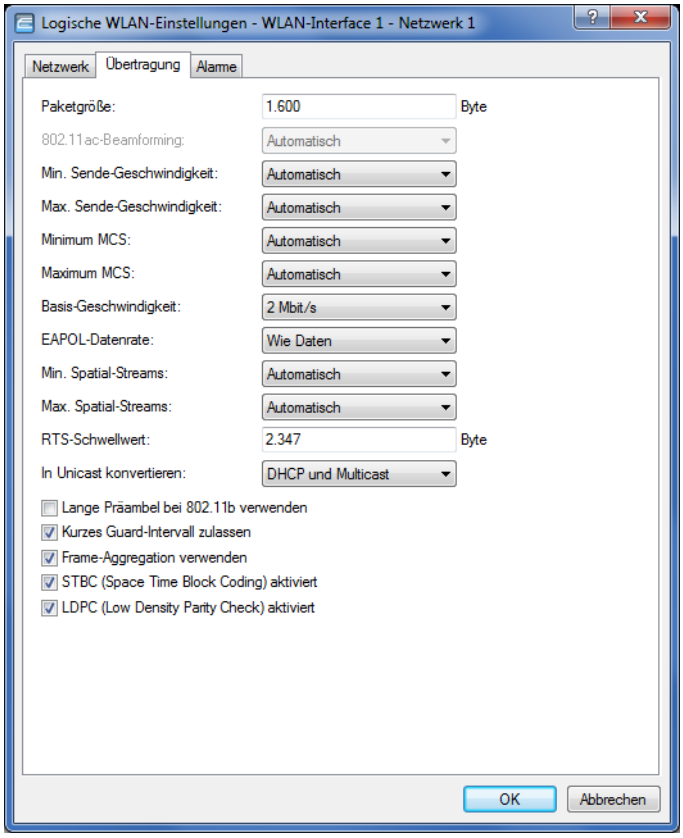
Damit das Feature funktioniert, ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren. Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

3.3.1 Konfiguration in LANconfig

Sie finden das neue Feature unter **Wireless-LAN** > **Allgemein** > **Interfaces** > **Logische WLAN-Einstellungen**



nach Auswahl einer WLAN-Schnittstelle im Reiter **Übertragung**.



In Unicast konvertieren

Sie haben folgende Optionen für die Umwandlung von Datenströmen in Unicast:

Keine

Es werden keine Datenströme in Unicast umgewandelt.

DHCP

Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

Multicast

Multicast-Datenströme, die über WLAN-Interfaces übertragen werden sollen, werden nach Aktivierung des Features in einzelne Unicast-Datenströme je Client auf dem MAC-Layer bzw. WLAN-Layer konvertiert.

DHCP und Multicast

Wandelt DHCP- und Multicast-Datenstöme in Unicast um.

3.3.2 show-Kommando über CLI

Mittels des Befehls `show igmp-snooping` lässt sich einsehen, welche Clients an welchen Ports welche Multicast-Gruppen "abonniert" haben. Bei aktivem Feature wird für die Clients (Members), die hier aufgeführt sind, eine Konvertierung durchgeführt. Hier ein Beispiel:

```
> show igmp-snooping
```

```
Group           | VLAN  | Ports
=======================================
224.0.0.251     |     1 | WLAN-1


Group           | VLAN  | Member            | Port
=================================================
224.0.0.251     |     1 | a0:18:28:0c:9c:af | WLAN-1
```

3.3.3 Ergänzungen im Setup-Menü

in-Unicast-wandeln

Über diesen Parameter legen Sie fest, welche Art von als Broadcast gesendeten Datenpaketen das Gerät innerhalb eines WLAN-Netzwerks automatisch in Unicast umwandelt.

SNMP-ID:

2.23.20.2.25

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Uebertragung**

Mögliche Werte:

0

Keine Auswahl

1

DHCP: Wandelt Antwort-Nachrichten des DHCP-Servers in Unicasts um, sofern der Server sie als Broadcast versendet hat. Dies steigert die Zuverlässigkeit der Zustellung, da als Broadcast gesendete Datenpakete keinen speziellen Adressaten, keine optimierten Sendetechniken wie ARP-Spoofing oder IGMP/MLD-Snooping und eine niedrige Datenrate aufweisen.

2

Multicast: Damit das Feature funktioniert, ist es erforderlich, das IGMP-Snooping auf dem Gerät zu aktivieren und korrekt zu konfigurieren. Über das IGMP-Snooping ermittelt das Gerät, welcher Client welchen Multicast-Strom empfangen möchte. Der Multicast-Konvertierung stehen somit die passenden Ziel-Clients bzw -Adressen für die Konvertierung zur Verfügung.

3

DHCP- und Multicast-Konvertierung

Default-Wert:

1

4 Routing und WAN-Verbindungen

4.1 OSPF

Ab LCOS-Version 10.12 steht Ihnen OSPF zur Auswahl.

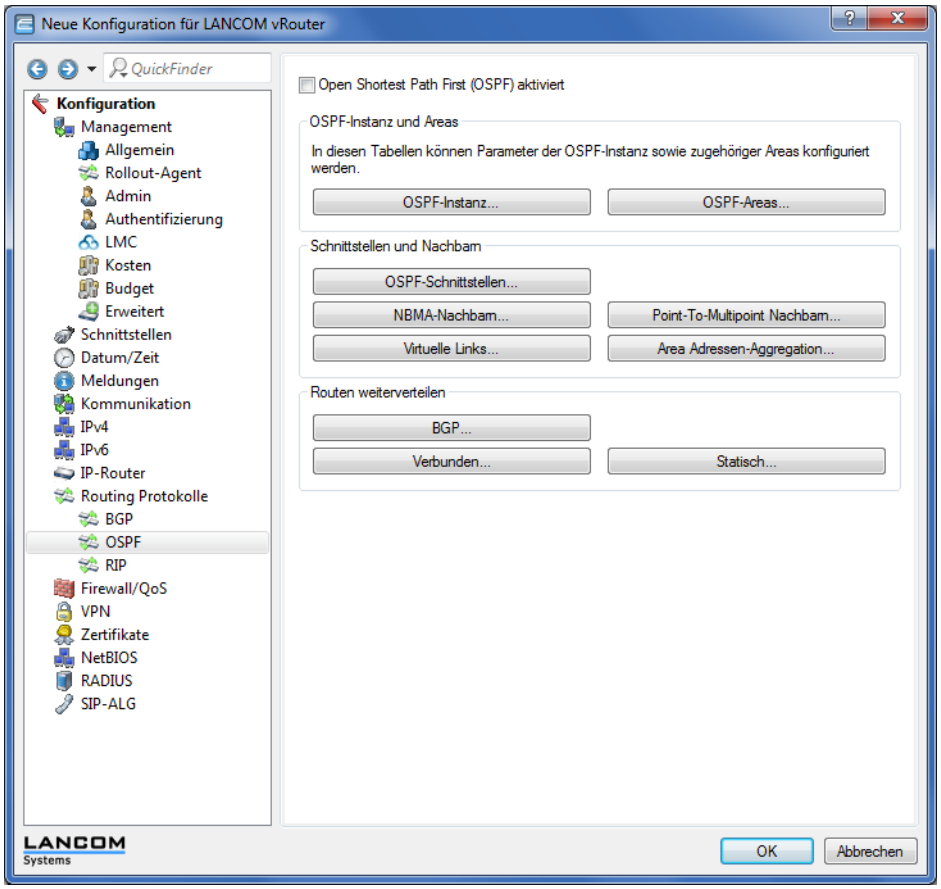
Open Shortest Path First (OSPF) ist ein Link State Routing Protokoll nach RFC 2328. Es gehört zur Kategorie der **Interior-Gateway-Protokolle** (IGP). Dabei tauschen die Router regelmäßig Link-Status-Informationen per Link State Advertisement (LSA) aus. Die Router finden sich automatisch im lokalen Netzwerk per Multicast. OSPF wird in der Regel dazu verwendet um in großen Netzen (LANs) interne Routinginformationen auszutauschen.

Jeder Router hat dabei eine identische Kopie der Datenbank (Link State Database, LSDB) vorliegen, woraus er Router mit Hilfe des Dijkstra-Algorithmus (Shortest Path First, SPF) den Kürzeste-Pfad-Baum bestimmt.

Im Gegensatz hierzu gehört BGP zur Kategorie der **Exterior Gateway Protokolle** (EGP) und wird in der Regel dazu verwendet, um Routen zwischen autonomen Systemen oder innerhalb von VPNs auszutauschen.

4.1.1 OSPF mit LANconfig konfigurieren

Um OSPF mit LANconfig zu konfigurieren, wechseln Sie in die Ansicht **Routing Protokolle** > **OSPF**.



Open Shortest Path First (OSPF) aktiviert

Um die OSPF-Funktion zu aktivieren, markieren Sie die Option **Open Shortest Path First (OSPF) aktiviert**.

OSPF-Instanz

Die Tabelle **OSPF-Instanz** definiert die OSPF-Instanzen auf diesem Gerät. Es werden mehrere gleichzeitig aktive OSPF-Instanzen auf einem Gerät unterstützt. Jede Instanz entspricht dann einem autonomen System bzw. einer OSPF-Domäne.

OSPF-Areas

Die Tabelle **OSPF-Areas** definiert die Parameter der OSPF-Areas.

OSPF-Schnittstellen

In dieser Tabelle werden die Schnittstellen definiert, auf denen OSPF verwendet werden soll.

NBMA-Nachbarn

Non-Broadcast-Multiaccess-Netzwerke sind Netzwerke, in denen mehrere Router vorhanden sind, aber kein Broadcast unterstützt wird. OSPF emuliert in diesem Netzwerktyp den Betrieb in einem Broadcast-Netzwerk. In diesem Netzwerktyp wird ein Designierter Router gewählt.

Die Kommunikation findet nicht per Multicast statt, sondern per Unicast. Nachbarschaftsbeziehungen müssen manuell konfiguriert werden, da sich die Router nicht automatisch per Multicast finden können.

Point-To-Multipoint Nachbarn

In einem Point-To-Multipoint-Netzwerk werden alle Nachbarn so behandelt als wären Point-To-Point-Nachbarn über ein Nicht-Broadcast-Netzwerk direkt verbunden. Es wird keine Designierter Router gewählt, die Kommunikation erfolgt per Multicast.

Virtuelle Links

In dieser Tabelle können Virtuelle Links (auch bezeichnet als Transit-Area) definiert werden. Grundsätzlich müssen bei OSPF alle Areas direkt mit der Backbone-Area verbunden sein. In Fällen, wo dies nicht möglich ist, können virtuelle Links verwendet werden. Ein virtueller Link verbindet einen Router durch eine nicht-Backbone-Area mit der Backbone-Area.

Area Adressen-Aggregation

Um die Anzahl der Einträge in den Routing-Tabellen zu reduzieren, können durch Adressen-Aggregation an Area-Grenzen, beim Übergang von einer Nicht-Backbone-Area zur Backbone-Area, IP-Adressen zusammengefasst werden. Das entsprechende Subnetz wird als Summary LSA angekündigt.

BGP

Dynamisch gelernte Routen aus BGP-Quellen bzw. -Protokollen können nach OSPF weiterverteilt werden.

Verbunden

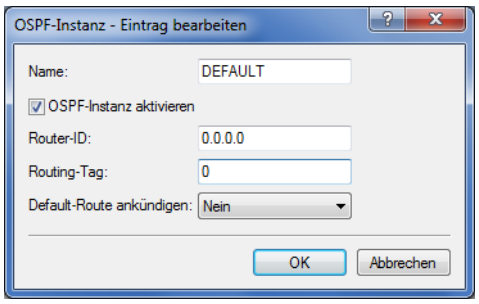
Verbundene Routen, d.h. Routen, die vom Betriebssystem automatisch in die Routing-Tabelle eingetragen werden, können nach OSPF weiterverteilt werden.

Statisch

Statische Routen, d.h. Routen, die manuell vom Benutzer in die Routing-Tabelle eingetragen werden, können nach OSPF weiterverteilt werden.

OSPF-Instanz

Die OSPF-Instanz des Gerätes konfigurieren Sie unter **OSPF-Instanz**.



Name

Enthält den Namen der OSPF-Instanz.

OSPF-Instanz aktivieren

Aktiviert bzw. deaktiviert diese OSPF-Instanz.

Router-ID

Enthält die 32 Bit Router-ID (repräsentiert als IPv4-Adresse), die dieser OSPF-Instanz zugeordnet ist. Die Router-ID identifiziert diesen Router eindeutig innerhalb einer OSPF-Domäne.

Routing-Tag

Enthält das dieser Instanz zugeordnete Routing-Tag.

Default-Route ankündigen

Definiert, ob dieser Router in dieser Instanz die Default-Route ankündigen bzw. propagieren soll.

Mögliche Werte:

Nein (Default)

Der Router kündigt keine Default-Route an.

Ja

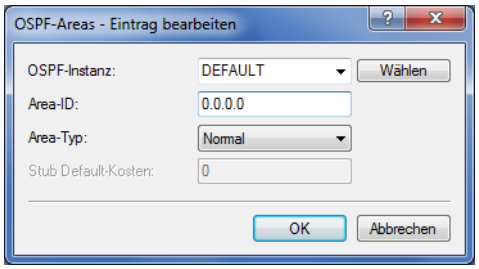
Der Router kündigt die Default-Route immer an, unabhängig davon, ob die Default-Route in seiner Routing-Tabelle vorhanden ist.

Dynamisch

Der Router kündigt die Default Route nur an, falls die Default-Route in seiner Routing-Tabelle auch vorhanden ist.

OSPF-Areas

Die Parameter der OSPF-Areas konfigurieren Sie unter **OSPF-Areas**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Area-ID

Die Area-ID (dargestellt als IPv4-Adresse) identifiziert die Area.

Falls diese Instanz die Backbone Area sein soll, so muss der Wert 0.0.0.0 verwendet werden.

Area-Typ

Legt den Typ der Area fest.

Mögliche Werte:

Normal (Default)

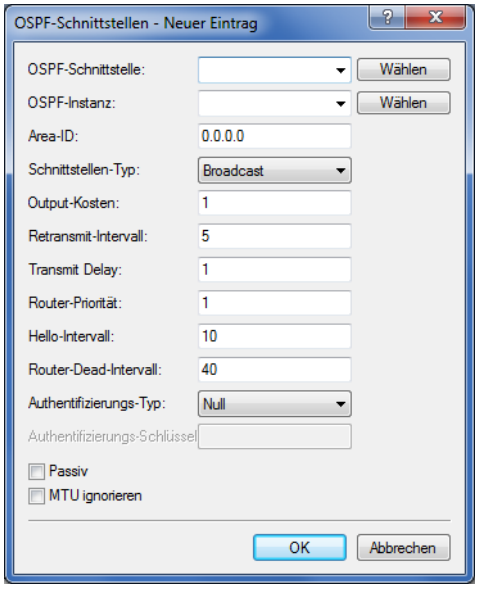
Stub

Stub-Default-Kosten

Falls die Area als Stub Area konfiguriert ist und der Router selbst Area Border Router ist, bezeichnet der Parameter **Stub-Default-Kosten** die Kosten der Default Summary-LSA, die dieser Router in dieser Area ankündigen soll.

OSPF-Schnittstellen

Definiert die Schnittstellen, auf denen OSPF verwendet werden soll.



OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

OSPF-Instanz

Enthält den Namen der OSPF Instanz.

Area-ID

Identifiziert die Area über eine IPv4-Adresse.

Schnittstellen-Typ

Definiert den Schnittstellen-Typ.

Mögliche Werte:

Broadcast

Ethernet-basiertes Netzwerk, es wird ein Designierter Router gewählt, es wird - Multicast zur Kommunikation verwendet.

Point-to-Point

Netzwerk, das nur aus zwei Routern besteht (z.B. GRE-Tunnel), oder Ethernets per P2P-Link, es wird kein Designierter Router gewählt, es wird Multicast zur Kommunikation verwendet.

Point-to-Multipoint

Netzwerk als "Hub-and-Spoke-Topologie", es wird ein Designierter Router gewählt, es wird Multicast zur Kommunikation verwendet.

Non-Broadcast Multi-Access (NBMA)

Point-to-Multipoint-Netzwerke, die kein Broadcast bzw. Multicast unterstützen, es wird ein Designierter Router gewählt, es wird Unicast zur Kommunikation verwendet, die Nachbarn müssen manuell konfiguriert werden.

Output-Kosten

Definiert die Kosten, um ein Paket auf dieser Schnittstelle zu senden, dargestellt in der Link State Metrik. Die Ankündigung erfolgt als als Link-Kosten für diese Schnittstelle in den LSA-Nachrichten des Routers.

Der Wert muss immer größer als Null sein.

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

Transmit Delay

Enthält die geschätzte Anzahl an Sekunden, die benötigt wird, um ein Link-State-Update-Paket über diese Schnittstelle zu übertragen.

Router-Priorität

Definiert die Priorität dieses Routers auf dieser Schnittstelle bei der Wahl zum Designierten Router (DR). Der Router mit der höchsten Priorität wird Designierter Router (Designated Router).

Der Wert 0 verhindert, dass der Router Designierter Router auf dieser Schnittstelle wird.

Hello-Intervall

Enthält das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

Router-Dead-Intervall

Legt die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben, in Sekunden fest.

Dieser Wert muss größer als das Hello-Intervall sein.

Authentifizierungs-Typ

Enthält die Authentifizierungsmethode, die für diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Null

Einfaches Passwort

Kryptographisch-MD5

Authentifizierungs-Schlüssel

Enthält den Authentifizierungsschlüssel für dieses Netzwerk.

Hierzu darf nicht der Authentifizierungs-Typ **Null** gewählt worden sein.

Passiv

Definiert, ob OSPF aktiv oder passiv auf dieser Schnittstelle arbeiten soll.

Mögliche Werte:

Ja

Es werden keine Routing-Updates sowie Hello-Nachrichten von diesem Router auf diesem Interface versendet. Ebenso werden keine eingehenden OSPF-Nachrichten verarbeitet. Die entsprechende Route bzw. Netzwerk dieser Schnittstelle wird aber weiterhin in die LSDB eingefügt und damit auf anderen Schnittstellen angekündigt.

Nein (Default)

MTU ignorieren

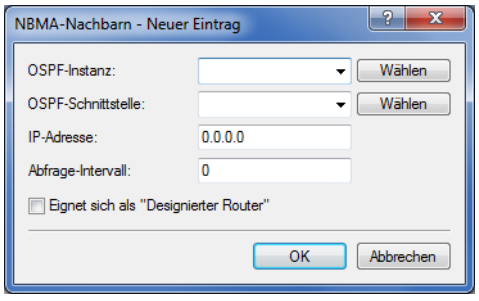
Deaktiviert die Überprüfung des MTU-Werts in Database Description Paketen.

Dies ermöglicht, dass Router eine vollständige Nachbarschaftsbeziehung etablieren können, obwohl die MTU der entsprechenden Schnittstellen nicht einheitlich ist.

NBMA-Nachbarn

Non-Broadcast-Multiaccess-Netzwerke sind Netzwerke, in denen mehrere Router vorhanden sind, aber kein Broadcast unterstützt wird. OSPF emuliert in diesem Netzwerktyp den Betrieb in einem Broadcast-Netzwerk. Hierzu wird zuvor ein Designierter Router gewählt.

Die Kommunikation findet nicht per Multicast statt, sondern per Unicast. Nachbarschaftsbeziehungen müssen manuell konfiguriert werden, da sich die Router nicht automatisch per Multicast finden können.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

IP-Adresse

Enthält IPv4-Adresse des Nachbar-Routers (Router auf der Gegenseite).

Abfrage-Intervall

Enthält das Intervall, in dem Hello-Nachrichten zu diesem Router gesendet werden.

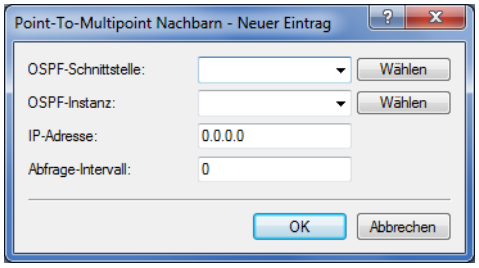
Der Wert Null deaktiviert das Senden von Hello-Nachrichten.

Eignet sich als "Designierter Router"

Definiert, ob das lokale Gerät selbst als Designierter Router wählbar ist.

Point-To-Multipoint Nachbarn

In einem Point-To-Multipoint-Netzwerk werden alle Nachbarn so behandelt, als wären sie wie Point-To-Point-Nachbarn über ein Nicht-Broadcast-Netzwerk direkt miteinander verbunden. Es wird keine Designierter Router gewählt, und die Kommunikation erfolgt per Multicast.



OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

IP-Adresse

Enthält IPv4-Adresse des Nachbar-Routers (Router auf der Gegenseite).

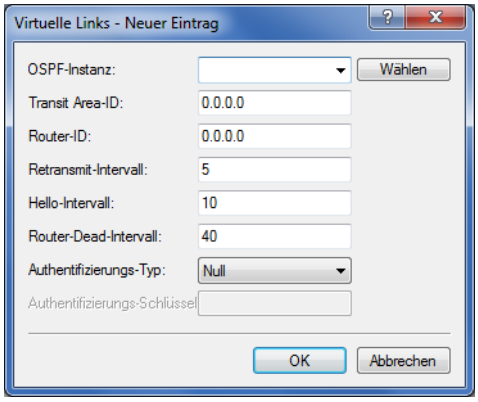
Abfrage-Intervall

Enthält das Intervall, in dem Hello-Nachrichten zu diesem Router gesendet werden.

Der Wert Null deaktiviert das Senden von Hello-Nachrichten.

Virtuelle Links

In dieser Tabelle können Virtuellen Links (auch bezeichnet als Transit-Area) definiert werden. Grundsätzlich müssen bei OSPF alle Areas direkt mit der Backbone-Area verbunden sein. In Fällen, wo dies nicht möglich ist, können virtuelle Links verwendet werden. Ein virtueller Link verbindet einen Router durch eine nicht-Backbone-Area mit der Backbone-Area.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Transit Area-ID

Enthält die Area-ID der Transit-Area, definiert als IPv4-Adresse.

Router-ID

Enthält die Router-ID des Routers auf der Gegenseite des virtuellen Links als IPv4-Adresse.

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

Hello-Intervall

Definiert das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

Router-Dead-Intervall

Legt die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben, in Sekunden fest.

Dieser Wert muss größer als das Hello-Intervall sein.

Authentifizierungs-Typ

Enthält die Authentifizierungsmethode, die für diese Schnittstelle verwendet werden soll.

Mögliche Werte:

Null

Einfaches Passwort

Kryptographisch-MD5

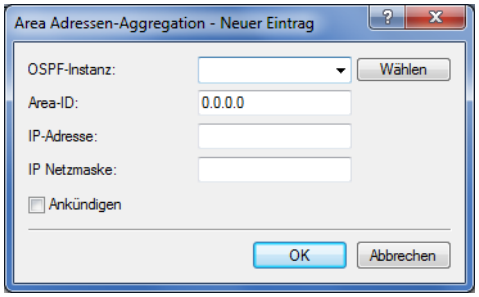
Authentifizierungs-Schlüssel

Enthält den Authentifizierungsschlüssel für dieses Netzwerk.

Hierzu darf nicht der Authentifizierungs-Typ **Null** gewählt worden sein.

Area Addressen-Aggregation

Um die Anzahl der Einträge in den Routing-Tabellen zu reduzieren, können durch Adressen-Aggregation an Area-Grenzen, beim Übergang von einer Nicht-Backbone-Area zur Backbone-Area, IP-Adressen zusammengefasst werden. Das entsprechende Subnetz wird als Summary-LSA angekündigt.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Area-ID

Identifiziert die Area über eine IPv4-Adresse.

Falls diese Instanz die Backbone Area sein soll, so muss der Wert 0.0.0.0 verwendet werden.

IP-Adresse

Enthält die IPv4-Adresse.

IP Netzmaske

Enthält die IPv4-Subnetzmaske.

Ankündigen

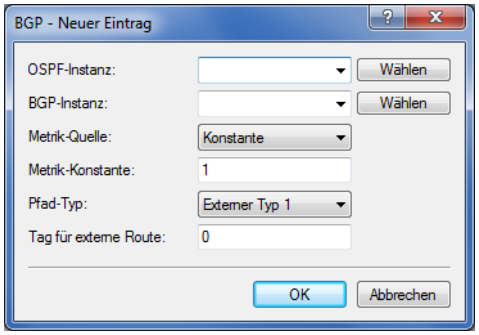
Aktiviert bzw. deaktiviert das Ankündigen dieser Adressen-Aggregation.

Route-Redistribution

Durch Routen-Redistribution können Routen von anderen Routen-Quellen bzw. Protokollen nach OSPF weiterverteilt werden. Hierzu werden die Routen mit entsprechendem Typ aus der Routing-Tabelle ausgelesen und durch OSPF weiterverteilt.

BGP

Das Weiterverteilen von dynamisch gelernte Routen aus dem Border Gateway Protocol konfigurieren Sie unter **BGP**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

BGP-Instanz

Enthält den Namen der BGP-Instanz.

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Es wird der Wert "Lokale Präferenz" des BGP-Präfix verwendet bzw. importiert.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

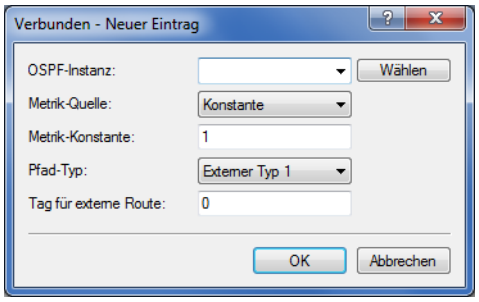
Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

Verbunden

Das Weiterverteilen von Routen, die vom Betriebssystem automatisch in die Routing-Tabelle eingetragen werden, konfigurieren Sie unter **Verbunden**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Der Wert wird automatisch gesetzt.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

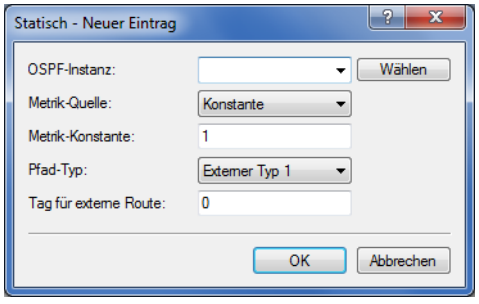
Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

Statisch

Das Weiterverteilen statischer Routen, d.h. Routen, die manuell vom Benutzer in die Routing-Tabelle eingetragen werden, konfigurieren Sie unter **Statisch**.



OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

Mögliche Werte:

Konstante

Es wird eine benutzerdefinierte konstante Metrik verwendet.

Protokoll

Der Wert wird automatisch gesetzt.

Metrik-Konstante

Falls als Metrik-Quelle "Konstante" konfiguriert ist, wird der Wert Metrik-Konstante für die OSPF-Metrik der importierten Routen verwendet.

Pfad-Typ

Definiert, als welcher Typ die Routen in OSPF importiert werden.

Mögliche Werte:

Externer Typ 1

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten + Total Path Metrik, um diesen ASBR zu erreichen.

Im OSPF-Routing-Algorithmus von Routern werden Typ 1 Routen vor Typ 2 Routen grundsätzlich bevorzugt.

Externer Typ 2

Die OSPF-Metrik wird gebildet aus der Redistribution-Metrik bzw. Metrik-Konstanten.

Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

4.1.2 Show-Commands über CLI

Ihnen stehen folgende Show-Kommandos zur Verfügung:

- **show ospf-config**

  Zeigt eine Zusammenfassung der konfigurierten OSPF-Instanzen an.

- **show ospf-database**

  Zeigt die OSPF-Datenbank an.

- **show ospf-graph**

  Zeigt die OSPF-Areas als Graphenbeschreibung im Graphviz-Format an.

- **show ospf-neighbor**

  Zeigt Informationen über OSPF-Nachbarn an.

- **show ospf-rib**

  Zeigt Informationen über die OSPF Routing Information Base an.

4.1.3 Ergänzungen im Setup-Menü

OSPF

In diesem Verzeichnis konfigurieren Sie das Gerät für das Open Shortest Path First-Protokoll.

SNMP-ID:

2.93.3.

Pfad Telnet:

Setup > **Routing-Protokolle**

OSPF-Instanz

In dieser Tabelle konfigurieren Sie die OSPF-Instanzen.

SNMP-ID:

2.93.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

Name

Dieser Parameter enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.1.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

OSPF-Instanz aktivieren

Aktiviert bzw. deaktiviert diese OSPF-Instanz.

SNMP-ID:

2.93.3.1.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

0
deaktiviert

1
aktiviert

Default-Wert:

0

Router-ID

Die 32 Bit Router-ID, die dieser OSPF-Instanz zugeordnet ist. Die Router-ID identifiziert diesen Router eindeutig innerhalb einer OSPF-Domäne.

SNMP-ID:

2.93.3.1.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Routing-Tag

Enthält das Routing-Tag, das dieser Instanz zugeordnet ist.

SNMP-ID:

2.93.3.1.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

0 … 65535

Default-Route-ankündigen

Definiert, ob dieser Router in dieser Instanz die Default-Route ankündigen bzw. propagieren soll.

SNMP-ID:

2.93.3.1.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Instanz**

Mögliche Werte:

Nein

Der Router kündigt keine Default-Route an.

Ja

Der Router kündigt die Default-Route immer an, unabhängig davon, ob die Default-Route in seiner Routing-Tabelle vorhanden ist.

Dynamisch

Der Router kündigt die Default Route nur an, falls die Default-Route in seiner Routing-Tabelle auch vorhanden ist.

Default-Wert:

Nein

OSPF-Areas

In dieser Tabelle konfigurieren Sie die OSPF-Areas.

SNMP-ID:

2.93.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Dieser Parameter enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.2.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Areas**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area-ID

Die Area-ID (dargestellt als IPv4-Adresse) identifiziert die Area.

SNMP-ID:

2.93.3.2.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Areas**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Besondere Werte:

0.0.0.0

Ernennt diese Instanz zur Backbone Area.

Area-Typ

Dieser Parameter beschreibt den Typ der Area.

SNMP-ID:

2.93.3.2.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Areas**

Mögliche Werte:

Normal
Stub

Default-Wert:

Normal

Stub-Default-Kosten

Falls die Area als Stub Area konfiguriert wurde und der Router selbst Area Border Router ist, so bezeichnet der Parameter **Stub-Default-Kosten** die Kosten der Default Summary-LSA, die dieser Router in dieser Area ankündigt.

SNMP-ID:

2.93.3.2.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Areas**

Mögliche Werte:

0 … 4294967295

Area-Addressen-Aggregation

In dieser Tabelle konfigurieren Sie die Area-Addressen-Aggregation.

SNMP-ID:

2.93.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Dieser Parameter enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.3.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Area-Addressen-Aggregation**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area-ID

Enthält die ID der Area.

SNMP-ID:

2.93.3.3.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Area-Addressen-Aggregation**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

IP-Adresse

Dieser Parameter enthält die IPv4-Adresse.

SNMP-ID:

2.93.3.3.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Area-Addressen-Aggregation**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

IP Netzmaske

Dieser Prameter enthält die IPv4-Subnetzmaske.

SNMP-ID:

2.93.3.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Area-Addressen-Aggregation**

Mögliche Werte:

IPv4-Netzmaske `[0-9.]`

Ankündigen

Aktiviert bzw. deaktiviert das Ankündigen dieser Adressen-Aggregation.

SNMP-ID:

2.93.3.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Area-Addressen-Aggregation**

Mögliche Werte:

Nein

Ankündigen deaktiviert

Ja

Ankündigen aktiviert

Default-Wert:

Nein

OSPF-Schnittstellen

Definiert die Schnittstellen, auf denen OSPF verwendet wird.

SNMP-ID:

2.93.3.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

SNMP-ID:

2.93.3.4.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

Zeichen aus folgendem Zeichensatz: `[a-z A-Z 0-9 .]`

OSPF-Instanz

Dieser Parameter enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.4.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area-ID

Enthält die ID der Area.

SNMP-ID:

2.93.3.4.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Schnittstellen-Typ

Enthält den Typ der Schnittstelle.

SNMP-ID:

2.93.3.4.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

Broadcast

Ethernet-basiertes Netzwerk, es wird ein Designierter Router gewählt und Multicast zur Kommunikation verwendet.

Point-To-Point

Netzwerk, das nur aus zwei Routern besteht (z.B. GRE-Tunnel), oder Ethernets per P2P-Link, es wird kein Designierter Router gewählt und Multicast zur Kommunikation verwendet.

Point-To-Multipoint

Netzwerk als "Hub-and-Spoke-Topologie", es wird ein Designierter Router gewählt und Multicast zur Kommunikation verwendet.

Non-Broadcast Multi-Access (NBMA)

Point-to-Multipoint-Netzwerke, die kein Broadcast bzw. Multicast unterstützen, es wird ein Designierter Router gewählt und Unicast zur Kommunikation verwendet. Sämtliche Nachbarn müssen manuell konfiguriert werden.

Default-Wert:

Broadcast

Output-Kosten

Definiert die Kosten, um ein Paket auf dieser Schnittstelle zu senden, dargestellt in der Link State Metrik. Die Ankündigung erfolgt als Link-Kosten für diese Schnittstelle in den LSA-Nachrichten des Routers.

SNMP-ID:

2.93.3.4.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 4294967295

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

SNMP-ID:

2.93.3.4.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 4294967295

Transmit-Delay

Enthält die geschätzte Anzahl an Sekunden die benötigt wird, um ein Link-State-Update-Paket über diese Schnittstelle zu übertragen.

SNMP-ID:

2.93.3.4.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 4294967295

Router-Priorität

Die Priorität dieses Routers auf diesem Interface bei der Wahl zum Designierten Router (DR). Der Router mit der höchsten Priorität wird Designierter Router (Designated Router).

SNMP-ID:

2.93.3.4.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 255

Besondere Werte:

0

Der Wert 0 verhindert, dass der Router Designierter Router auf diesem Interface wird.

Hello-Intervall

Das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

SNMP-ID:

2.93.3.4.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 4294967295

Router-Dead-Intervall

Enthält die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben.

Dieser Wert muss größer als das Hello-Intervall sein.

SNMP-ID:

2.93.3.4.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

0 … 4294967295

Authentifizierungs-Typ

Authentifizierungsmethode, die für diese Schnittstelle verwendet wird.

SNMP-ID:

2.93.3.4.11

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

Null
Einfaches Passwort
Kryptographisch-MD5

Default-Wert:

Null

Authentifizierungs-Schlüssel

Authentifizierungsschlüssel für dieses Netzwerk, falls nicht der Authentifizierungstyp **Null** verwendet wird.

SNMP-ID:

2.93.3.4.12

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

16 Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

Passiv

Definiert, ob OSPF aktiv oder passiv auf dieser Schnittstelle arbeitet.

SNMP-ID:

2.93.3.4.13

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **OSPF-Schnittstellen**

Mögliche Werte:

Nein

Ja

Es werden keine Routing-Updates sowie Hello-Nachrichten von diesem Router auf dieser Schnittstelle versendet. Ebenso werden keine eingehenden OSPF-Nachrichten verarbeitet. Die entsprechende Route bzw. Netzwerk dieser Schnittstelle wird aber weiterhin in die LSDB eingefügt und damit auf anderen Schnittstellen angekündigt.

Default-Wert:

Nein

MTU Ignorieren

Deaktiviert die Überprüfung des MTU-Werts in Database Description Paketen. Dies ermöglicht, dass Router eine vollständige Nachbarschaftsbeziehung etablieren können, obwohl die MTU der entsprechenden Schnittstellen nicht einheitlich ist.

SNMP-ID:

2.93.3.4.14

Pfad Telnet:

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Virtuelle Links

In dieser Tabelle können Virtuelle Links (auch bezeichnet als Transit-Area) definiert werden. Grundsätzlich müssen bei OSPF alle Areas direkt mit der Backbone-Area verbunden sein. In Fällen, wo dies nicht möglich ist, können virtuelle Links verwendet werden. Ein virtueller Link verbindet einen Router durch eine Nicht-Backbone-Area mit der Backbone-Area.

SNMP-ID:

2.93.3.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.5.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Transit-Area-ID

Definiert die Area-ID der Transit-Area.

SNMP-ID:

2.93.3.5.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Router-ID

Definiert die Router-ID des Routers auf der Gegenseite des virtuellen Links.

SNMP-ID:

2.93.3.5.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Retransmit-Intervall

Enthält die Anzahl an Sekunden zwischen LSA-Wiederholungen (Retransmissions).

SNMP-ID:

2.93.3.5.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

0 … 4294967295

Hello-Intervall

Das Intervall in Sekunden, in dem dieser Router auf der Schnittstelle Hello-Nachrichten versendet.

SNMP-ID:

2.93.3.5.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

0 … 4294967295

Router-Dead-Intervall

Enthält die verstrichene Zeit, nach der ein Router als nicht mehr verfügbar gilt, seitdem seine Nachbarn zuletzt Hello-Nachrichten von ihm empfangen haben.

Dieser Wert muss größer als das Hello-Intervall sein.

SNMP-ID:

2.93.3.5.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

0 … 4294967295

Authentifizierungs-Typ

Authentifizierungsmethode, die für diese Schnittstelle verwendet wird.

SNMP-ID:

2.93.3.5.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

Null
Einfaches Passwort
Kryptographisch-MD5

Default-Wert:

Null

Authentifizierungs-Schlüssel

Authentifizierungsschlüssel für dieses Netzwerk, falls nicht der Authentifizierungstyp **Null** verwendet wird.

SNMP-ID:

2.93.3.5.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Virtuelle Links**

Mögliche Werte:

16 Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

NBMA-Nachbarn

Die Nachbarn Ihres Non-Broadcast-Multi-Access-Netzwerkes konfigurieren Sie im Menü **NBMA-Nachbarn**.

Non-Broadcast-Multiaccess-Netzwerke sind Netzwerke, in denen mehrere Router vorhanden sind, aber kein Broadcast unterstützt wird. OSPF emuliert in diesem Netzwerktyp den Betrieb in einem Broadcast-Netzwerk. In diesem Netzwerktyp wird ein Designierter Router gewählt.

Die Kommunikation findet nicht per Multicast statt, sondern per Unicast. Nachbarschaftsbeziehungen müssen manuell konfiguriert werden, da sich die Router nicht automatisch per Multicast finden können.

SNMP-ID:

2.93.3.6

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.6.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **NBMA-Nachbarn**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

SNMP-ID:

2.93.3.6.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **NBMA-Nachbarn**

Mögliche Werte:

Zeichen aus folgendem Zeichensatz: `[a-z A-Z 0-9 .]`

IP-Adresse

Enthält die IPv4-Adresse des Nachbar-Routers auf der Gegenseite.

SNMP-ID:

2.93.3.6.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **NBMA-Nachbarn**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Abfrage-Intervall

Definiert das Intervall, in dem Hello-Nachrichten zu diesem Router versendet werden.

SNMP-ID:

2.93.3.6.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **NBMA-Nachbarn**

Mögliche Werte:

0 … 4294967295

Besondere Werte:

0

Deaktiviert das Senden von Hello-Nachrichten.

Eignet sich als "Designierter Router"

Definiert, ob das lokale Gerät selbst als Designierter Router wählbar ist.

SNMP-ID:

2.93.3.6.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **NBMA-Nachbarn**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Point-To-Multipoint-Nachbarn

In dieser Tabelle konfigurieren Sie Ihre Point-To-Multipoint-Nachbarn.

In einem Point-To-Multipoint-Netzwerk werden alle Nachbarn so behandelt, als wären sie wie Point-To-Point-Nachbarn über ein Nicht-Broadcast-Netzwerk direkt miteinander verbunden.

Es wird kein Designierter Router gewählt, die Kommunikation erfolgt per Multicast.

SNMP-ID:

2.93.3.7

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.7.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Point-To-Multipoint-Nachbarn**

Mögliche Werte:

16 Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

OSPF-Schnittstelle

Enthält die Schnittstelle (IPv4-Netzwerk oder WAN-Gegenstelle), wo OSPF aktiviert werden soll.

SNMP-ID:

2.93.3.7.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Point-To-Multipoint-Nachbarn**

Mögliche Werte:

Zeichen aus folgendem Zeichensatz: `[a-z A-Z 0-9 .]`

IP-Adresse

Enthält die IPv4-Adresse des Nachbar-Routers auf der Gegenseite.

SNMP-ID:

2.93.3.7.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Point-To-Multipoint-Nachbarn**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

0.0.0.0

Abfrage-Intervall

Definiert das Intervall, in dem Hello-Nachrichten zu diesem Router versendet werden.

SNMP-ID:

2.93.3.7.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Point-To-Multipoint-Nachbarn**

Mögliche Werte:

0 … 4294967295

Besondere Werte:

0

Deaktiviert das Senden von Hello-Nachrichten.

BGP

Im Menü **BGP** konfigurieren Sie das Weiterverteilen von dynamisch gelernten Routen aus dem Border Gateway Protocol.

SNMP-ID:

2.93.3.8

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.8.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **BGP**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

BGP-Instanz

Enthält den Namen der BGP-Instanz.

SNMP-ID:

2.93.3.8.2

Pfad Telnet:

Routing-Protokolle > **OSPF** > **BGP**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

SNMP-ID:

2.93.3.8.3

Pfad Telnet:

Routing-Protokolle > **OSPF** > **BGP**

Mögliche Werte:

Konstante

Verwendet eine benutzerdefinierte konstante Metrik.

Protokoll

Verwendet den Wert "Lokale Präferenz" des BGP-Präfix.

Default-Wert:

Konstante

Metrik-Konstante

Enthält die Konstante für die OSPF-Metrik der importierten Routen.

Als Metrik-Quelle muss zuvor **Konstante** ausgewählt worden sein.

SNMP-ID:

2.93.3.8.4

Pfad Telnet:

Routing-Protokolle > **OSPF** > **BGP**

Mögliche Werte:

0 … 4294967295

Pfad-Typ

Definiert, als was für ein Typ die Routen in OSPF importiert werden.

SNMP-ID:

2.93.3.8.5

Pfad Telnet:

Routing-Protokolle > **OSPF** > **BGP**

Mögliche Werte:

Externer Typ 1

Im OSPF-Routing-Algorithmus grundsätzlich bevorzugt vor Externer Typ 2.

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante + Total Path Metrik, um diesen ASBR zu erreichen.

Externer Typ 2

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante.

Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

SNMP-ID:

2.93.3.8.6

Pfad Telnet:

Routing-Protokolle > **OSPF** > **BGP**

Mögliche Werte:

0 … 4294967295

Verbunden

Routen, die vom Betriebssystem automatisch in die Routing-Tabelle eingetragen werden, konfigurieren Sie in Menü **Verbunden**.

SNMP-ID:

2.93.3.9

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.9.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Verbunden**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

SNMP-ID:

2.93.3.9.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Verbunden**

Mögliche Werte:

Konstante

Verwendet eine benutzerdefinierte konstante Metrik.

Protokoll

Verwendet einen automatisch gesetzten Wert.

Default-Wert:

Konstante

Metrik-Konstante

Enthält die Konstante für die OSPF-Metrik der importierten Routen.

Als Metrik-Quelle muss zuvor **Konstante** ausgewählt worden sein.

SNMP-ID:

2.93.3.9.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Verbunden**

Mögliche Werte:

0 … 4294967295

Pfad-Typ

Definiert, als was für ein Typ die Routen in OSPF importiert werden.

SNMP-ID:

2.93.3.9.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Verbunden**

Mögliche Werte:

Externer Typ 1

Im OSPF-Routing-Algorithmus grundsätzlich bevorzugt vor Externer Typ 2.

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante + Total Path Metrik, um diesen ASBR zu erreichen.

Externer Typ 2

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante.

Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

SNMP-ID:

2.93.3.9.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Verbunden**

Mögliche Werte:

0 … 4294967295

Statisch

Routen, die manuell vom Benutzer in die Routing-Tabelle eingetragen werden, konfigurieren Sie im Menü **Statisch**.

SNMP-ID:

2.93.3.10

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF**

OSPF-Instanz

Enthält den Namen der OSPF-Instanz.

SNMP-ID:

2.93.3.10.1

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Statisch**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metrik-Quelle

Definiert, welche Quelle zum Setzen der OSPF-Metrik verwendet wird.

SNMP-ID:

2.93.3.10.2

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Statisch**

Mögliche Werte:

Konstante

Verwendet eine benutzerdefinierte konstante Metrik.

Protokoll

Verwendet einen automatisch gesetzten Wert.

Default-Wert:

Konstante

Metrik-Konstante

Enthält die Konstante für die OSPF-Metrik der importierten Routen.

Als Metrik-Quelle muss zuvor **Konstante** ausgewählt worden sein.

SNMP-ID:

2.93.3.10.3

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Statisch**

Mögliche Werte:

0 … 4294967295

Pfad-Typ

Definiert, als was für ein Typ die Routen in OSPF importiert werden.

SNMP-ID:

2.93.3.10.4

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Statisch**

Mögliche Werte:

Externer Typ 1

Im OSPF-Routing-Algorithmus grundsätzlich bevorzugt vor Externer Typ 2.

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante + Total Path Metrik, um diesen ASBR zu erreichen.

Externer Typ 2

Die OSPF-Metrik wird wie folgt gebildet:

Redistribution-Metrik bzw. Metrik-Konstante.

Tag für externe Route

Definiert, mit welchem External-Route-Tag die Routen importiert werden.

Der Wert wird von OSPF selbst nicht ausgewertet.

SNMP-ID:

2.93.3.10.5

Pfad Telnet:

Setup > **Routing-Protokolle** > **OSPF** > **Statisch**

Mögliche Werte:

0 … 4294967295

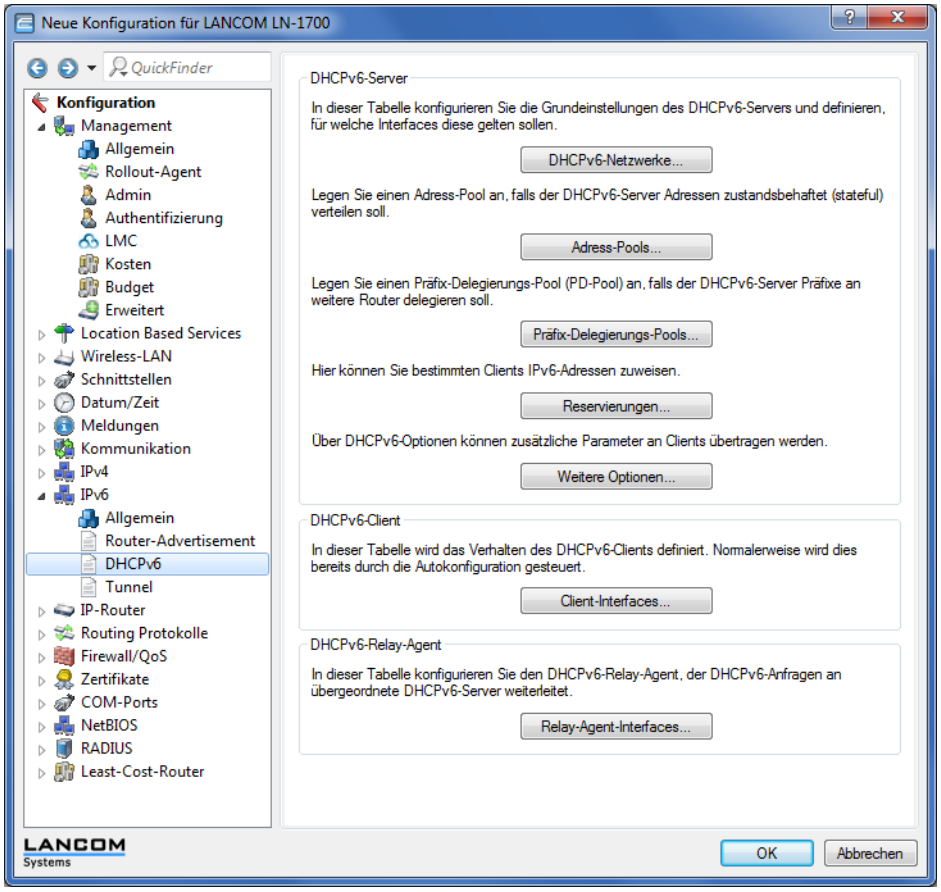
5 IPv6

5.1 Unterstützung für SNTP-Option im DHCPv6-Client

Ab LCOS-Version 10.12 kann der DHCPv6-Client beim DHCPv6-Server eine Liste von SNTP-Servern (Simple Network Time Protocol) anfragen.

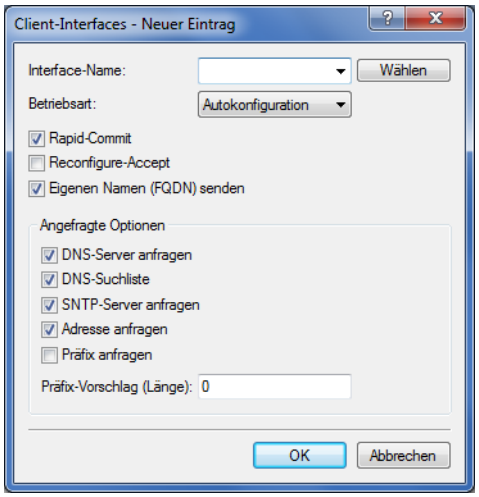
5.1.1 Konfiguration in LANconfig

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Navigieren Sie zu **IPv6** > **DHCPv6** > **DHCPv6-Client**.



3. Klicken Sie die Schaltfläche **Client-Interfaces**.

4. Klicken Sie die Schaltfläche **Hinzufügen**, um einen neuen Eintrag vorzunehmen oder **Bearbeiten**, um einen bereits existenten Eintrag zu bearbeiten.



5. Aktivieren Sie **SNTP-Server anfragen**, um das neue SNTP-Feature zu aktivieren.

5.1.2 Ergänzungen im Setup-Menü

SNTP-Anfragen

Legen Sie hier fest, ob der DHCPv6-Client beim DHCPv6-Server eine Liste von SNTP (Simple Network Time Protocol)-Servern anfragt.

Hierzu muss das regelmäßige Synchronisieren mit einem Timeserver aktiviert sein.

SNMP-ID:

2.70.3.2.1.10

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

Mögliche Werte:

0

Nein

1

Ja

Default-Wert:

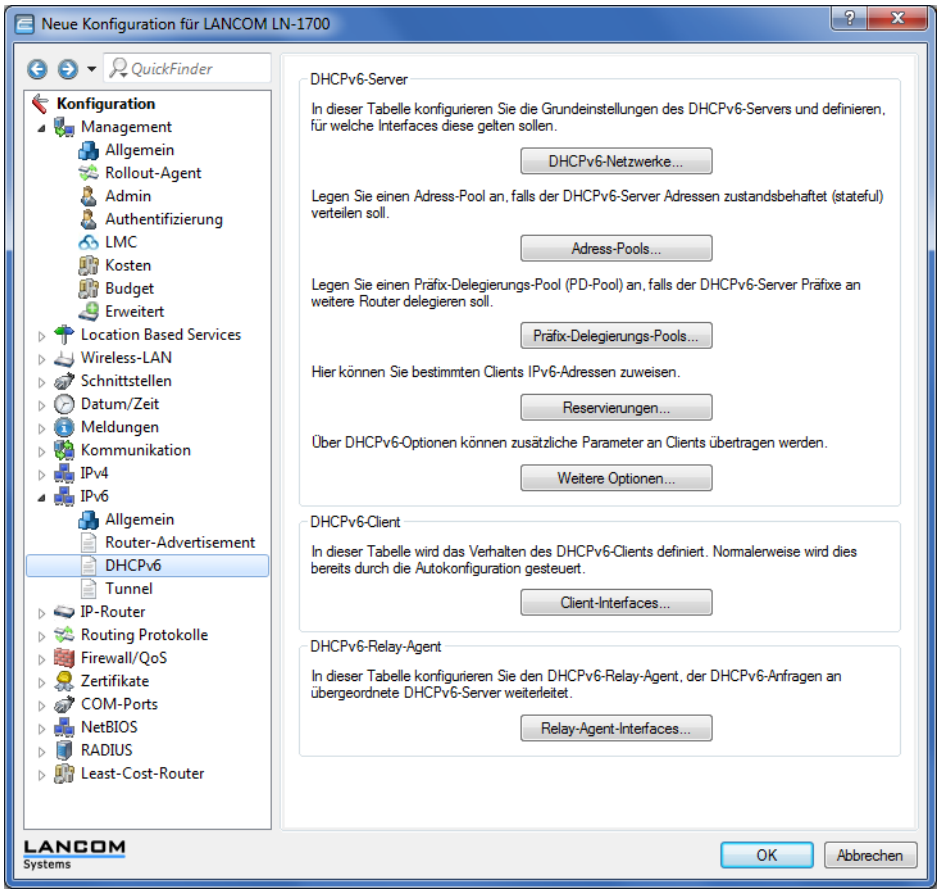
0

5.2 Unterstützung für Präfix-Vorschlag im DHCPv6-Client

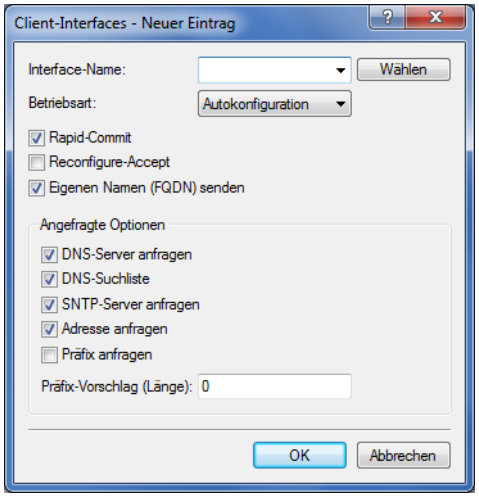
Ab LCOS-Version 10.12 kann der DHCPv6-Client beim DHCPv6-Server eine gewünschte Präfix-Länge anfragen, z.B. 56 oder 48 Bits. Der Server kann dem Client darauf das Präfix mit gewünschter Länge zuteilen.

5.2.1 Konfiguration in LANconfig

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Navigieren Sie zu **IPv6** > **DHCPv6** > **DHCPv6-Client**.



3. Klicken Sie die Schaltfläche **Client-Interfaces**.
4. Klicken Sie die Schaltfläche **Hinzufügen**, um einen neuen Eintrag vorzunehmen oder **Bearbeiten**, um einen bereits existenten Eintrag zu bearbeiten.



5. Tragen Sie Ihre gewünschte Präfixlänge in das Eingabefeld **Präfix-Vorschlag (Länge)** ein.

Um die gewünschte Präfixlänge an den DHCPv6-Server zu senden, muss zuvor Präfix anfragen aktiviert worden sein. Sie können einen dreistelligen Zahlenwert eingeben.

5.2.2 Ergänzungen im Setup-Menü

PD-Vorschlag

Hier legen Sie fest, ob der DHCPv6-Client beim DHCPv6-Server eine gewünschte Präfix-Länge anfragt.

SNMP-ID:

2.70.3.2.1.11

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-Liste**

Mögliche Werte:

Drei Zeichen aus folgendem Zeichensatz: `[0-9]`

5.3 Übermittlung des IPv6-LAN-Präfix in der Aktionstabelle

Ab LCOS-Version 10.12 stehen Ihnen zwei neue Variablen in der Aktionstabelle zur Verfügung.

Einige Dynamic DNS-Anbieter wie feste-ip.net und Dynv6.com können aus dem vom Router übermittelten IPv6-LAN-Präfix und den beim Anbieter hinterlegten Host-Identifiern der Clients im LAN vollwertige GUAs (Global Unicast Addresses) bilden, die über das Internet erreichbar sind. Hierzu wird der Host-Identifier vom Anbieter einfach an das übermittelte LAN-Präfix angehängt. Diese GUA wird vom Anbieter dann als AAAA-Record im DNS angeboten. Auf diese Weise kann man seine IPv6-fähigen Geräte im LAN über einen festen Hostnamen global erreichen, selbst wenn sich das IPv6-Präfix nach einer Zwangstrennung geändert hat.

Damit die gewünschten LAN-Clients tatsächlich von außen erreichbar sind, ist die IPv6-Firewall des LANCOM Routers passend mit entsprechenden Ausnahmen zu konfigurieren. Standardmäßig sind jegliche Verbindungsaufbauten von außen ins LAN verboten.

Tabelle 1: Folgende Variable können Sie in der Aktionstabelle nutzen:

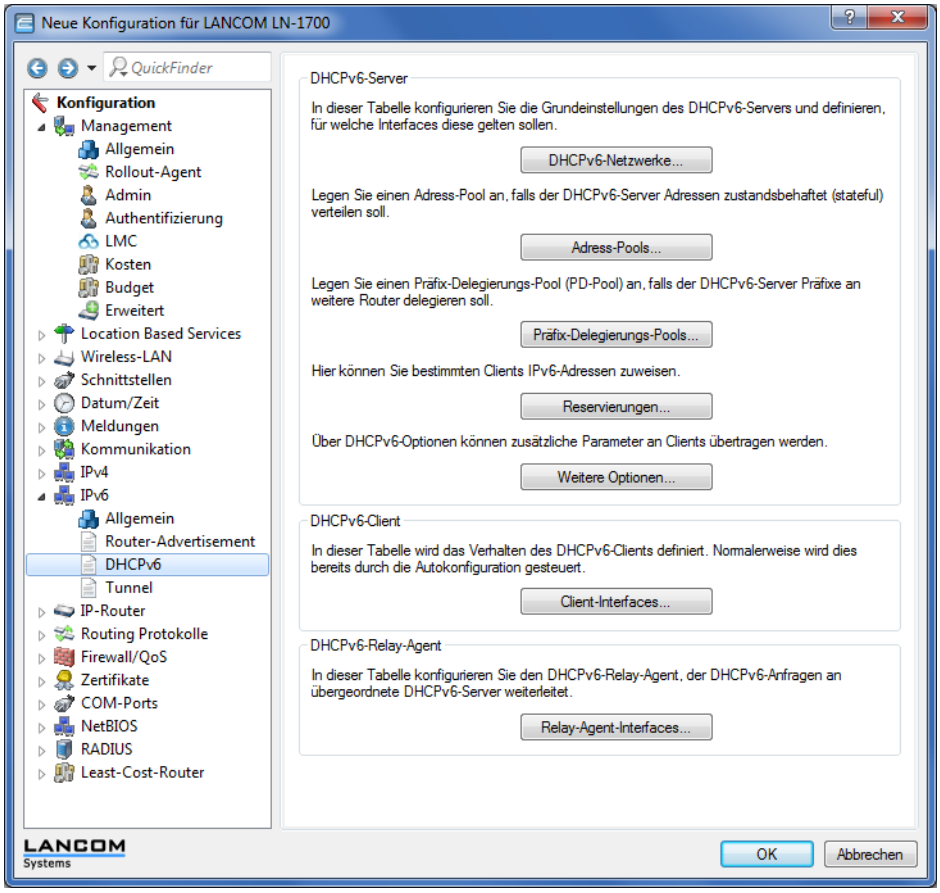
Variable	Bedeutung
%x	das aktuelle IPv6-LAN-Präfix als String im Format "fd00:0:0:1::/64"
%y	die aktuelle IPv6-LAN-Adresse des Geräts als String im Format "fd00::1:2a0:57ff:fa1b:9d7b"

5.4 DHCPv6-Optionen

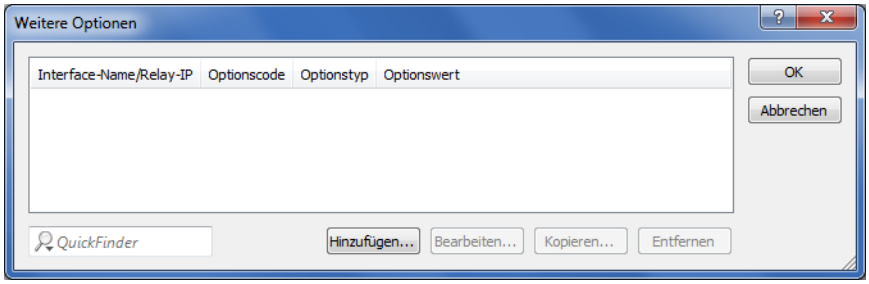
Ab LCOS-Version 10.12 kann der DHCPv6-Server seinen DHCPv6-Clients beliebige DHCPv6-Optionen übertragen.

5.4.1 Konfiguration in LANconfig

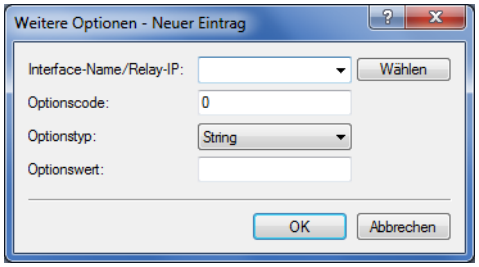
1. Navigieren Sie im Konfigurationsmenü zu **IPv6** > **DHCPv6** > **DHCPv6-Server**.



2. Klicken Sie die Schaltfläche **Weitere Optionen**.



3. Klicken Sie je nach Wunsch auf **Bearbeiten** oder auf **Hinzufügen**.



4. Bestimmen Sie den Namen der IPv6-Schnittstelle bzw. die entfernte IPv6-Adresse eines Relay-Agenten, für die der DHCPv6-Server die weitere Option verteilen soll, aus der Auswahlliste **Interface-Name/Relay-IP** .

Hinweis: Damit diese Option auch an Clients ausgeliefert wird, muss der Client den entsprechenden Optionscode auch in seiner Anfrage erfragen.

5. Tragen Sie den Code der DHCPv6-Option in das Eingabefeld **Optionscode** ein.
6. Legen Sie den Typ der DHCPv6-Option über die Auswahlliste **Optionstyp** fest.

Es stehen Ihnen mehrere Typen zur Auswahl:

- **String**: übernimmt die Zeichen als String.
- Alle weiteren Typen verwenden komma- und leerzeichenseparierte Listen, wobei leere Listenelemente ignoriert werden und eine leere Liste erlaubt ist und zu einer Option der Länge 0 führt.
- **Integertypen** sind dezimal, oktal mit vorangestellter 0 und hexadezimal mit vorangestelltem 0x ohne Beachtung der Groß-/Kleinschreibung einzugeben. Der Wertebereich geht bei Integer8 von -128 bis 127, bei Integer16 von -32768 bis 32767 und bei Integer32 von -2147483648 bis 2147483647, jeweils inklusive. Ein Vorzeichen + oder - ist generell zulässig.
- **IPv6Address** akzeptiert IPv6-Adressen ohne Beachtung der Groß-/Kleinschreibung in allen zulässigen Darstellungen, inklusive der gemischten IPv4/IPv6-Darstellung von Mapped-V4-Adressen (z.B. ::ffff:1.2.3.4).
- **Domain-List** akzeptiert alle Strings, die Labels ergeben, die höchstens 63 Zeichen lang sind. Leere Labels sind erlaubt, werden aber ignoriert. Eine Domain endet immer mit dem leeren Label 0.
- **Hexdump** erwartet in jedem Block nur Hexziffern ohne 0x-Präfix und füllt jeden Block ggf. mit einer führenden 0 zu gerader Länge auf und übernimmt anschließend den Block **Bigendian**.

7. Tragen Sie in das Eingabefeld **Optionswert** den Inhalt der DHCPv6-Option, formatiert entsprechend dem Optionstyp, ein.
8. Um die Konfiguration zu übernehmen, klicken Sie bitte die Schaltfläche **OK**.

5.4.2 Ergänzungen im Setup-Menü

Weitere Optionen

Dies ist die Tabelle **Weitere Optionen...** für den DHCP-Server.

Damit diese Option an Clients ausgeliefert wird, muss der Client den entsprechenden Optionscode auch in seiner Anfrage erfragen.

SNMP-ID:

2.70.3.1.8

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server**

Interface-Name-oder-Relay

Hier wählen Sie den Namen der IPv6-Schnittstelle oder die entfernte IPv6-Adresse eines Relay-Agenten, für die der DHCPv6-Server die weitere Option verteilen soll, aus.

SNMP-ID:

2.70.3.1.8.1

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Weitere-Optionen**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz:
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Optionscode

Tragen Sie hier den Code Ihrer DHCPv6-Option ein.

SNMP-ID:

2.70.3.1.8.2

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Weitere-Optionen**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Options-Typ

Wählen Sie hier den Typ Ihrer DHCPv6-Option.

SNMP-ID:

2.70.3.1.8.3

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Weitere-Optionen**

Mögliche Werte:

String

Die Zeichen werden als String übernommen. Bitte beachten Sie: Alle weiteren Typen verwenden komma- und leerzeichenseparierte Listen, wobei leere Listenelemente ignoriert werden und auch eine leere Liste erlaubt ist und zu einer Option der Länge 0 führt.

Integer8

Ein 8-Bit Integer von -128 bis 127 wahlweise dezimal, oktal mit Präfix '0' oder hexadezimal mit Präfix '0x'.

Integer16

Ein 16-Bit Integer von -32768 bis 32767.

Integer32

Ein 32-Bit Integer von -2147483648 bis 2147483647.

IPv6-Address

IPv6-Adressen ohne Beachtung der Groß-/Kleinschreibung in allen zulässigen Darstellungen inklusive der gemischten IPv4-/IPv6-Darstellung von Mapped-V4-Adressen wie z.B. ::ffff:1.2.3.4.

Domain-List

Alle Strings, die Labels ergeben, die höchstens 63 Zeichen lang sind. Leere Labels sind zulässig, werden aber ignoriert. Eine Domain endet grundsätzlich mit dem leeren Label 0.

Hexdump

Erwartet in jedem Block nur Hexziffern ohne 0x-Präfix und füllt jeden Block ggf. mit einer führenden 0 zu gerader Länge auf. Der Block wird als **Bigendian** übernommen.

Options-Wert

Hier tragen Sie den Inhalt Ihrer DHCPv6-Optionein. Der Inhalt muss entsprechend dem gewählten Optionstyp formatiert sein.

SNMP-ID:

2.70.3.1.8.4

Pfad Telnet:

Setup > **IPv6** > **DHCPv6** > **Server** > **Weitere-Optionen**

Mögliche Werte:

Je nach gewähltem Optionstypen Zeichen aus:

```
[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`
```

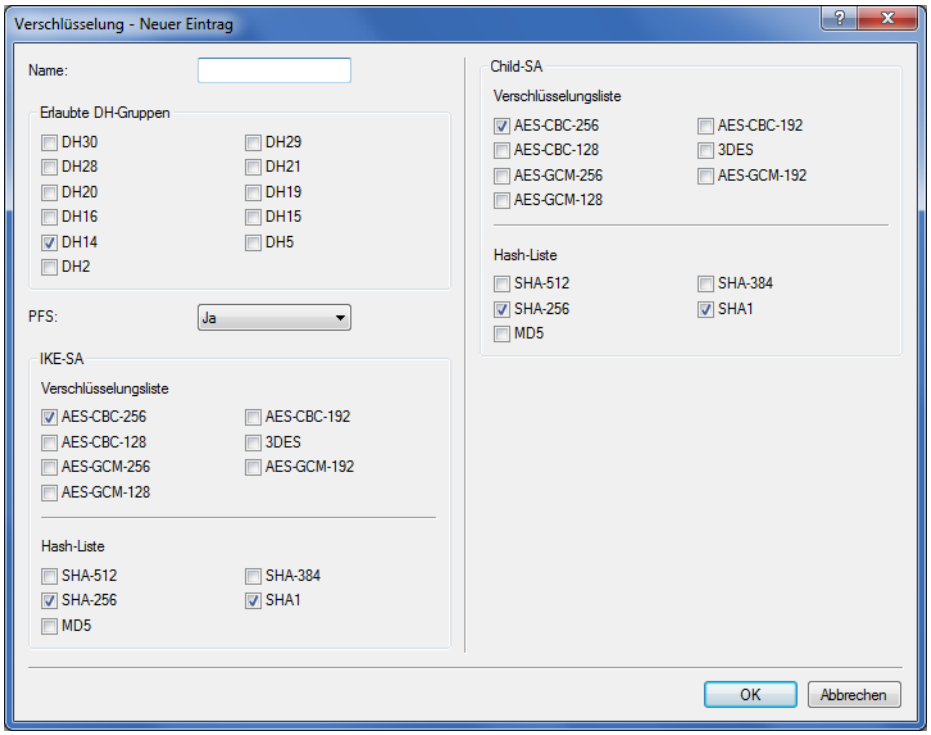
6 Virtual Private Networks - VPN

6.1 Erweiterung der IKEv2-Verschlüsselungsalgorithmen

Ab LCOS-Version 10.12 wird mit GCM (Galois/Counter Mode) ein weiterer Verschlüsselungsalgorithmus unterstützt.

Dieser Algorithmus ist besonders effizient und sorgt für ein spürbares Plus an Performance.

Zusätzlich stehen neue Gruppen für den Diffie-Hellmann-Schlüsselaustausch zur Verfügung, und zwar DH-19 bis DH-21 nach RFC5903 sowie DH-28 bis DH-30 nach RFC 6954.



Die neuen Gruppen für den Diffie-Hellmann-Schlüsseltausch:

- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)

Die Varianten des neu hinzugekommenen Galois/Counter Mode-Verschlüsselungsalgorithmus:

- AES-GCM-128
- AES-GCM-192
- AES-GCM-256

6.1.1 Ergänzungen im Setup-Menü

DH-Gruppen

Enthält die Auswahl der Diffie-Hellman-Gruppen.

SNMP-ID:

2.19.36.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschlüsselung**

Mögliche Werte:

DH30
(ab LCOS-Version 10.12)
DH29
(ab LCOS-Version 10.12)
DH28
(ab LCOS-Version 10.12)
DH21
(ab LCOS-Version 10.12)
DH20
(ab LCOS-Version 10.12)
DH19
(ab LCOS-Version 10.12)
DH16
DH15
DH14
DH5
DH2

Default-Wert:

DH14

IKE-SA-Verschlüsselungsliste

Gibt an, welche Verschlüsselungsalgorithmen aktiviert sind. Ab LCOS-Version 10.12 wird auch AES-GCM (Galois/Counter Mode) unterstützt.

SNMP-ID:

2.19.36.2.4

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschlüsselung**

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(ab LCOS-Version 10.12)
AES-GCM-192
(ab LCOS-Version 10.12)
AES-GCM-128
(ab LCOS-Version 10.12)

Default-Wert:

AES-CBC-256

AES-GCM-256

Child-SA-Verschlüsselungsliste

Gibt an, welche Verschlüsselungsalgorithmen in der Child-SA aktiviert sind. Ab LCOS-Version 10.12 wird auch AES-GCM (Galois/Counter Mode) unterstützt.

SNMP-ID:

2.19.36.2.6

Pfad Telnet:

Setup > **VPN** > **IKEv2** > **Verschlüsselung**

Mögliche Werte:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(ab LCOS-Version 10.12)
AES-GCM-192
(ab LCOS-Version 10.12)
AES-GCM-128
(ab LCOS-Version 10.12)

Default-Wert:

AES-CBC-256

AES-GCM-256

6.2 IKEv2 Load Balancer

Ab LCOS-Version 10.12 steht Ihnen der IKEv2 Load Balancer zur Verfügung. Mit ihm ist es möglich, eine beliebige Anzahl von VPN-Zentralen in Betrieb zu nehmen und die Anzahl der eingehenden VPN-Verbindungen auf diese sinnvoll und je nach Last zu verteilen.

Der IKEv2 Load Balancer ermöglicht es, eingehende IKEv2-Verbindungen abhängig von momentaner Auslastung / Anzahl VPN-Tunnel etc. sinnvoll auf andere Gateways zu verteilen. Um dies zu erreichen wird der IKEv2 Redirect Mechanismus verwendet.

In größeren VPN-Szenarien werden in der Regel redundante VPN-Gateways verwendet. Oft werden davon allerdings nicht alle Gateways gleichmäßig genutzt bzw. manche Gateways werden als Reserve für den Backup-Fall vorgehalten. Dies führt zu einer ungleichmäßigen Ressourcen-Auslastung der Gesamtinstallation.

Werden mehrere VPN-Gateways genutzt, so müssen diese Gateways auf allen Clients konfiguriert werden. Soll insbesondere ein neues VPN-Gateway installiert werden, so muss dieses Gateway auf allen Clients nachträglich konfiguriert werden. IKEv2 bietet mit dem Redirect-Mechanismus (RFC 5685) eine Erweiterung bei der ein VPN-Gateway einen Client auf ein anderes Gateway umleiten bzw. weiterleiten kann.

Auf Basis des IKEv2- Redirect-Mechanismus kann im Zusammenspiel mit VRRP ein hochverfügbarer IKEv2 Load Balancer für Enterprise-Szenarien erreicht werden.

Im ersten Schritt wird ein VRRP-Verbund auf allen beteiligen VPN-Gateways aktiviert. Die virtuelle VRRP-IP-Adresse ist gleichzeitig die Master-IP-Adresse des IKEv2-Load-Balancer-Verbundes. Die VPN-Gateways tauschen nun durch regelmäßige Status-Nachrichten per Multicast Informationen über ihre Last bzw. ihre Verfügbarkeit aus. Sollte der Master ausfallen, so wird automatisch ein anderes VPN-Gateway zum Master gewählt.

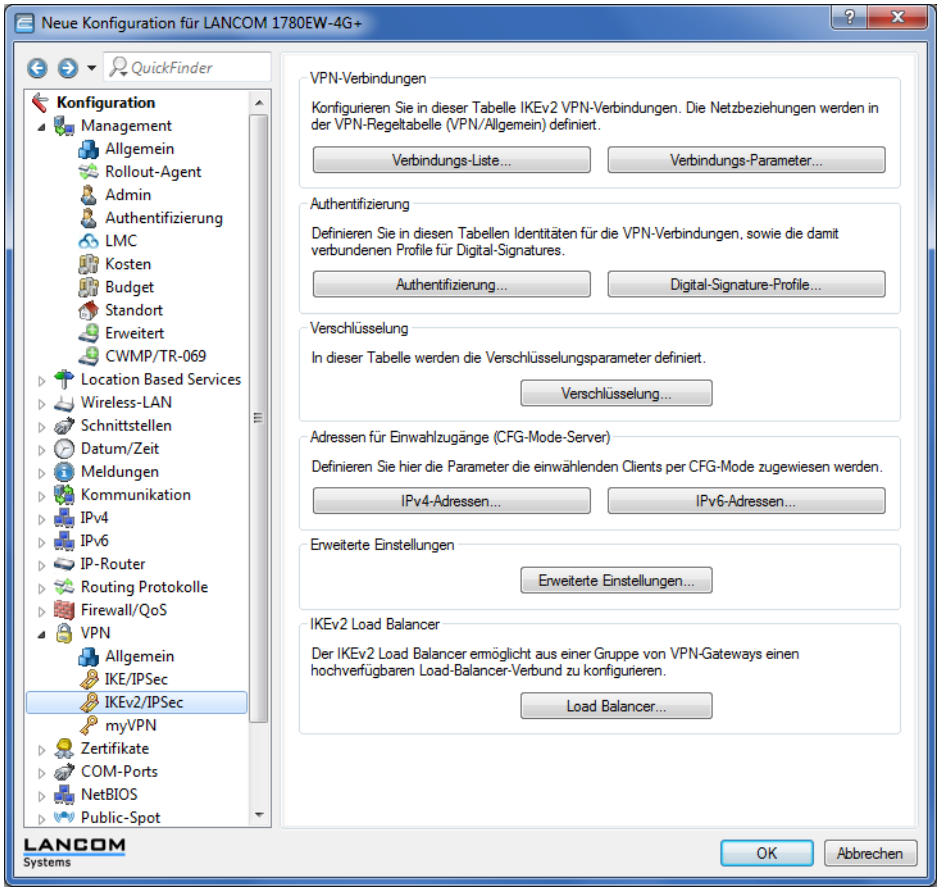
Auf den Clients wird nur noch die Master-IP-Adresse konfiguriert. Baut nun ein Client eine VPN-Verbindung zu dieser IP-Adresse auf, so prüft das Master Gateway die Last der VPN-Gateways und leitet den Client auf das Gateway mit der geringsten Last um. Dabei schickt das Master Gateway entweder ein Redirect in der IKE_SA_INIT-Antwort oder in der IKE-Auth-Phase. Die Umleitungsentscheidung wird anhand der freien VPN-Tunnel der beteiligen Gateways getroffen. Dabei wird der VPN-Client auf das VPN-Gateway mit der niedrigsten Anzahl an aktiven Tunneln umgeleitet.

Die virtuelle Gateway-Adresse dient somit nur für den ersten Kontakt mit anschließendem Redirect. Der Client baut dann den eigentlichen VPN-Tunnel zu einer anderen Gateway-Adresse auf.

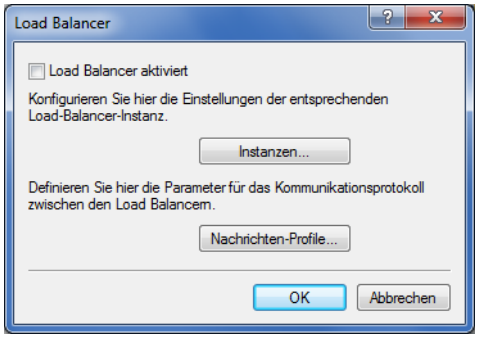
Folgende Randbedingungen sind zu beachten:

- VRRP wird für die automatische Wahl des Master-Gateways benötigt.
- Die beteiligten VPN-Gateways müssen eine gemeinsame Layer-2 Verbindung für VRRP und dem Austausch von Status-Nachrichten per Multicast haben.
- VRRP wird aktuell nur auf LAN-Schnittstellen unterstützt.
- Es wird ein vorgeschalteter Router (ggf. ebenfalls redundant ausgelegt) für den WAN-Zugang benötigt.
- Der Client muss IKEv2-Gateway Redirect nach RFC 5685 unterstützen (gilt aktuell für LANCOM Router und den LANCOM Advanced VPN-Client unter Windows).

In **LANconfig** konfigurieren Sie den IKEv2 Load Balancer unter **VPN** > **IKEv2/IPSec** > **IKEv2 Load Balancer**



im Menü **Load Balancer**.

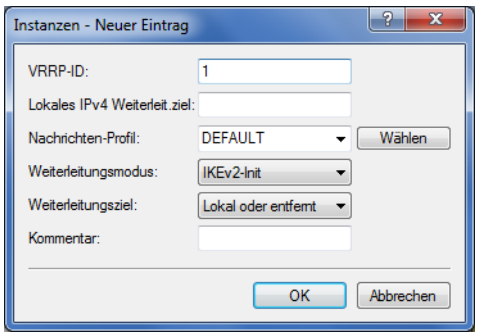


Load Balancer aktiviert

Aktiviert den IKEv2 Load Balancer.

6.2.1 Instanzen

Load-Balancer-Instanzen konfigurieren Sie in der Tabelle **Instanzen**.



VRRP-ID

VRRP-ID (Router-ID), die für diese IKEv2 Load-Balancer-Instanz verwendet werden soll. VRRP muss dazu auf diesem Gerät aktiviert und für diese VRRP-ID konfiguriert sein.

Mögliche Werte:

0 bis 255

Default: 1

Lokales IPv4 Weiterleitungsziel

IPv4-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet.

Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

Nachrichten-Profil

Nachrichten-Profil, das für diese Instanz verwendet werden soll. Das Nachrichten-Profil enthält die Parameter für das Status-Protokoll, mit dem das Gerät seine Status-Informationen an den Load-Balancer-Verbund kommuniziert.

Default: DEFAULT.

Weiterleitungsmodus

Definiert, in welcher Phase der IKEv2-Verhandlung das VPN-Gateway Clients auf ein anderes Gateway weiterleitet.

Dieser Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

Mögliche Werte:

IKEv2-Init (Default)

Die Redirect-Nachricht wird innerhalb der IKE_SA_INIT Antwort des VPN-Gateways gesendet.

IKEv2-Auth

Die Redirect-Nachricht wird innerhalb der IKE_AUTH-Phase gesendet, nachdem der Client sich beim VPN-Gateway identifiziert hat.

Weiterleitungsziel

Definiert das Weiterleitungsziel an das VPN-Clients weitergeleitet werden.

Der Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

Mögliche Werte:

Lokal oder Entfernte

Clients werden sowohl auf die eigene IP-Adresse des Geräts als auch auf andere entfernte Gateways des Verbunds umgeleitet.

Nur Entfernte

Clients werden nur auf andere VPN-Gateways weitergeleitet. Dies führt dazu, dass VPN-Clients gleichmäßig auf alle anderen Gateways mit Ausnahme des Master Gateways umgeleitet werden.

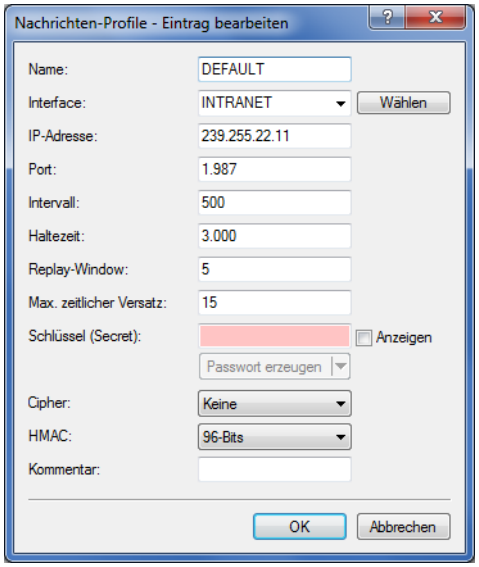
Hiermit lassen sich Szenarien konfigurieren, in denen der Load-Balancer-Master nur Clients verteilt, aber selbst keine VPN-Tunnel terminiert.

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

6.2.2 Nachrichten-Profile

Die Tabelle **Nachrichten-Profile** enthält die Parameter für das Status-Protokoll, mit dem VPN-Gateways ihre Status-Informationen an den Load-Balancer-Verbund kommunizieren.



Name

Eindeutiger Name für dieses Profil

Interface

Interface, auf dem der IKEv2 Load Balancer Statusnachrichten mit anderen VPN-Gateways des Verbunds austauscht.

Mögliche Werte:

Einträge aus der Tabelle IPv4-Netzwerke

IP-Adresse

Definiert die Multicast IP-Adresse zur Kommunikation der IKEv2 Load Balancer im lokalen Netzwerk.

Default: 239.255.22.11

Port

Definiert den Port zur Kommunikation der IKEv2 Load Balancer im lokalen Netzwerk.

Default: 1987

Intervall

Intervall (in Millisekunden), in dem Status-Nachrichten zwischen den IKEv2 Load Balancern ausgetauscht werden.

Mögliche Werte:

0 bis 65535

Default: 500

Haltezeit

Definiert die Zeit in Millisekunden, nach der das Gerät von anderen IKEv2 Load Balancern bei ausbleibenden Status-Nachrichten als deaktiviert vermerkt wird.

Die Haltezeit muss größer als das Intervall sein. Empfohlen wird der mindestens dreifache Wert des Parameters **Intervall**.

Mögliche Werte:

0 bis 65535

Default: 3000

Replay Window

Größe des Replay Windows (Anzahl Nachrichten) für Status-Nachrichten der IKEv2 Load Balancer. Nachrichten, die nicht mehr in das Replay Windows passen, werden bei Empfang verworfen.

Mögliche Werte:

1 bis 9

Default: 5

0

Deaktiviert die Replay Detection.

Max. zeitlicher Versatz

Maximal erlaubte zeitliche Abweichung (in Sekunden) der Zeitstempel in Status-Nachrichten der IKEv2 Load Balancer. Nachrichten mit einer höheren Abweichung werden bei Empfang verworfen.

Mögliche Werte:

0 bis 255

Default: 15

Schlüssel

Gemeinsames Passwort für das Kommunikationsprotokoll der Load Balancer.

Das Passwort muss auf allen VPN-Gateways eines Verbundes identisch sein.

Mögliche Werte:

Bis zu 32 beliebige Zeichen

Cipher

Definiert den verwendeten Verschlüsselungsalgorithmus für Status-Nachrichten der IKEv2 Load Balancer.

Mögliche Werte:

Keine (Default)

AES-128-GCM

AES-192-GCM

AES-256-GCM

HMAC

Definiert den verwendeten Signierungsalgorithmus für Status-Nachrichten der IKEv2 Load Balancer.

Mögliche Werte:

Keine

96 Bits (Default)

128 Bits

Kommentar

Geben Sie eine aussagekräftige Beschreibung für diesen Eintrag an.

6.2.3 Show-Commands über CLI

`show vlb-status`: Zeigt den Status der einzelnen Gateways im Verbund an.

6.2.4 Trace-Commands

Es stehen folgende Trace-Kommandos zur Verfügung:

- VLB-Status
- VLB-Packet

6.2.5 Ergänzungen im Setup-Menü

IKEv2 Load Balancer

Konfiguriert den IKEv2 Load Balancer.

SNMP-ID:

2.19.50

Pfad Telnet:

Setup > **VPN**

Aktiv

Aktiviert/deaktiviert den IKEv2 Load Balancer.

SNMP-ID:

2.19.50.1

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer**

Mögliche Werte:

Ja

Aktiviert den IKEv2 Load Balancer.

Nein

Deaktiviert den IKEv2 Load Balancer.

Default-Wert:

Nein

Instanzen

Load-Balancer-Instanzen konfigurieren Sie in der Tabelle **Instanzen**.

SNMP-ID:

2.19.50.2

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer**

VRRP-ID

VRRP-ID (Router-ID), die für diese IKEv2 Load-Balancer-Instanz verwendet werden soll. VRRP muss dazu auf diesem Gerät aktiviert und für diese VRRP-ID konfiguriert sein.

SNMP-ID:

2.19.50.2.1

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

0 … 255

Default-Wert:

1

Lokales IPv4 Weiterleitungsziel

IPv4-Adresse oder FQDN, auf dem das Gerät VPN-Tunnel annehmen soll. Auf diese Adresse wird ein VPN-Client durch den Master im Load-Balancer-Verbund weitergeleitet.

Hierbei handelt es sich nicht um die virtuelle VRRP-IP-Adresse.

SNMP-ID:

2.19.50.2.2

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Nachrichten-Profil

Nachrichten-Profil, das für diese Instanz verwendet werden soll. Das Nachrichten-Profil enthält die Parameter für das Status-Protokoll, mit dem das Gerät seine Status-Informationen an den Load-Balancer-Verbund kommuniziert.

SNMP-ID:

2.19.50.2.4

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Default-Wert:

DEFAULT

Weiterleitungsmodus

Definiert, in welcher Phase der IKEv2-Verhandlung das VPN-Gateway Clients auf ein anderes Gateway weiterleitet.

Dieser Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

SNMP-ID:

2.19.50.2.5

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

IKEv2-Init

Die Redirect-Nachricht wird innerhalb der IKE_SA_INIT Antwort des VPN-Gateways gesendet.

IKEv2-Auth

Die Redirect-Nachricht wird innerhalb der IKE_AUTH-Phase gesendet, nachdem der Client sich beim VPN-Gateway identifiziert hat.

Default-Wert:

IKEv2-Init

Weiterleitungsziel

Definiert das Weiterleitungsziel an das VPN-Clients weitergeleitet werden.

Der Parameter ist nur wirksam, falls das Gerät VRRP-Master ist.

Hiermit lassen sich Szenarien konfigurieren, in denen der Load-Balancer-Master nur Clients verteilt, aber selbst keine VPN-Tunnel terminiert.

SNMP-ID:

2.19.50.2.6

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

Lokal oder Entfernte

Clients werden sowohl auf die eigene IP-Adresse des Geräts als auch auf andere entfernte Gateways des Verbunds umgeleitet.

Nur Entfernte

Clients werden nur auf andere VPN-Gateways weitergeleitet. Dies führt dazu, dass VPN-Clients gleichmäßig auf alle anderen Gateways mit Ausnahme des Master Gateways umgeleitet werden.

Kommentar

Enthält einen Kommentar zu dieser Instanz.

SNMP-ID:

2.19.50.2.7

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Nachrichten-Profile

Die Tabelle **Nachrichten-Profile** enthält die Parameter für das Status-Protokoll, mit dem VPN-Gateways ihre Status-Informationen an den Load-Balancer-Verbund kommunizieren.

SNMP-ID:

2.19.50.3

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer**

Name

Eindeutiger Name für dieses Profil

SNMP-ID:

2.19.50.3.1

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Interface

Interface, auf dem der IKEv2 Load Balancer Statusnachrichten mit anderen VPN-Gateways des Verbunds austauscht.

SNMP-ID:

2.19.50.3.2

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

Einträge aus der Tabelle IPv4-Netzwerke

IP-Adresse

Definiert die Multicast IP-Adresse zur Kommunikation der IKEv2 Load Balancer im lokalen Netzwerk.

SNMP-ID:

2.19.50.3.3

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

IPv4-Adresse `[0-9.]`

Default-Wert:

239.255.22.11

Port

Definiert den Port zur Kommunikation der IKEv2 Load Balancer im lokalen Netzwerk.

SNMP-ID:

2.19.50.3.4

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

0 … 65535

Default-Wert:

1987

Intervall

Intervall (in Millisekunden), in dem Status-Nachrichten zwischen den IKEv2 Load Balancern ausgetauscht werden.

SNMP-ID:

2.19.50.3.5

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

0 … 65535

Default-Wert:

500

Haltezeit

Definiert die Zeit in Millisekunden, nach der das Gerät von anderen IKEv2 Load Balancern bei ausbleibenden Status-Nachrichten als deaktiviert vermerkt wird.

Die Haltezeit muss größer als das Intervall sein. Empfohlen wird der mindestens dreifache Wert des Parameters **Intervall**.

SNMP-ID:

2.19.50.3.6

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

0 … 65535

Default-Wert:

3000

Replay Window

Größe des Replay Windows (Anzahl Nachrichten) für Status-Nachrichten der IKEv2 Load Balancer. Nachrichten, die nicht mehr in das Replay Windows passen, werden bei Empfang verworfen.

SNMP-ID:

2.19.50.3.7

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

0 … 9

Default-Wert:

5

Besondere Werte:

0

Deaktiviert die Replay Detection.

Max. zeitlicher Versatz

Maximal erlaubte zeitliche Abweichung (in Sekunden) der Zeitstempel in Status-Nachrichten der IKEv2 Load Balancer. Nachrichten mit einer höheren Abweichung werden bei Empfang verworfen.

SNMP-ID:

2.19.50.3.8

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

0 … 255

Default-Wert:

15

Schlüssel

Gemeinsames Passwort für das Kommunikationsprotokoll der Load Balancer.

Das Passwort muss auf allen VPN-Gateways eines Verbundes identisch sein.

SNMP-ID:

2.19.50.3.9

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

32 Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Cipher

Definiert den verwendeten Verschlüsselungsalgorithmus für Status-Nachrichten der IKEv2 Load Balancer.

SNMP-ID:

2.19.50.3.10

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

Keine
AES-128-GCM
AES-192-GCM
AES-256-GCM

Default-Wert:

Keine

HMAC

Definiert den verwendeten Signierungsalgorithmus für Status-Nachrichten der IKEv2 Load Balancer.

SNMP-ID:

2.19.50.3.11

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Nachrichten-Profile**

Mögliche Werte:

Keine
96 Bits
128 Bits

Default-Wert:

96 Bits

Kommentar

Enthält einen Kommentar zu diesem Nachrichten-Profil.

SNMP-ID:

2.19.50.3.12

Pfad Telnet:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instanzen**

Mögliche Werte:

Zeichen aus nachfolgendem Zeichensatz `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

6.3 Flexibler Identitätsvergleich für PSK-Verbindungen

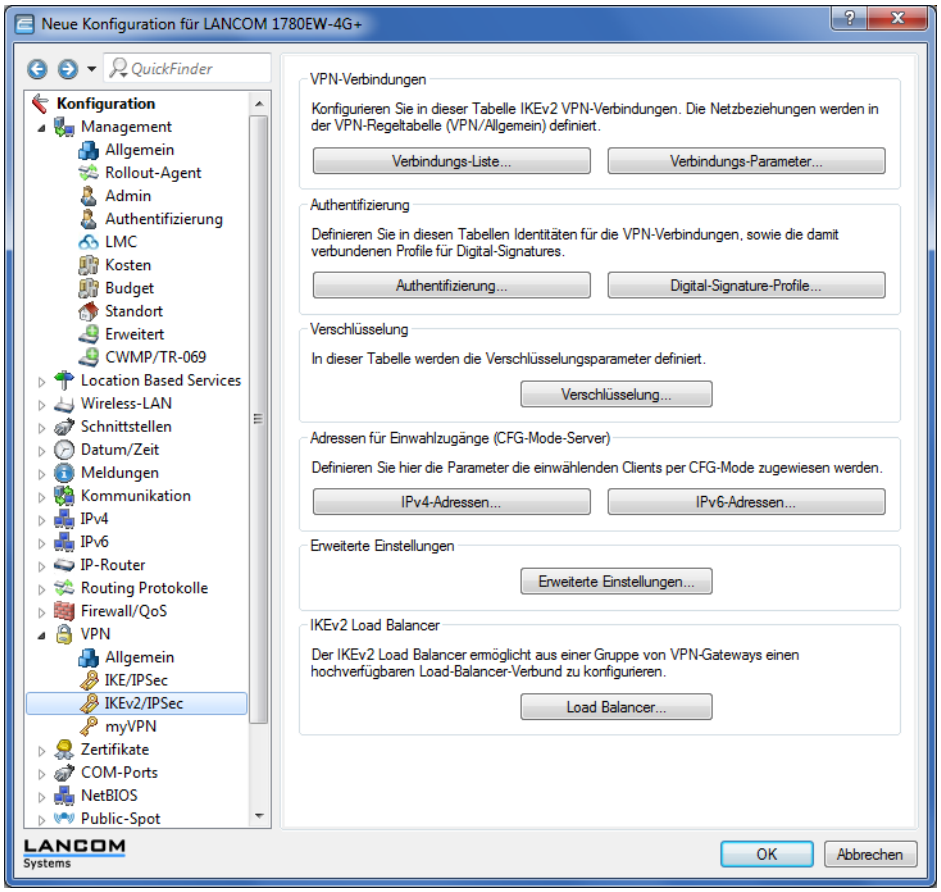
Ab LCOS-Version 10.12 wird der flexible Identitätsvergleich um PSK-Verbindungen (IKEv2) erweitert. Bisher war der Identitätsvergleich nur für zertifikatsbasierte VPN-Verbindungen möglich (Distinguished-Name).

Für die IKEv2-Identitäten wird das so genannte "Wildcard-Globbing" unterstützt. Hierbei wird '?' für genau ein beliebiges Zeichen und '*' für beliebig viele (inklusive Null) Zeichen benutzt.

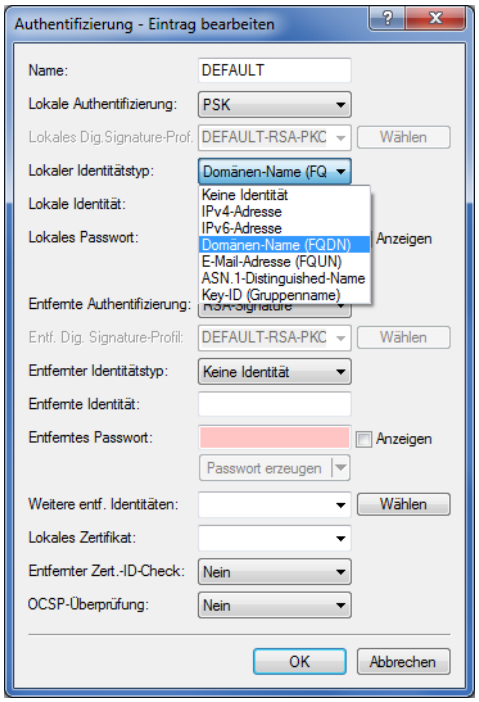
Dieses Feature ermöglicht Ihnen eine übersichtlichere VPN-Konfiguration, da für eingehende IKEv2-Verbindungen prinzipiell ein einziger Eintrag genügt.

Voraussetzung ist, dass alle eingehenden Verbindungen eine bestimmte Syntax verwenden und der flexible Vergleich aktiviert ist.

Sie konfigurieren den flexiblen Identitätsvergleich in **LANconfig** unter **VPN** > **IKEv2/IPSec** > **Authentifizierung** nach einem Klick auf die Schaltfläche **Authentifizierung**.



Für den flexiblen Identitätsvergleich für PSK-Verbindungen werden die beiden Identitätstypen **FQUN** und **FQDN** unterstützt.



Bitte beachten Sie, dass alle Parameter case-sensitive sind.

Auf der Kommandozeile erreichen Sie die Parameter über den Pfad **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

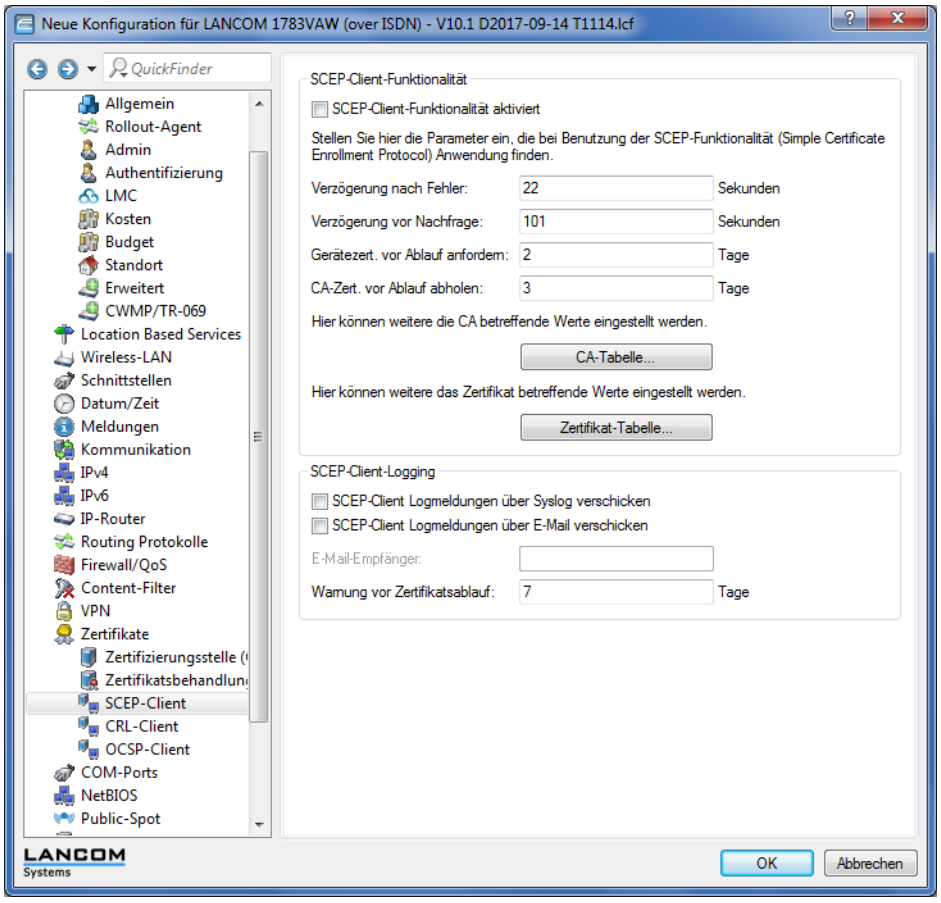
6.4 SCEP-Client-Logging

Ab LCOS-Version 10.12 haben Sie die Möglichkeit, per E-Mail bzw. SYSLOG-Meldung darüber zu informieren, dass das Zertifikat infolge einer gescheiterten Anfrage zur Zertifikatserneuerung abgelaufen ist.

Sie können auch vor Ablauf eines Sicherheitszeitraumes eine Warnmeldung herausgeben. Auf diese Weise verbleibt noch ein zeitlicher Puffer, um das Zertifikat rechtzeitig zu erneuern.

6.4.1 Konfiguration in LANconfig

Sie konfigurieren das neue Feature unter **Zertifikate** > **SCEP-Client** > **SCEP-Client-Logging**.



Die neuen Parameter:

SCEP-Client Logmeldungen über Syslog verschicken

Aktiviert/deaktiviert das Verschicken der Logmeldung über SYSLOG.

SCEP-Client Logmeldungen über E-Mail verschicken

Aktiviert/deaktiviert das Verschicken der Logmeldung per E-Mail.

Hierzu tragen Sie bitte eine E-Mail-Adresse in das folgende Eingabefenster ein.

E-Mail-Empfänger

E-Mail-Adresse zum Empfang der Logmeldung.

Um eine Eintragung vorzunehmen, muss zuvor **SCEP-Client Logmeldungen über E-Mail verschicken** aktiviert worden sein.

Warnung vor Zertifikatsablauf

Zeitintervall bis zum Ablauf des Zertifikates in Tagen.

7 Public Spot

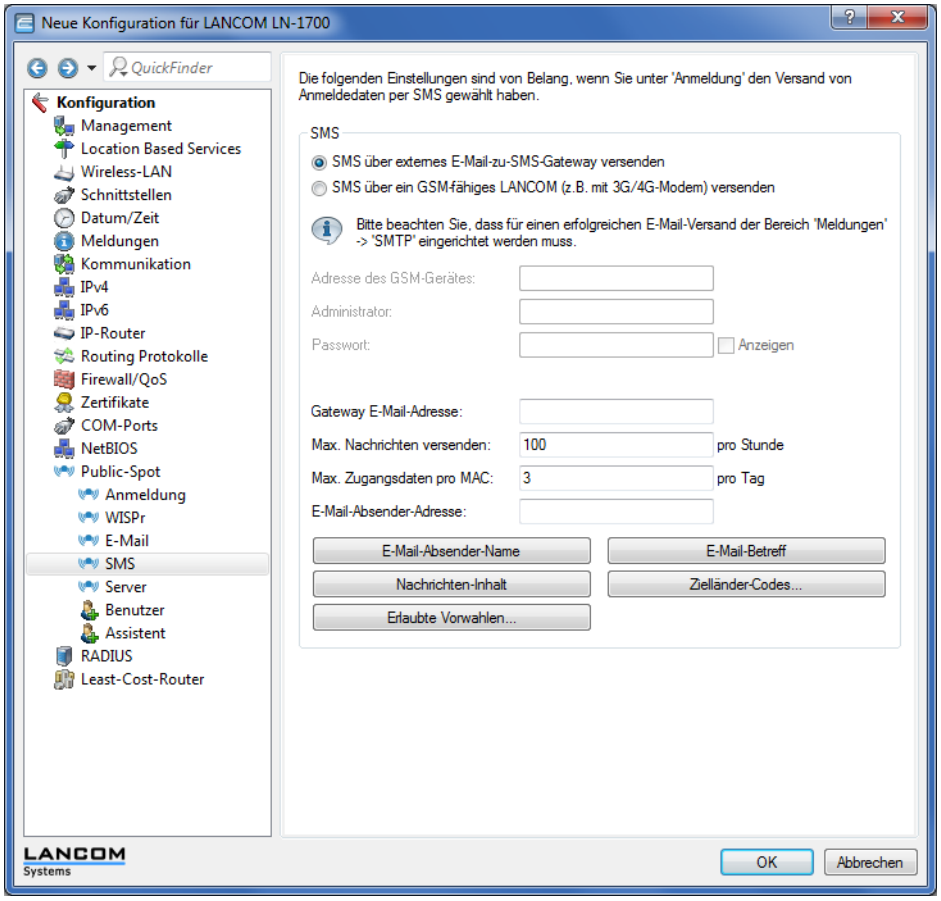
7.1 Selbständige Benutzeranmeldung (Smart Ticket)

7.1.1 Einschränkung der erlaubten Rufnummern-Vorwahlen bei Verwendung von Smart Ticket via SMS

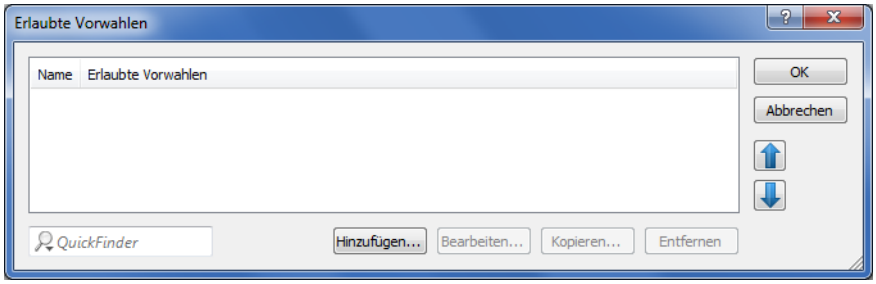
Ab LCOS-Version 10.12 haben Sie die Option, erlaubte Rufnummern-Vorwahlen auch landesspezifisch einzugrenzen.

Eine Einschränkung der erlaubten Rufnummern-Vorwahlen verhindert, dass teure Mehrwert- oder Servicerufnummern angegeben werden können, an die dann eine SMS generiert würde.

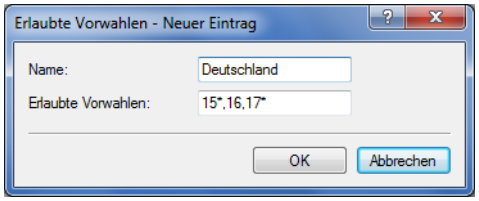
Sie können so unnötig hohe Kosten für die SMS-Anmeldung vermeiden.



1. Klicken Sie die Schaltfläche **Erlaubte Vorwahlen**.



2. Klicken Sie **Hinzufügen**.



3. Tragen Sie den Namen des Landes in das Eingabefeld **Name** ein.
4. Um den SMS-Versand auf bestimmte landesspezifische Vorwahlen zu beschränken, geben Sie die zulässigen Vorwahlen gefolgt von einem '*' in einer kommaseparierten Liste ein. Ein Beispiel für deutsche Mobilfunkanbieter: `15*, 16*, 17*`.

Wenn Sie für ein Land hier keine Eintragung vornehmen, so werden alle landesspezifischen Vorwahlen zugelassen. Zu dem jeweiligen Land muss zuvor ein Eintrag in der Tabelle Erlaubte-Landesvorwahlen angelegt worden sein.

7.1.2 Ergänzungen im Setup-Menü

Einschränkung der erlaubten Rufnummern-Vorwahlen bei Verwendung von Smart Ticket via SMS

In dieser Tabelle legen Sie die erlaubten landesspezifischen Vorwahlen für die Option Smart Ticket via SMS fest. Für das jeweilige Land muss zuvor ein Eintrag in der Tabelle Erlaubte-Landesvorwahlen angelegt worden sein.

SNMP-ID:

2.24.41.2.26

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung**

Landesname

Hier tragen Sie den Namen des Landes ein, für das Sie die erlaubten landesspezifischen Vorwahlen eingrenzen wollen, z. B. Deutschland oder DE.

Zu dem jeweiligen Land muss zuvor ein Eintrag in der Tabelle Erlaubte-Landesvorwahlen angelegt worden sein.

SNMP-ID:

2.24.41.2.26.1

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Erlaubte Prefixes**

Mögliche Werte:

max. 150 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

Deutschland

Erlaubte landesspezifische Vorwahlen

Hier tragen Sie für jedes Land aus der Liste Erlaubte-Landesvorwahlen ein, auf welche Vorwahlen(en) Sie die Verwendung von Smart Ticket via SMS eingrenzen wollen.

Wenn Sie für ein Land hier keine Eintragung vornehmen, so werden alle landesspezifischen Vorwahlen zugelassen.

SNMP-ID:

2.24.41.2.26.2

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **E-Mail2Sms-Authentifizierung** > **Erlaubte-Prefixes**

Mögliche Werte:

max. 50 Zeichen aus `[0-9 , *]`

Default-Wert:

15*,16*,17*

8 Konfiguration

8.1 Dateiimport auf der Konsole per Copy&Paste

Ab LCOS-Version 10.12 unterstützt Ihr Gerät das Laden von Dateien in Datei-Slots sowohl von der Konsole als auch aus einem Skript.

Somit können Dateien komfortabel per Skript zusammen mit der Konfiguration ausgerollt oder z.B. SSH-Schlüssel und VPN-Zertifikate importiert werden.

- Das entsprechende Dateiformat muss vom Typ Text bzw. ASCII sein, Binärformate werden nicht unterstützt.
- Bei Zertifikaten muss das Dateiformat entsprechend PEM-codiert (ASCII/Base64) sein. DER-codierte Zertifikate werden nicht unterstützt.

Syntax des CLI-Befehls **importfile**:

importfile -a <application> [-p <passphrase>] [-n] [-h <Hash> -f <Fingerprint>] [-c] [-r]

Notwendige Parameter:

-a <application>

<application> bestimmt den Speicherort und somit die Nutzung für die eingegebenen Daten. Für eine vollständige Liste der in Ihrem Gerät vorhandenen Speicherorte geben Sie **importfile -?** ein.

Optionale Parameter:

-n

-n startet den nicht-interaktiven Modus. Es gibt keine Eingabeaufforderungen oder andere Ausgaben auf der CLI. Der nicht-interaktive Modus ist für die Nutzung in Skripten vorgesehen.

-p <passphrase>

<passphrase> ist das Passwort, was zum Entschlüsseln eines eingegebenen privaten Schlüssels benötigt wird.

-h <hash>

Der Hash-Algorithmus, mit dem der Fingerprint des Root-CA-Zertifikats ermittelt wurde.

-f <fingerprint>

Der Fingerprint des Root-CA-Zertifikats, erstellt mit **–h**. Der Fingerprint kann sowohl mit Doppelpunkten eingegebenen werden, als auch ohne.

-c

Es werden nur CA-Zertifikate hochgeladen.

-r

Hochgeladene CA-Zertifikate ersetzen bereits vorhandene.

Mit STRG + Z kann eine aktive Eingabe abgebrochen werden.

Beispiel:

In diesem Beispiel ist die Eingabe des Benutzers in **Fett** dargestellt und Eingabeaufforderungen für den Benutzer in *Kursiv*. Zertifikate und weitere lange, mehrzeilige Ausgaben werden zur Übersichtlichkeit mit **[...]** abgekürzt. Am Ende des Beispiels finden Sie die Erläuterungen zu den einzelnen Schritten.

```
root@test:/
    importfile    -a    VPN2    -p    lancom    -h    SHA512    -f
4F:A7:5E:C9:D4:77:CE:D3:06:4C:79:93:D8:FA:3A:8E:7B:FE:19:61:B2:0C:37:4F:BB:7A:E6:46:36:04:46:EE:F6:DA:97:15:6B:BB:
2D:8F:B6:66:E6:7C:54:1E:B4:02:79:54:D6:DF:1E:9B:27:7C:9C:EA:B8:CB:1B:6D:90:1C

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device certificate, the end of the input will be
detected automatically:
importfile>-----BEGIN CERTIFICATE-----
importfile>MIID9DCCAtwCCQDgaoWRCmWaLjANBgkqhkiG9w0BAQ0FADAkMQswCQYDVQQG[…]
importfile>[…]s7pM5l0L0d0=
importfile>-----END CERTIFICATE-----
Importing device certificate:
        Version: 1 (0x0)
        Serial Number:
            e0:6a:85:91:0a:65:9a:2e
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jul  4 12:34:07 2017 GMT
            Not After : Oct  5 12:34:07 2024 GMT
        Subject: CN=TEST,O=Internet Widgits Pty Ltd,ST=Some-State,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:93:f6:b9:9a:41:b2:3e:30:2b:09:7f:d1:f9:
                    49:54:5a:82:c9:17:10:1f:79:6d:ab:55:df:b8[…]
                   […]2f:0c:8a:69:7b:a9:82:32:f3:ca:9c:02:20:14:
                    bd:8b:0d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha512WithRSAEncryption
         06:5b:a4:1a:a2:69:c1:bf:6f:b1:d2:6c:b0:21:e1:10:43:[…]
         […]50:e6:a3:1d:f3:15:b7:87:8c:65:2f:25:f6:b3:ba:4c:e6:
         5d:0b:d1:dd

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device private key, the end the input will be detected
 automatically:
importfile>-----BEGIN RSA PRIVATE KEY-----
importfile>Proc-Type: 4,ENCRYPTED
importfile>DEK-Info: AES-128-CBC,8FB95ED0568DA9AE17D7573BC294ACD8
importfile>[…]5Cuf2p798Obhw3isAe04XRwmdLno8ZcPDyB33ZKPjmhUzB0WsdzGdSSq5iYjD
importfile>-----END RSA PRIVATE KEY-----
The private key was read successfully.
The private key matches the device certificate.
The input can be aborted by pressing CTRL+Z.
Please enter the chain of PEM-encoded (Base64) CA certificates.
The input is closed with "endcachain":
importfile>-----BEGIN CERTIFICATE-----
importfile>MIIDGzCCAgOgAwIBAgIJAMlNxBFGQqpoMA0GCSqGSIb3DQEBDQUAMCQxCzAJB[…]
importfile>[…]EUDI9giYt9tnAT8hJfLkkyN/PHSiP+e+vopjSpKuyg==
importfile>-----END CERTIFICATE-----
importfile>endcachain
Importing CA certificate:
        Version: 3 (0x2)
        Serial Number:
            c9:4d:c4:11:46:42:aa:68
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
```

```
        Validity
            Not Before: Jun  6 13:56:49 2017 GMT
            Not After : Jun 19 13:56:49 2045 GMT
        Subject: CN=OCSP-TEST-CA,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:ba:04:74:7d:78:5a:84:b3:63:cc:ad:4d:[…]
                    […]14:0e:27:c8:8c:5a:00:a3:4c:ed:4f:02:e8:0b:
                    fb:07
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30
            X509v3 Authority Key Identifier:
                keyid:57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha512WithRSAEncryption
         c8:cf:3b:97:1a:56:61:13:9c:61:ed:21:23:7a:37:b4:a8:[…]
        […]3f:21:25:f2:e4:93:23:7f:3c:74:a2:3f:e7:be:be:8a:63:
         4a:92:ae:ca

Content of the PKCS12 file: private key: 1, device certificate: 1, CA certificates: 1
root@test:/
```

1. Es wird der Befehl importfile für den Speicherplatz VPN2 aufgerufen, somit handelt es sich um ein Zertifikat für die Nutzung im VPN. Das Passwort für den privaten Schlüssel ist lancom und das Root-CA-Zertifikat kann mit SHA512 und dem angegebenen Fingerprint geprüft werden.
2. Es folgt die Aufforderung an den Benutzer das Zertifikat einzugeben.
3. Nach Eingabe des Zertifikats wird dieses importiert.
4. Es folgt die Aufforderung an den Benutzer den privaten Schlüssel einzugeben.
5. Nach der Eingabe wird der Schlüssel geprüft.
6. Es folgt die Aufforderung an den Benutzer die Kette der CA-Zertifikate einzugeben. Das Ende der Eingabe wird nicht automatisch erkannt. Nach dem letzten Zertifikat muss das Ende über die Eingabe von endcachain ausgelöst werden. Geben Sie den Befehl in einer neuen Zeile ein, da alle Eingaben innerhalb der Zeile die Zeichenfolge **endcachain** enthält verworfen werden.
7. Nach der Eingabe werden die CA-Zertifikate importiert und der Vorgang abgeschlossen.

8.2 FirmSafe

8.2.1 Aktive Firmware über Konsolenbefehl umschalten

Ab LCOS-Version 10.12 kann mit einem Kommando die aktuelle Firmware auf die alternative Firmware umgeschaltet werden. Hierbei wird die zuvor inaktive Firmware auf "aktiv" gesetzt und die bislang aktive Firmware auf "inaktiv". Das Gerät führt nach Eingabe des Kommandos automatisch ohne weitere Bestätigung einen Neustart aus.

Geben Sie unter **/Firmware** den Befehl `do Switch-Firmware` ein.

Der Neustart wird automatisch ausgeführt.

8.2.2 Ergänzungen im Firmware-Menü

Firmware-umschalten

Hier schalten Sie via Kommandozeile die aktive Firmware um in den inaktiven Zustand. Entsprechend wird die alternative, nicht aktive Firmware in den aktiven Zustand geschaltet.

Das Gerät startet automatisch neu und verwendet sogleich die alternative Firmware. Durch nochmaliges Umschalten stellen Sie den Ausgangszustand wieder her.

SNMP-ID:

3.8

Pfad Telnet:

Firmware

Mögliche Werte:

`do Switch-Firmware`

Firmware umschalten und Gerät neu starten

9 Voice over IP - VoIP

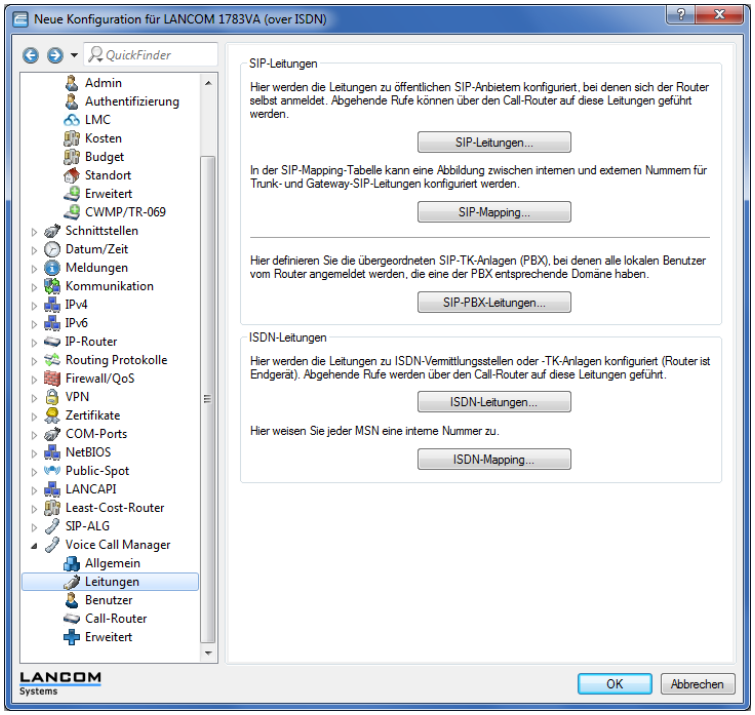
9.1 Übermittlung der Rufnummer bei VoIP-Verbindungen

9.1.1 SIP-Leitungen

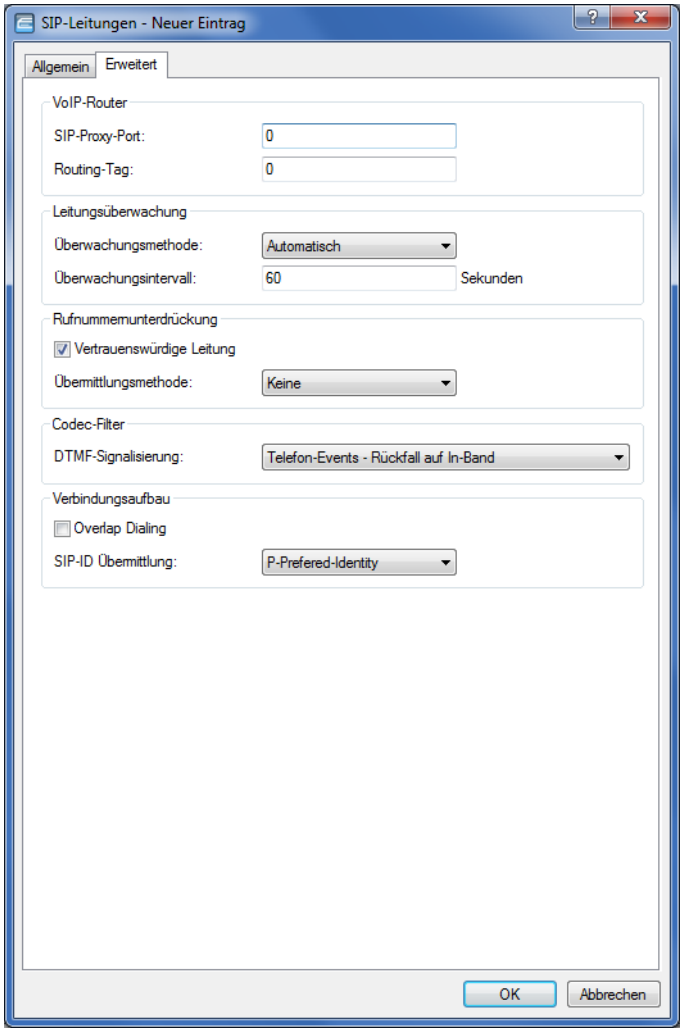
Um die eigene Rufnummer und die Anschlusskennung an den SIP-Trunk-Provider zu übermitteln, gibt es im SIP-Protokoll verschiedene Möglichkeiten. Somit muss die Übertragung der Informationen an den VoIP-Provider bei Bedarf angepasst werden.

Über den Schalter "SIP-ID Übermittlung" lässt sich ab LCOS-Version 10.12 der Aufbau des SIP-Paketes konfigurieren und somit das Feld, in dem die SIP-ID übertragen wird, festlegen.

In **LANconfig** konfigurieren Sie das neue Feature unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen**



unter **SIP-Leitungen** im Reiter **Erweitert**:



Die möglichen Werte des neuen Features:

- P-Preferred Identity (DEFAULT)
- FROM

9.1.2 Ergänzungen im Setup-Menü

User-Id-Field

Bestimmt das Feld, in dem die SIP-ID übertragen wird.

Damit das P-Preferred-Identity-Feld überhaupt übertragen wird, muss unter **Rufnummernunterdrückung** "Vertrauenswürdige Leitung" angeklickt werden und als **Übermittlungsmethode** "RFC3325" ausgewählt werden.

SNMP-ID:

2.33.4.1.1.39

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

P-Prefered Identity

Die SIP-ID des Anschlusses wird im P-Prefered-Identity-Feld übertragen.

Die Absenderkennung, die dem angerufenen übermittelt wird, wird in das FROM-Feld des SIP-Pakets eingetragen.

FROM

Die SIP-ID des Anschlusses wird im FROM-Feld übertragen.

Die Absenderkennung, die dem Angerufenen übermittelt wird, wird in das P-Prefered-Identity Feld des SIP-Pakets eingetragen.

Default-Wert:

P-Prefered Identity

9.2 Overlap Dialing für Geräte mit Voice Call Manager

Ab LCOS-Version 10.12 können Sie mittels Overlap Dialing die Wartezeit zwischen gewählter Rufnummer und Rufaufbau deutlich verkürzen.

Ihr LANCOM Gerät verwendet bei deaktiviertem Overlap Dialing einen Overlap-Timer. Werksseitig ist er fest auf 6 Sekunden eingestellt. Falls Sie nach Ablaufen des Timers keine weitere Ziffer gewählt haben, so wird die bis dahin eingegebene Rufnummer als vollständig angesehen und der Ruf aufgebaut.

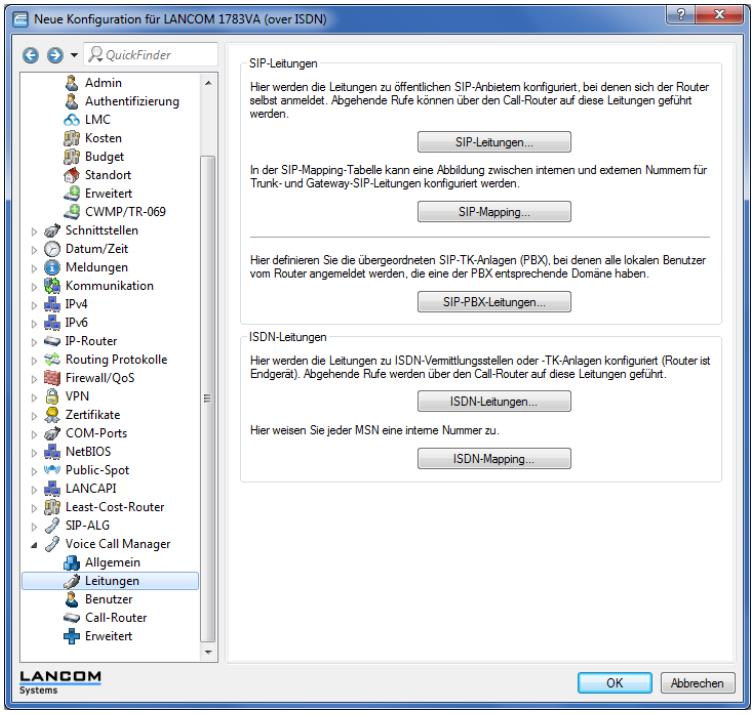
Ist Overlap Dialing für die Leitung aktiviert, werden schon vorab Teile der gewählten Rufnummer zum All-IP-Provider geschickt.

Antwortet der All-IP-Provider auf eine unvollständige Rufnummer mit einem "484 number incomplete", so sammelt der Voice Call Manager weiter gewählte Ziffern auf und schickt diese erneut zur Vermittlungsstelle.

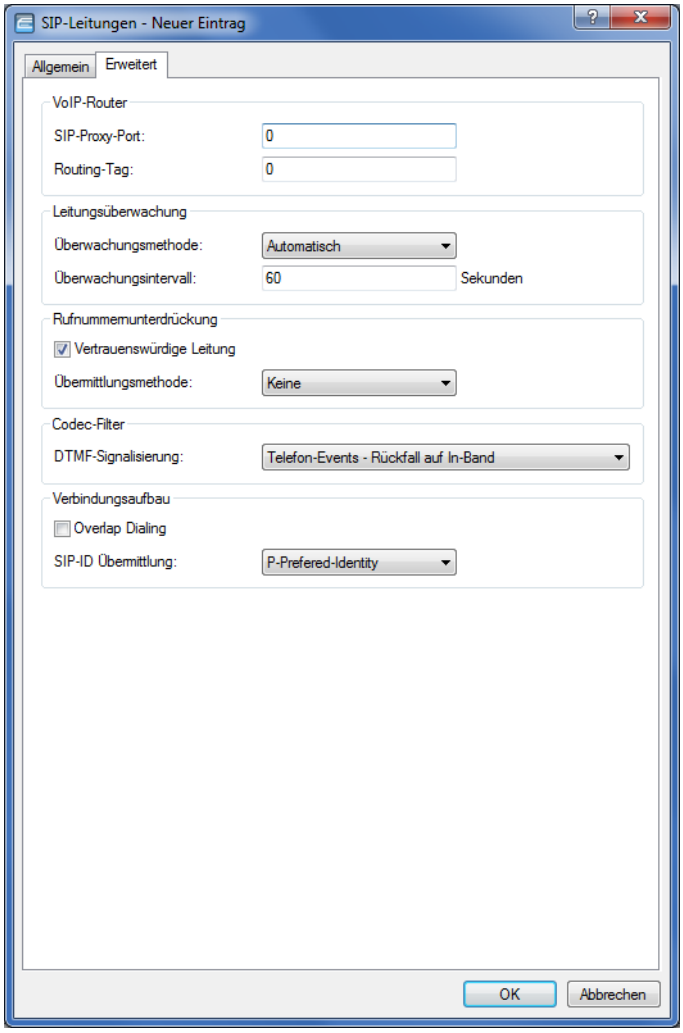
Auf diese Weise kann ohne den 6-Sekunden-Timer schnellstmöglich ein Ruf aufgebaut werden, wie Sie es von Ihrem ISDN-Anschluss gewohnt sind.

Da diese Funktionalität jedoch nicht von allen SIP-Providern unterstützt wird, ist das Overlap Dialing für jede einzelne SIP-Leitung zu konfigurieren.

In **LANconfig** konfigurieren Sie das neue Feature unter **Voice Call Manager** > **Leitungen** > **SIP-Leitungen**



unter **SIP-Leitungen** im Reiter **Erweitert**:



Die möglichen Werte des Features **Overlap Dialing**:

Deaktiviert

Deaktiviert das Overlap Dialing (Default).

Aktiviert

Aktiviert das Overlap Dialing.

9.2.1 Ergänzungen im Setup-Menü

Overlap-Dialing

Hier aktivieren bzw. deaktivieren Sie das Overlap-Dialing.

SNMP-ID:

2.33.4.1.1.36

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

0
Deaktiviert

1
Aktiviert

Default-Wert:

0

9.3 Rückfall von einer verschlüsselten auf eine unverschlüsselte VoIP-Verbindung

Ab LCOS-Version 10.12 verfügen Geräte mit Voice Call Manager über einen Rückfallmechansimus von einer verschlüsselten auf eine unverschlüsselte VoIP-Verbindung.

Nicht alle VoIP-Provider unterstützen an allen Anschlüssen verschlüsselte VoIP-Verbindungen. Sollen Standorte dennoch einheitlich konfiguriert werden, kann dieser Fallback-Mechanismus genutzt werden. Ist eine verschlüsselte Verbindung dann zu einem späteren Zeitpunkt möglich, wird diese vom LANCOM Router automatisch genutzt.

9.3.1 Ergänzungen im Setup-Menü

Fallback

Konfiguriert den Rückfallmechanismus für die SIP-Provider-Leitung.

SNMP-ID:

2.33.4.1.1.38

Pfad Telnet:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider** > **Line**

Mögliche Werte:

Nein
Es wird kein Rückfall auf eine unverschlüsselte Verbindung durchgeführt. Kann eine verschlüsselte Verbindung zum VoIP-Provider nicht aufgebaut werden, so bleibt die Leitung unregistriert.

UDP
In der Regel werden verschlüsselte SIP-Verbindungen über das TCP-Protokoll und unverschlüsselte Verbindungen über das UDP-Protokoll hergestellt. Mit dieser Einstellung wird direkt auf eine unverschlüsselte UDP-Verbindung gewechselt, wenn die verschlüsselte TCP-Verbindung nicht aufgebaut werden kann.

Complete
Wird eine verschlüsselte TCP-Verbindung mit der konfigurierten TLS-Version nicht aufgebaut, dann wird zunächst versucht, eine unverschlüsselte TCP- und zuletzt eine UDP-Verbindung aufzubauen, um die VoIP-Leitung zu registrieren.

Diese Einstellung bietet die beste Kompatibilität, führt aber unter Umständen zu einer längeren Registrierungszeit.

Default-Wert:

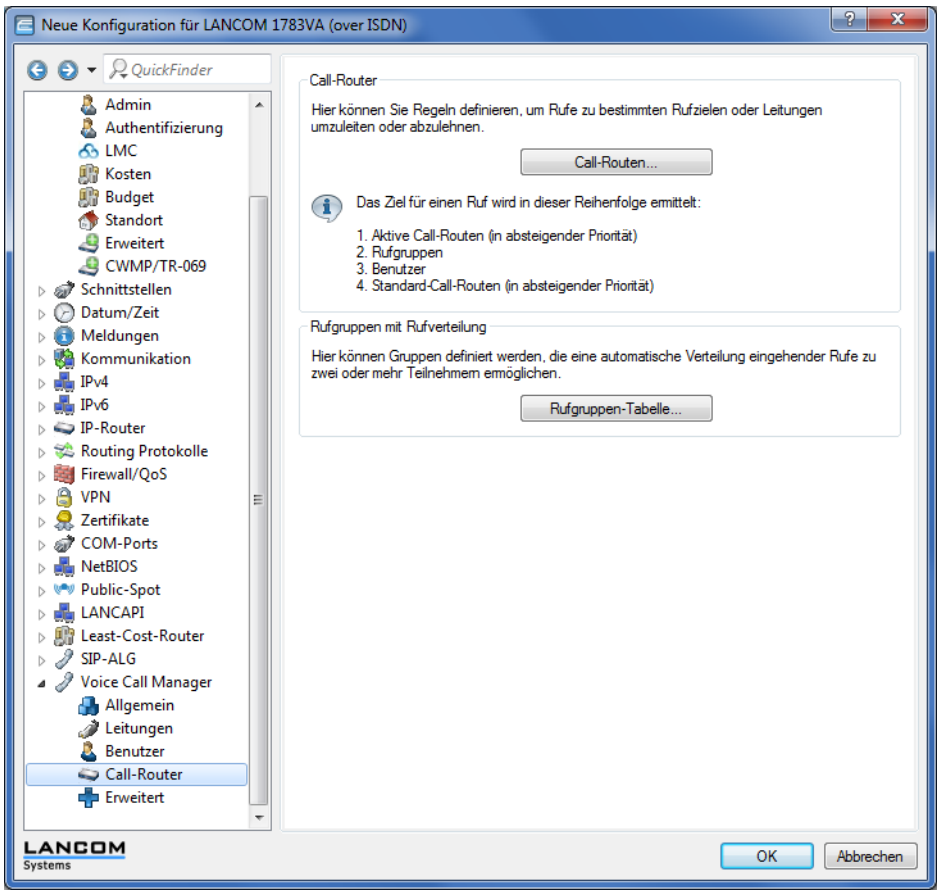
Nein

9.4 Steuercodes auf SIP-Leitungen verbieten

Ab LCOS-Version 10.12 haben Sie hier die Möglichkeit, Steuercodes nicht zuzulassen. Über Steuercodes können z.B. Rufumleitungen konfiguriert werden. Dies können Sie für beliebige Leitungen bzw. Mitarbeiter unterbinden.

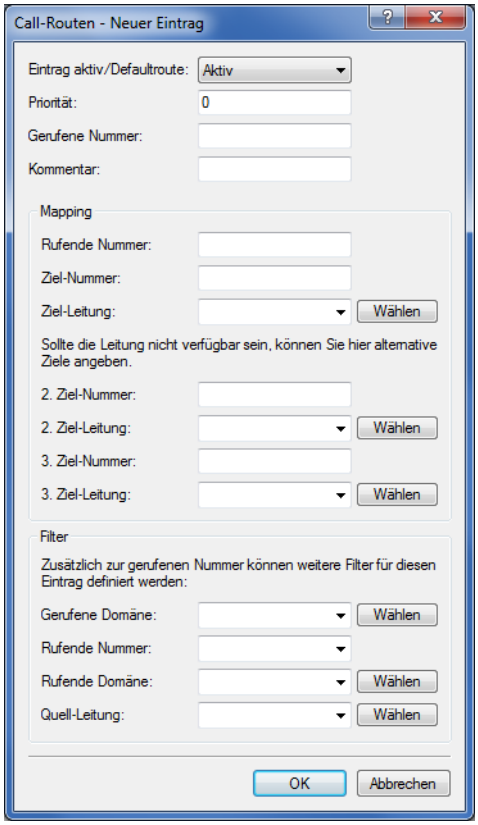
Hier ein Beispiel:

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.
2. Navigieren Sie zu **Voice Call Manager** > **Call-Router**.



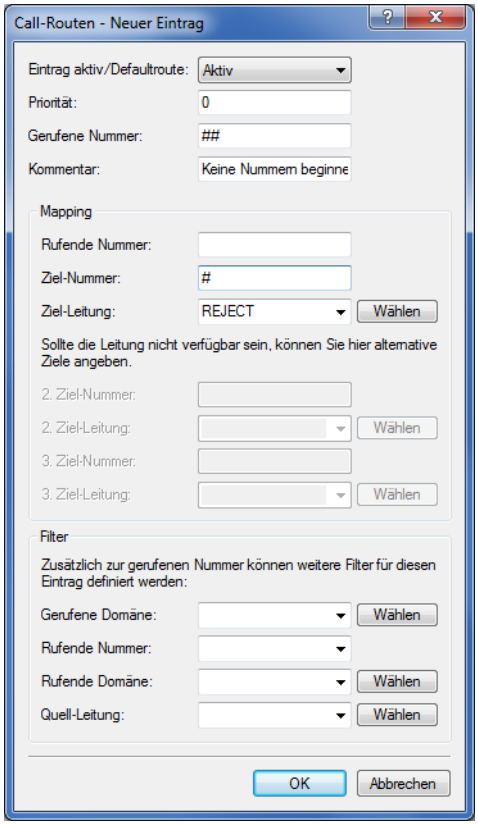
3. Klicken Sie die Schaltfläche **Call-Routen**.

4. Legen Sie eine neue Call-Route an.



5. Tragen Sie in **Gerufene Nummer:** ## ein.
6. Tragen Sie in **Ziel-Nummer:** # ein.
7. Wählen Sie für **Ziel-Leitung** REJECT.

8. Machen Sie in **Kommentar:** z. B. den Eintrag "Keine Nummern beginnend mit #".



9. Übernehmen Sie Ihre Einstellungen durch einen Klick auf die Schaltfläche **OK**.

10 Diagnose

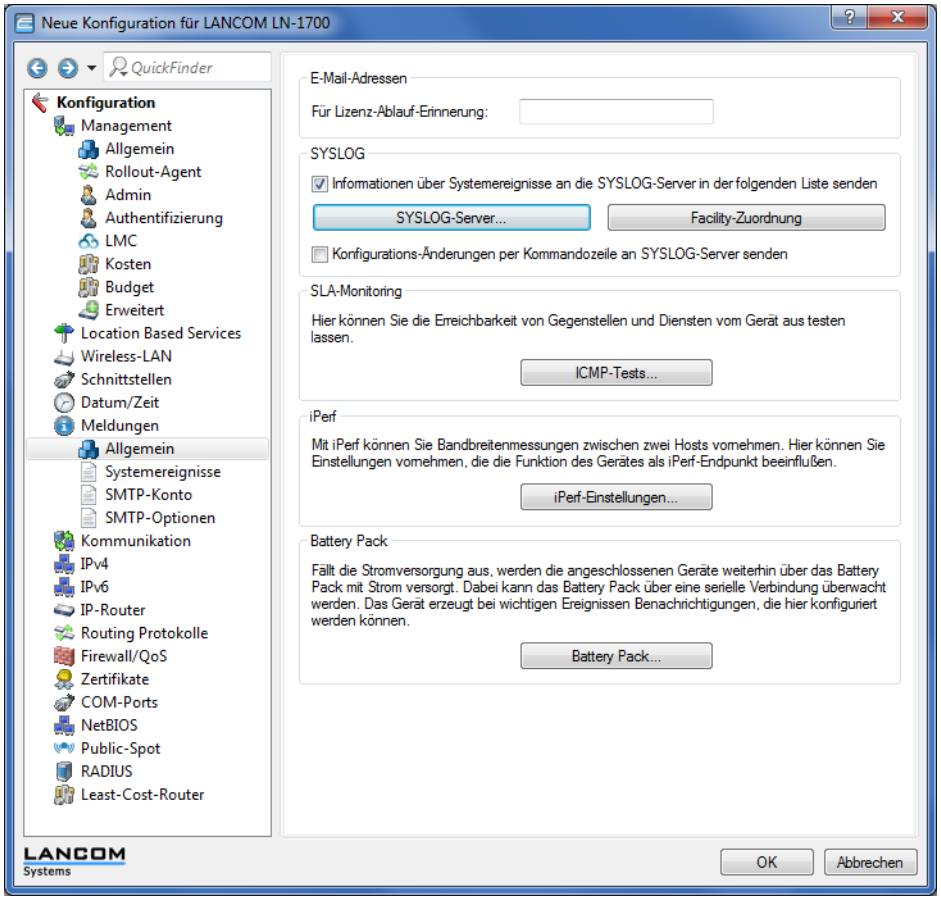
10.1 SYSLOG-Meldung über TCP

Ab LCOS-Version 10.12 kann der SYSLOG-Client seine SYSLOG-Meldung auch per TCP an einen SYSLOG-Server senden.

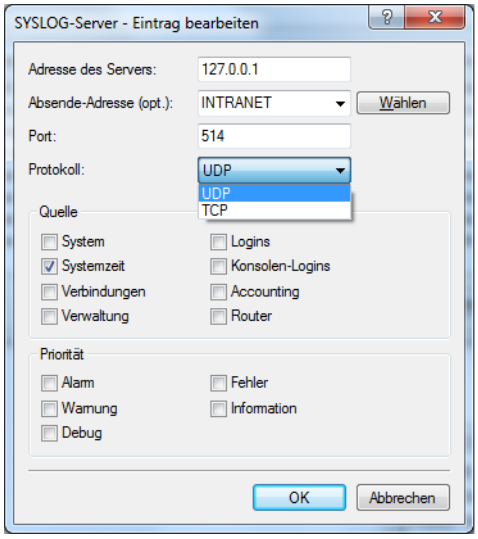
Bei einer Übertragung per TCP wird für jedes Datenpaket überprüft, ob es vollständig und unverändert an der Zieladresse angekommen ist.

10.1.1 Konfiguration in LANconfig

1. Starten Sie LANconfig und öffnen Sie den Konfigurationsdialog Ihres Gerätes.



2. Wechseln Sie in den Dialog **Meldungen** > **Allgemein** und öffnen Sie die Tabelle **SYSLOG-Server**.



3. Tragen Sie in das Eingabefeld **Port** 514 ein.
4. Wählen Sie in der Auswahlliste **Protokoll** TCP.

10.1.2 Ergänzungen im Setup-Menü

Port

Dieser Eintrag enthält den für SYSLOG verwendeten Port.

SNMP-ID:

2.22.2.8

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

514

TCP/UDP

Default-Wert:

514

Protokoll

Dieser Eintrag enthält das für SYSLOG verwendete Protokoll.

SNMP-ID:

2.22.2.9

Pfad Telnet:

Setup > **SYSLOG** > **Tabelle-SYSLOG**

Mögliche Werte:

TCP
UDP

Default-Wert:

UDP

10.2 IPv4- / IPv6-Traffic-Accounting

Ab LCOS-Version 10.12 erfasst die Layer-7-Anwendungserkennung auch separat IPv4- und IPv6-Traffic.

Ein gesondertes Einschalten dieses Features ist nicht erforderlich. Bei aktiver Layer-7-Anwendererkennung werden automatisch sowohl IPv4- als auch IPv6-Anwendungen separat aufgelöst.

Die Layer-7-Anwendungserkennung erfasst, zusätzlich zur ihrer Kernaufgabe, das Protokoll des über die entsprechende Schnittstelle übertragenen Traffics.

Für die Darstellung dient folgende Statustabelle:

```
root@LN-1700Esc:/Status/Layer-7-App-Detection/Total-Traffic-per-Protocol
> ls -a

[1.3.6.1.4.1.2356.11][1.95.8]
Protocol-Name  Tx-KBytes  Rx-KBytes  Tx-KBytes-Curr.-Day  Rx-KBytes-Curr.-Day
[1]            [2]        [3]        [4]                  [5]
===============-------------------------------------------------------------
IPv4            522        259        522                  259
IPv6            2696       18         2696                 18
```

Der eingehende (RX) und der ausgehende (TX) Traffic werden zwischen IPv4 und IPv6 unterschieden und in KBytes gemessen aufgelistet.

10.2.1 Ergänzungen im Status-Menü

Gesamter-Traffic-pro-Protokoll

Diese Tabelle präsentiert den ein- wie ausgehenden IPv4- / IPv6-Traffic in KBytes.

SNMP-ID:

1.95.8

Pfad Telnet:

Status > **Layer-7-Anwendungserkennung**

Mögliche Werte:

0 … 4294967295

11 Schnittstellen-Bündelung mit LACP

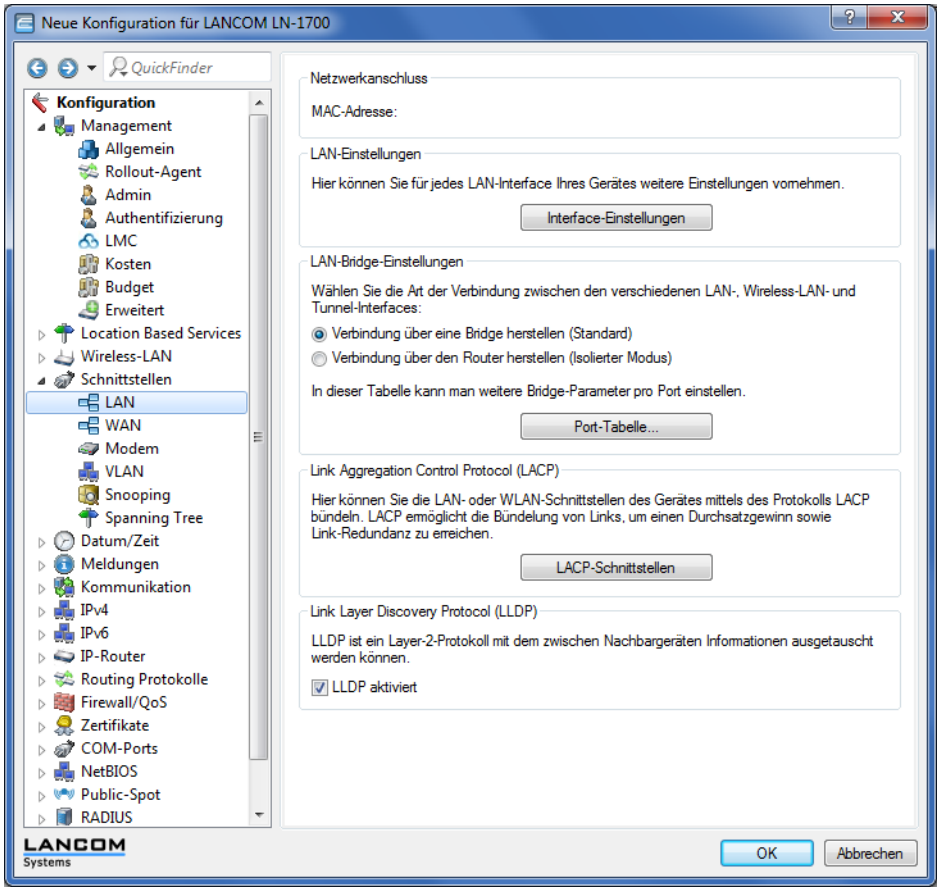
Einen enormen Mehrwert in puncto Ausfallsicherheit und Performance bietet Ihnen der mit LCOS-Version 10.12 unterstützte Standard LACP (Link Aggregation Control Protocol). LACP ermöglicht Ihnen die Bündelung von Ethernet-Ports zu einem virtuellen Link. Physikalische Ethernet-Verbindungen lassen sich zu einer logischen Verbindung zusammenfassen, sodass die Geschwindigkeit der Datenübertragung stark erhöht und die verfügbare Bandbreite optimal ausgenutzt wird.

Ein Datendurchsatz von über 1 GBit/s netto pro AP wird z. B. mit 11ac Wave 2 (4x4 MIMO) erreicht.

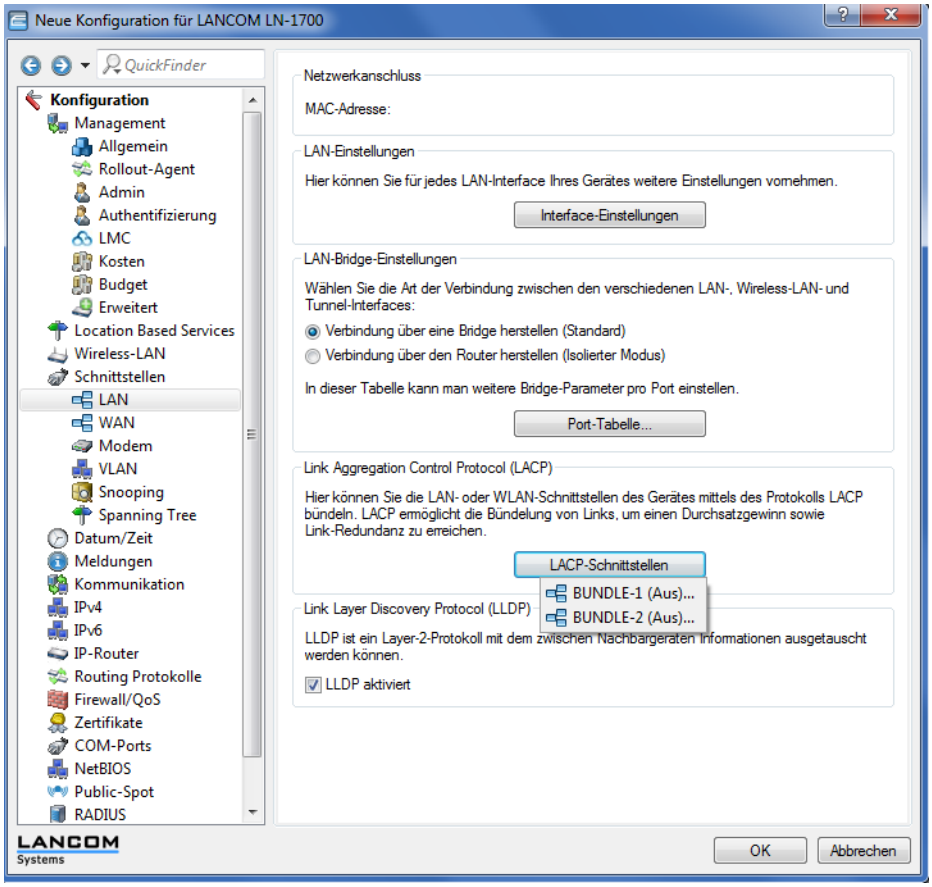
Neben einem echten Performance-Gewinn im Netzwerk dient LACP zugleich als ideale Redundanzoption, denn sobald eine physikalische Verbindung ausfällt, wird der Datenverkehr auf der anderen Leitung weiterhin übertragen.

11.1 Konfiguration der LACP-Schnittstellen

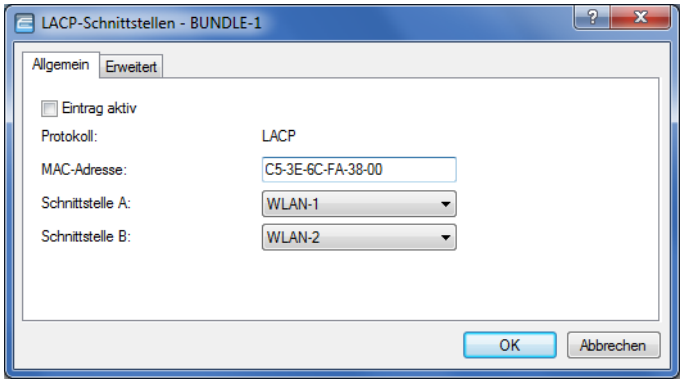
In LANconfig konfigurieren Sie LACP-Schnittstellen unter **Schnittstellen** > **LAN** im Abschnitt **Link Aggregation Control Protocol**.



1. Klicken Sie die Schaltfläche **LACP-Schnittstellen**, um auf die Liste der verfügbaren Bündel zuzugreifen.



2. Wählen Sie ein Bündel aus.



3. Tragen Sie die MAC-Adresse des Gerätes in das Eingabefeld **MAC-Adresse** ein.

> Die MAC-Adresse wird benutzt, um den LACP-Partner innerhalb der LAG zu identifizieren. Bleibt sie leer bzw. 0, wird automatisch die LAN-MAC-Adresse des Gerätes gesetzt. Die MAC-Adresse muss nicht zwingend zu einer Schnittstelle des Bundle gehören. Bei einem Konfig-Reset wird automatisch die systemweite MAC-Adresse dort als Default eingetragen.

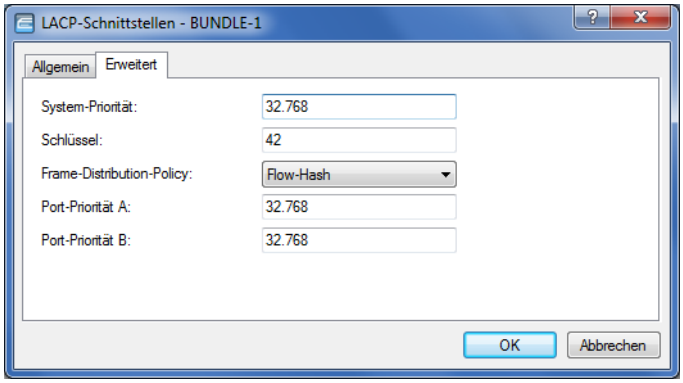
4. Wählen Sie die erste Schnittstelle aus dem Auswahlmenü **Schnittstelle A** aus.
5. Wählen Sie die zweite Schnittstelle aus dem Auswahlmenü **Schnittstelle B** aus.
6. Aktivieren Sie das Bündel durch Setzen des Häkchens in der Checkbox **Eintrag aktiv**.

> Die weiteren Schritte sind optional.

Die Standard-Einstellungen wurden angepasst an die meisten Anwendungen.

Bitte führen Sie eine individuelle Konfiguration nur als erfahrener Netzwerk-Techniker durch.

7. Navigieren Sie in die erweiterten Konfigurationsmöglichkeiten per Klick auf **Erweitert**.



8. Tragen Sie in das Eingabefeld **System-Priorität** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.
9. Machen Sie eine Eintragung in der Eingabezeile **Schlüssel**.

Der Schlüssel ist eine Zahl von 1 bis 54 und dient als Kennzeichnung des Bündels.

10. Wählen Sie eine Frame-Verteilungs-Regel in dem Auswahlmenü **Frame-Distribution-Policy**. Die für die meisten Szenarien empfohlene Default-Einstellung ist Flow-Hash.
11. Tragen Sie in das Eingabefeld **Port-Priorität A** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.
12. Tragen Sie in das Eingabefeld **Port-Priorität B** ein Vielfaches von 4.096 ein. Der Standardwert lautet 32.768.

11.1.1 Ergänzungen im Setup-Menü

LACP

In diesem Menü konfigurieren Sie das Link Aggregation Control Protocol (LACP).

SNMP-ID:

2.4.13.12

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung**

Schnittstellen

Hier wählen Sie ein Schnittstellen-Bündel aus.

SNMP-ID:

2.4.13.12.1

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP**

Mögliche Werte:

BUNDLE-1
Schnittstellen-Bündel 1
BUNDLE-2
Schnittstellen-Bündel 2

Schnittstelle

Über dieses Menü gelangen Sie zu den erweiterten Features.

SNMP-ID:
2.4.13.12.1.1

Pfad Telnet:
Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:

Allgemein
Enthält bereits bekannte Features der Schnittstellen-Bündelung.
Erweitert
Enthält die neuen Features der Schnittstellen-Bündelung.

Default-Wert:

Allgemein

System-Priorität

Hier legen Sie die System-Priorität fest.

SNMP-ID:
2.4.13.12.1.2

Pfad Telnet:
Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:
Vielfache von 4096 `[0-9]`

Default-Wert:
32768

Schlüssel

Hier vergeben Sie an das Bündel eine Zahl zur Kennzeichnung.

SNMP-ID:

2.4.13.12.1.3

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:

1 … 54

Default-Wert:

42

Frame-Verteilungs-Regel

Auf der sendenden Seite werden die ausgehenden Pakete anhand der konfigurierten Frame-Distribution-Policy auf die einzelnen Schnittstellen innerhalb der Link Aggregation Group verteilt.

SNMP-ID:

2.4.13.12.1.4

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:

VLAN

Ausgehende Pakete werden anhand ihres VLAN-Tags auf die einzelnen Links der LAG verteilt.

Flow-Hash

Für ausgehende Pakete wird ein Flow-Hash über die enthaltenen IP-Adressen und TCP/UDP-Ports gebildet. Anhand dieses Flow-Hashs werden die Pakete auf die einzelnen Links der LAG verteilt.

Quell-MAC-Adresse

Ausgehende Pakete werden anhand der enthaltenen Quell-MAC-Adresse auf die einzelnen Links der LAG verteilt.

Ziel-MAC-Adresse

Ausgehende Pakete werden anhand der enthaltenen Ziel-MAC-Adresse auf die einzelnen Links der LAG verteilt.

Quell/Ziel-MAC-Adresse

Ausgehende Pakete werden anhand des enthaltenen Paares aus Quell-MAC-Adresse und Ziel-MAC-Adresse auf die einzelnen Links der LAG verteilt.

Default-Wert:

Flow-Hash

Port-Priorität-A

Hier legen Sie die Statuswerte für Port-Priorität-A fest.

SNMP-ID:

2.4.13.12.1.5

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:

Vielfache von 4096 `[0-9]`

Default-Wert:

32768

Port-Priorität-B

Hier legen Sie die Statuswerte für Port-Priorität-A fest.

SNMP-ID:

2.4.13.12.1.6

Pfad Telnet:

Setup > **LAN** > **Schnittstellen-Bündelung** > **LACP** > **Schnittstellen**

Mögliche Werte:

Vielfache von 4096 `[0-9]`

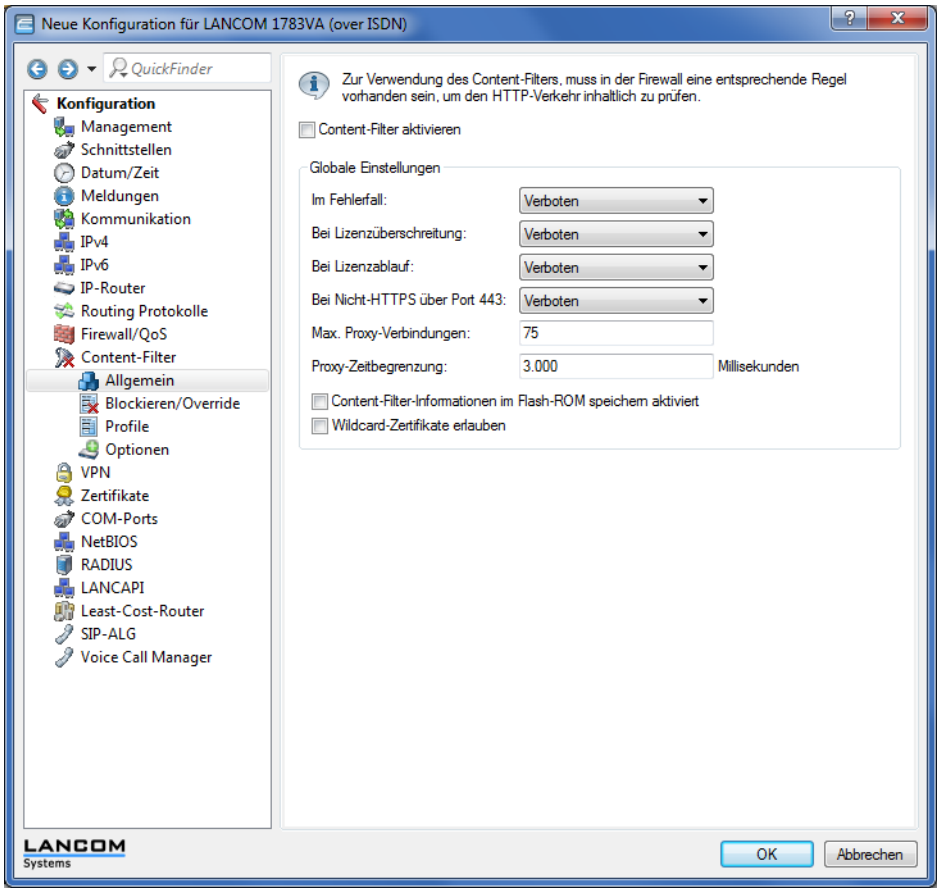
Default-Wert:

32768

12 LANCOM Content Filter

12.1 Unbekannter Traffic über Port 443

Ab LCOS-Version 10.12 können Sie Nicht-HTTPS-Verbindungen über Port 443 zulassen. Hierfür wurde ein neues Auswahlfenster in **LANconfig** implementiert:



Nicht-HTTPS-Traffic über Port 443

Verboten

Lässt Nicht-HTTPS-Traffic über Port 443 nicht zu.

Erlaubt

Lässt Nicht-HTTPS-Traffic über Port 443 zu.

Der TCP-Port 443 ist standardmäßig ausschließlich für HTTPS-Verbindungen reserviert.

Einige Applikationen, die nicht HTTPS nutzen, verwenden dennoch TCP-Port 443. Für diesen Fall haben Sie hier die Möglichkeit, den TCP-Port 443 auch für Nicht-HTTPS-Verbindungen zu öffnen.

Falls Sie Nicht-HTTPS-Verbindungen über Port 443 zulassen, wird der Traffic nicht weiter klassifiziert, sondern ganz pauschal zugelassen. Per Default werden Nicht-HTTPS-Verbindungen über Port 443 nicht zugelassen.

12.1.1 Ergänzungen im Setup-Menü

Unbekannter-443-Traffic

Hier können Sie Nicht-HTTPS-Kommunikation über TCP-Port 443 erlauben.

SNMP-ID:

2.41.2.2.30

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen**

Mögliche Werte:

0

Abweisen

1

Erlauben

Default-Wert:

0

12.2 IPv6-Unterstützung

Ab LCOS-Version 10.12 unterstützt der Content Filter neben IPv4 auch IPv6.

IPv6-Datenverkehr wird genau so geprüft und gefiltert wie IPv4-Datenverkehr. Die Konfiguration erfolgt, analog zu IPv4, in der Firewall. In der IPv6-Firewall lassen sich nun Aktionen definieren, die den Datenverkehr zur Prüfung an den Content Filter weiterleiten:

```
root@Router_PP:/Setup/IPv6/Firewall/Actions/CONTENT-FILTER-BASIC
> ls -a
[1.3.6.1.4.1.2356.11][2.70.5.7.1][column][20.67.79.78.84.69.78.84.45.70.73.76.84.69.82.45.66.65.83.73.67]

[  1] Name             INFO:    CONTENT-FILTER-BASIC
[  2] Limit            VALUE:   0
[  3] Unit             VALUE:   packets
[  4] Time             VALUE:   absolute
[  5] Context          VALUE:   session
[  6] Flags            VALUE:   none
[  7] Action           VALUE:   check
[ 10] Content-Filter   VALUE:   CF-BASIC-PROFILE
[ 11] DiffServ         VALUE:   No
[ 12] DSCP-value       VALUE:   0
[ 13] Conditions       VALUE:
```

```
[ 14] Trigger-actions  VALUE:
```

Wichtig ist die Aktion **check** in Zusammenhang mit dem unter **Content-Filter** angegebenen Content-Filter-Profil. Das Profil wird wie gewohnt in der Content-Filter-Konfiguration erstellt.

Per Default sind folgende Aktions-Objekte bereits in der IPv6-Firewall angelegt:

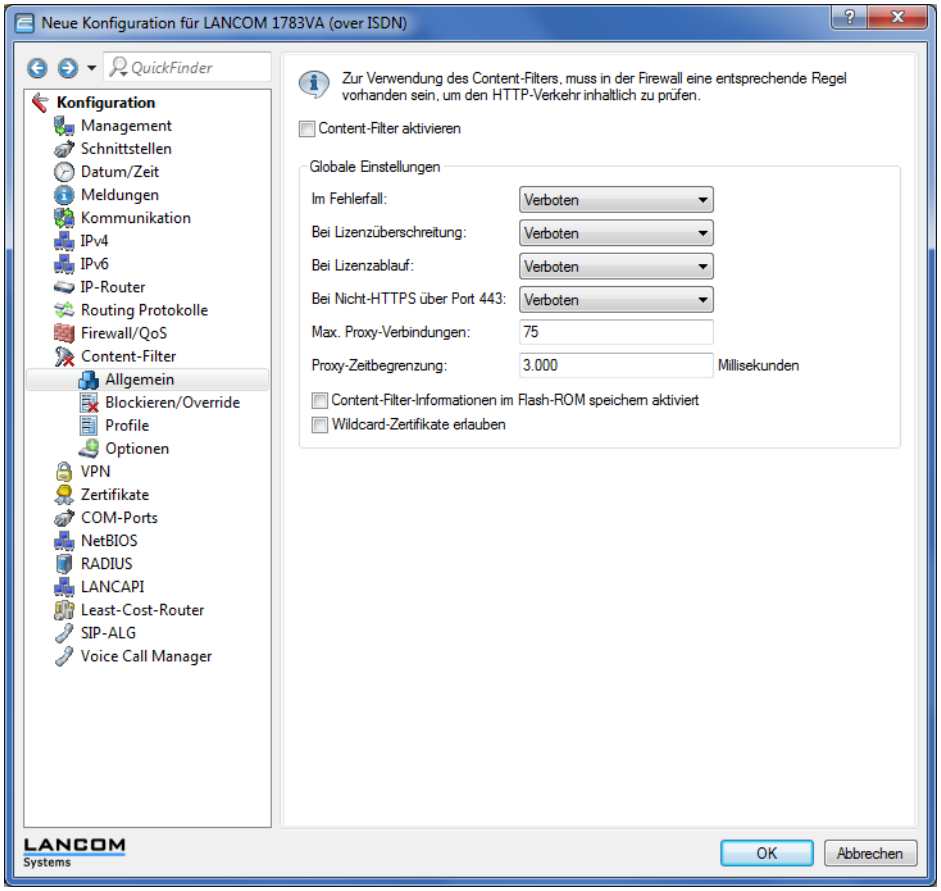
```
root@Router_PP:/Setup/IPv6/Firewall/Actions
> ls -a

[1.3.6.1.4.1.2356.11][2.70.5.7]
Name                            Limit   Unit       Time     Context   Flags   Action
Content-Filter
[1]                            [2]    [3]        [4]       [5]       [6]    [7]
[10]
CONTENT-FILTER-BASIC              0     packets    absolute    session    none    check
CF-BASIC-PROFILE
CONTENT-FILTER-PARENTIAL-CONTROL 0     packets    absolute    session    none    check
CF-PARENTIAL-CONTROL-PROFILE
CONTENT-FILTER-WORK               0     packets    absolute    session    none    check
CF-WORK-PROFILE
```

In der Regeltabelle (Forwarding-Rules) ist nachfolgende Regel per Default hinterlegt. Sie ist deaktiviert und kann vom Benutzer aktiviert werden:

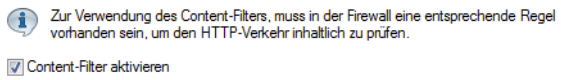
```
root@Router_PP:/Setup/IPv6/Firewall/Forwarding-Rules
> ls -a

[1.3.6.1.4.1.2356.11][2.70.5.2]
Name             Action           Services Source-Stations Destination-Stations Flags
   Comment
[1]                 [5]              [7]       [8]               [9]              [2]
     [10]
CONTENT-FILTER CONTENT-FILTER-BASIC  ANY     ANYHOST           ANYHOST        deactivated
  pass web traffic to...
...
  Content-Filter
```

12.2.1 Konfiguration in LANconfig

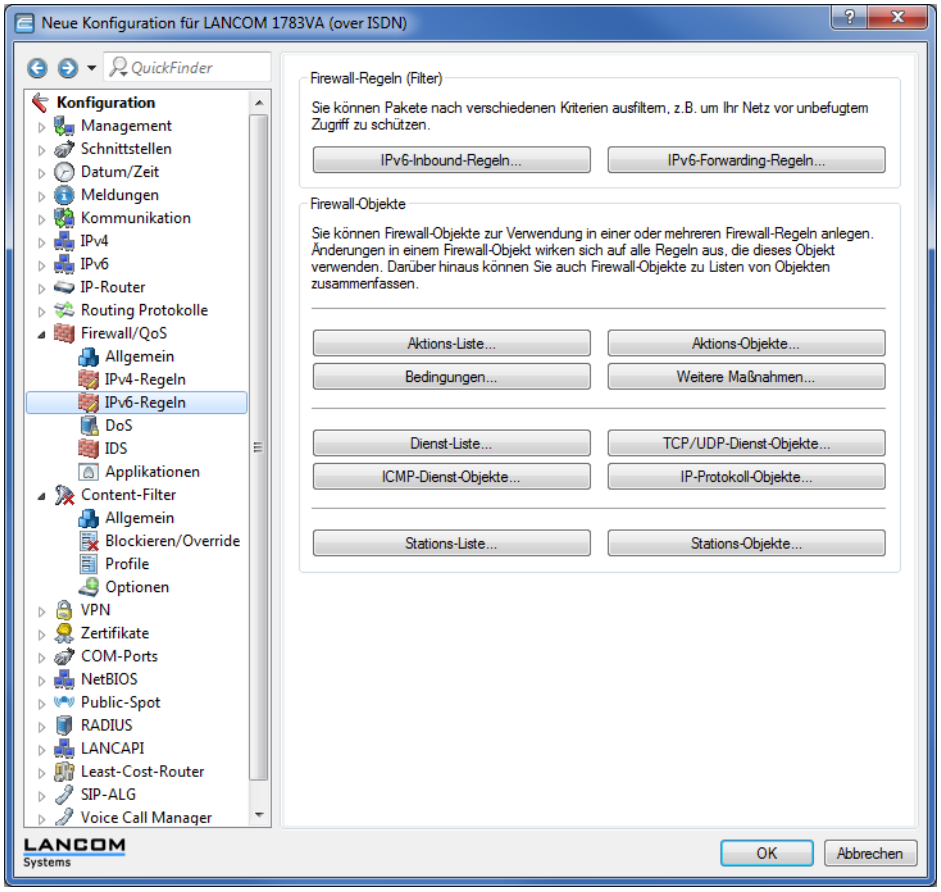
Navigieren Sie zu **Content-Filter** > **Allgemein**



und aktivieren Sie den Content-Filter über das Auswahlkästchen **Content-Filter aktivieren**.

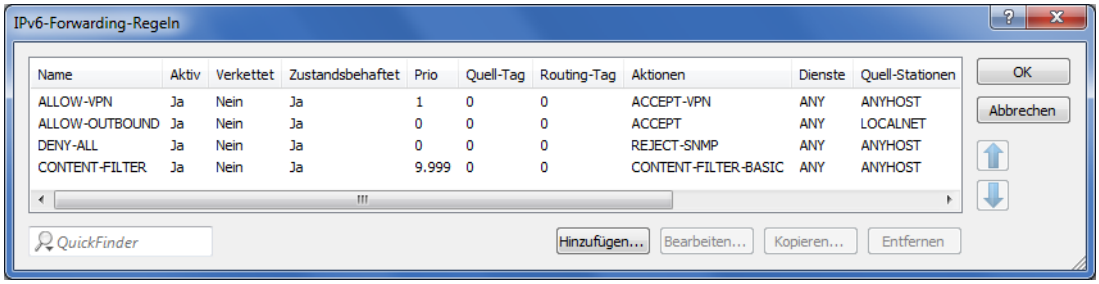


Navigieren Sie nun zu **Firewall/QoS** > **IPv6-Regeln**.

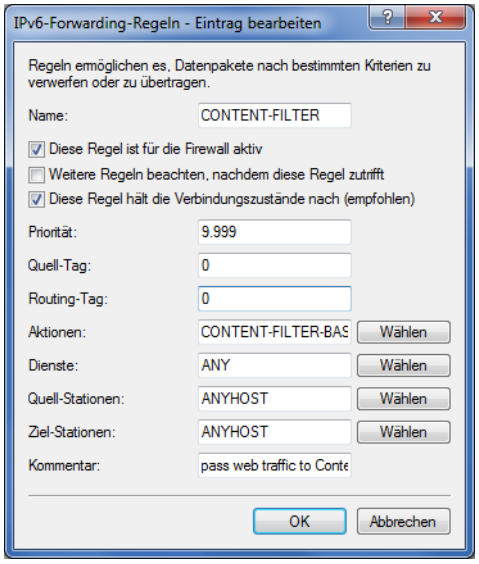


IPv6-Forwarding-Regeln

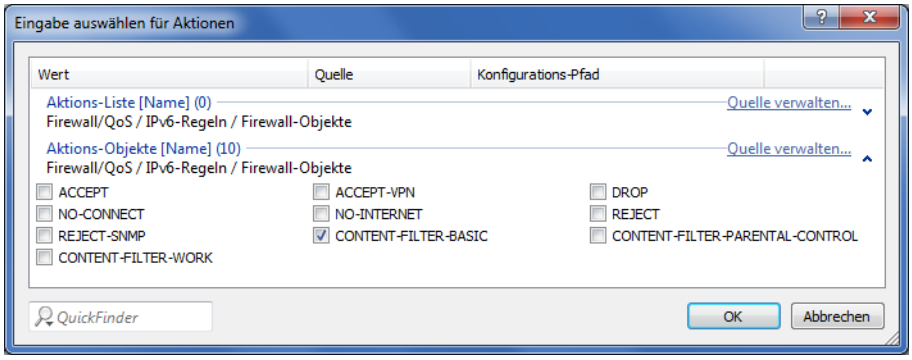
Weiterleitungsregeln definieren Sie unter **Firewall/QoS** > **IPv6-Regeln** > **Firewall-Regeln (Filter)** im Menü **IPv6-Forwarding-Regeln**:



Per Default ist bereits das Profil **CONTENT-FILTER** mit folgenden Einstellungen angelegt:



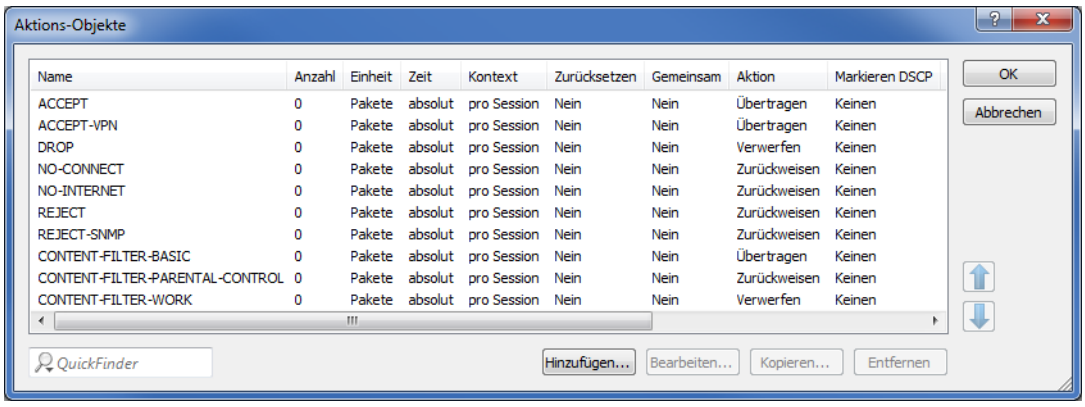
In der Auswahlliste **Aktionen** werden Ihnen per Default die Content-Filter-Profile **CONTENT-FILTER-BASIC**, **CONTENT-FILTER-PARENTAL-CONTROL** und **CONTENT-FILTER-WORK** angeboten:



IPv6-Aktions-Objekte

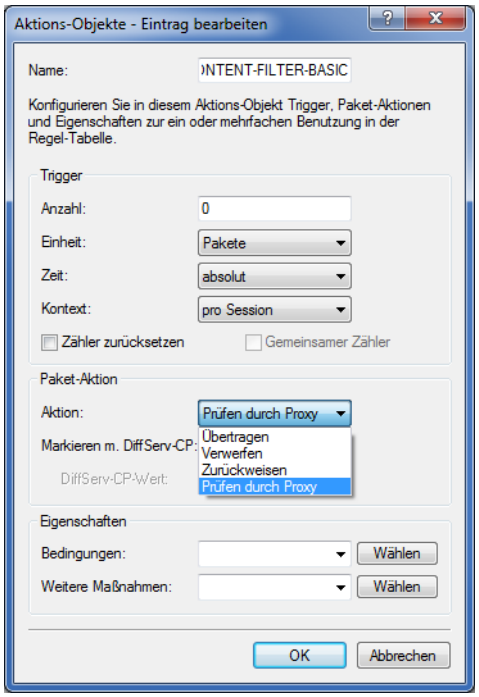
Die benötigten Firewall-Objekte definieren Sie unter **Firewall/QoS** > **IPv6-Regeln** > **Firewall-Objekte**

im Menü **Aktions-Objekte**:



Per Default sind bereits die Content-Filter-Profile **CONTENT-FILTER-BASIC**, **CONTENT-FILTER-PARENTAL-CONTROL** und **CONTENT-FILTER-WORK** als Aktions-Objekte angelegt.

Wenn Sie einen dieser drei Einträge bearbeiten, stehen Ihnen in dem Feld **Paket-Aktion** die Optionen des Content-Filter-Profils zur Auswahl:



Mögliche Optionen:

Prüfen durch Proxy (Default)

Der Proxy entscheidet, ob das Paket übertragen wird oder nicht.

Übertragen

Das Paket wird normal übertragen.

Verwerfen

Das Paket wird stillschweigend verworfen.

Zurückweisen

Das Paket wird zurückgewiesen, der Empfänger erhält eine entsprechende Nachricht über ICMPv6.

12.2.2 Ergänzungen im Setup-Menü

Content-Filter

Definiert das Content-Filter-Profil.

SNMP-ID:

2.70.5.7.10

Pfad Telnet:

Setup > **IPv6** > **Firewall** > **Aktionen**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

CF-BASIC-PROFILE

Default-Wert:

CF-PARENTAL-CONTROL-PROFILE

Default-Wert:

CF-WORK-PROFILE

13 Weitere Dienste

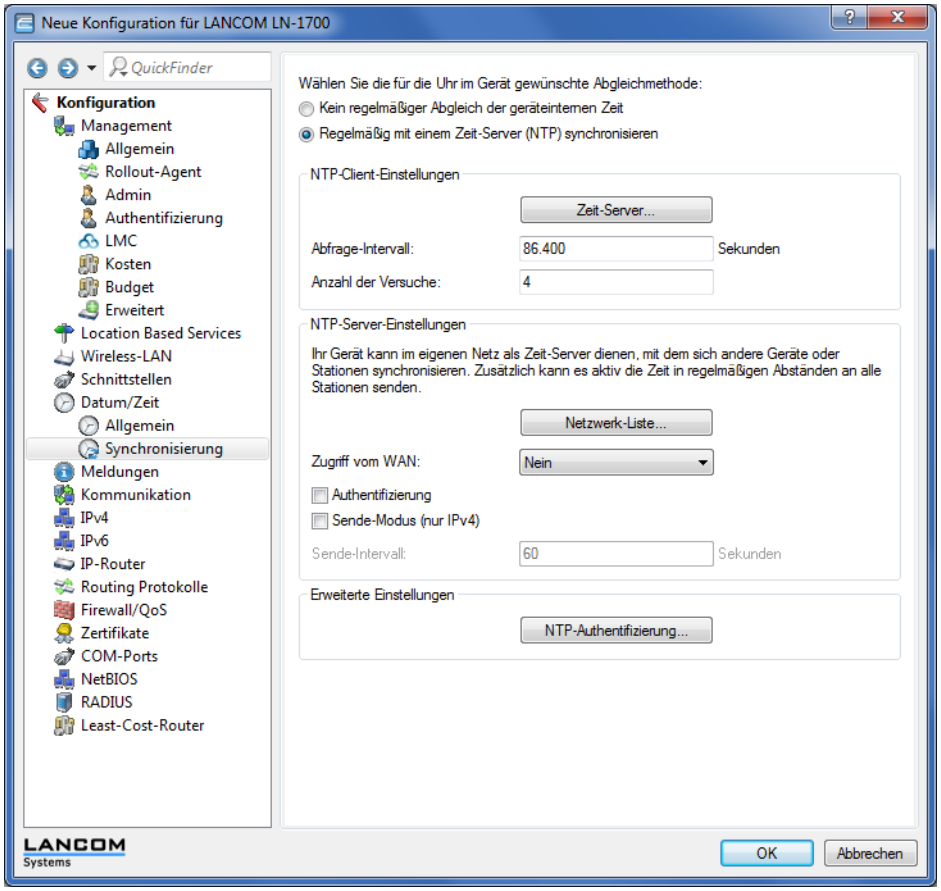
13.1 Zeit-Server für das lokale Netz

Ab LCOS-Version 10.12 stehen Ihnen weitere Features zur Verfügung:

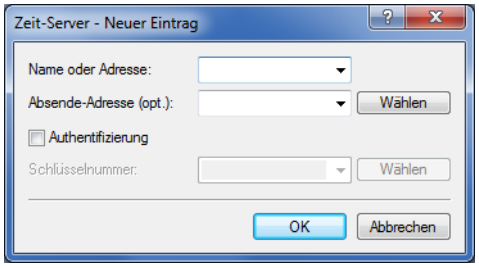
- Der NTP-Server ist pro ARF-Netz aktivierbar.
- NTP-Server und NTP-Client unterstützen MD5-Authentifierung.
- Der Zugriff vom WAN auf den NTP-Server ist schaltbar.

13.1.1 Konfiguration in LANconfig

Sie konfigurieren die neuen Features unter **Datum/Zeit** > **Synchronisierung**.



Im Abschnitt **NTP-Client-Einstellungen** enthält das Menü **Zeit-Server** zwei zusätzliche Parameter.



Authentifizierung

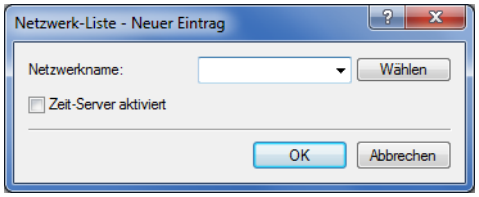
Aktiviert bzw. deaktiviert die MD5-Authentifizierung durch den Client.

Schlüsselnummer

Kennzeichnet den Schlüssel, den der Client zur MD5-Authentifizierung verwendet.

Neu im Abschnitt **NTP-Server-Einstellungen**:

Die Liste der Netzwerke, an welche Ihr Gerät die aktuelle Zeit weiterleitet, konfigurieren Sie unter **Netzwerkliste**.



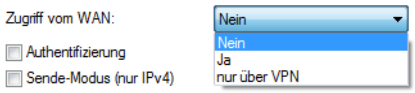
Netzwerkname

Definiert den Namen des Netzwerks.

Zeitserver aktiviert

Legt fest, ob die Zeitserver-Funktion Ihres Gerätes für das ausgewählte Netzwerk aktiviert ist.

Den Zugriff vom WAN konfigurieren Sie über die Auswahlliste **Zugriff vom WAN**.



Mögliche Optionen sind:

Nein

Der Zugriff vom WAN auf den NTP-Server ist deaktiviert.

Ja

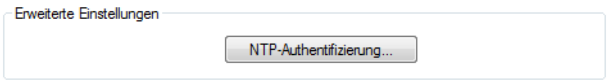
Der Zugriff vom WAN auf den NTP-Server ist möglich über unmaskierte Verbindungen, jedoch grundsätzlich nicht möglich bei maskierten WAN-Verbindungen.

Nur über VPN

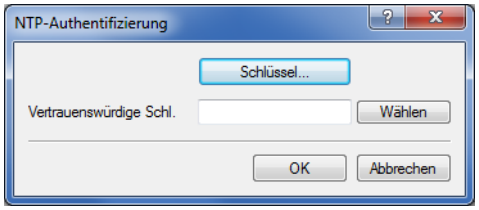
Der Zugriff über VPN auf den NTP-Server ist aktiviert.

Die Unterstützung für die MD5-Authentifizierung aktivieren Sie unter **Authentifizierung**.

Neuer Abschnitt **Erweiterte Einstellungen**:

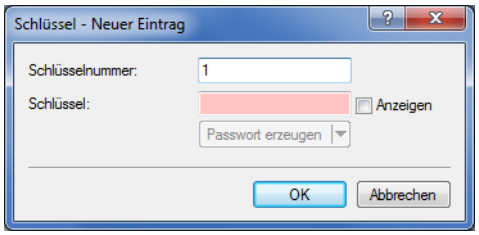


Die Liste der vertrauenswürdigen Schlüssel konfigurieren Sie unter **NTP-Authentifizierung**.



Die zur Verfügung stehenden Schlüssel befinden sich in der Liste **Vertrauenswürdige Schl.** und werden über **Wählen** ausgewählt.

Das Bearbeiten bzw. Hinzufügen eines Schlüssels erfolgt über **Schlüssel**.



13.1.2 Ergänzungen im Setup-Menü

Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Client.

SNMP-ID:

2.26.11.3

Pfad Telnet:

Setup > **NTP** > **RQ-Adresse**

Mögliche Werte:

Nein

Deaktiviert

Ja

Aktiviert

Default-Wert:

Nein

Schlüsselnummer

Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Client.

SNMP-ID:

2.26.11.4

Pfad Telnet:

Setup > **NTP** > **RQ-Adresse**

Mögliche Werte:

1 … 65535

Authentifizierung

Aktiviert bzw. deaktiviert die MD5-Authentifizierung für den Server.

SNMP-ID:

2.26.13

Pfad Telnet:

Setup > **NTP**

Mögliche Werte:

Nein

Deaktiviert

Ja

Aktiviert

Default-Wert:

Nein

Schlüssel

Konfiguriert die Tabelle **Schlüssel**.

SNMP-ID:

2.26.14

Pfad Telnet:

Setup > **NTP**

Schlüsselnummer

Kennzeichnet den zur MD5-Authentifizierung verwendeten Schlüssel für den Server.

SNMP-ID:

2.26.14.1

Pfad Telnet:

Setup > **NTP** > **Schlüssel**

Mögliche Werte:

1 … 65535

Schlüssel

Dieser Eintrag enthält den Wert des Schlüssels.

SNMP-ID:

2.26.14.2

Pfad Telnet:

Setup > **NTP** > **Schlüssel**

Mögliche Werte:

64 Zeichen aus `[A-Z@{|}~!$%&'()+-,/:;<=>?[\]^_.0-9]`

Vertrauenswürdige-Schlüssel

Enthält die Liste der vertrauenswürdigen Schlüssel (kommaseparierte Liste aus Schlüsselnummern).

SNMP-ID:

2.26.15

Pfad Telnet:

Setup > **NTP**

Mögliche Werte:

Maximal 63 Zeichen aus `[0-9,]`

Netzwerkliste

Diese Liste enthält die Netzwerke, die Ihr Gerät als Zeit-Server verwenden.

SNMP-ID:

2.26.16

Pfad Telnet:

Setup > **NTP**

Netzwerkname

Definiert den Namen des Netzwerks, auf dem der NTP-Server aktiviert werden soll.

SNMP-ID:

2.26.16.1

Pfad Telnet:

Setup > **NTP** > **Netzwerkliste**

Mögliche Werte:

Einträge aus der Setup/TCP-IP/-Netzwerkliste; Zeichen aus
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Aktiv

Definiert, ob der NTP-Server auf dem ausgewählten Netzwerk aktiviert ist.

SNMP-ID:

2.26.16.2

Pfad Telnet:

Setup > **NTP** > **Netzwerkliste**

Mögliche Werte:

Nein
Deaktiviert

Ja
Aktiviert

Default-Wert:

Nein

Server-WAN-Zugriff

Konfiguriert den WAN-Zugriff auf Ihr Gerät.

SNMP-ID:

2.26.17

Pfad Telnet:

Setup > **NTP**

Mögliche Werte:

Nein

Deaktiviert den Zugriff vom WAN auf den NTP-Server.

Ja

Der Zugriff vom WAN auf den NTP-Server ist möglich über unmaskierte Verbindungen, jedoch grundsätzlich nicht möglich bei maskierten Verbindungen.

VPN

Der Zugriff über VPN auf den NTP-Server ist aktiviert.

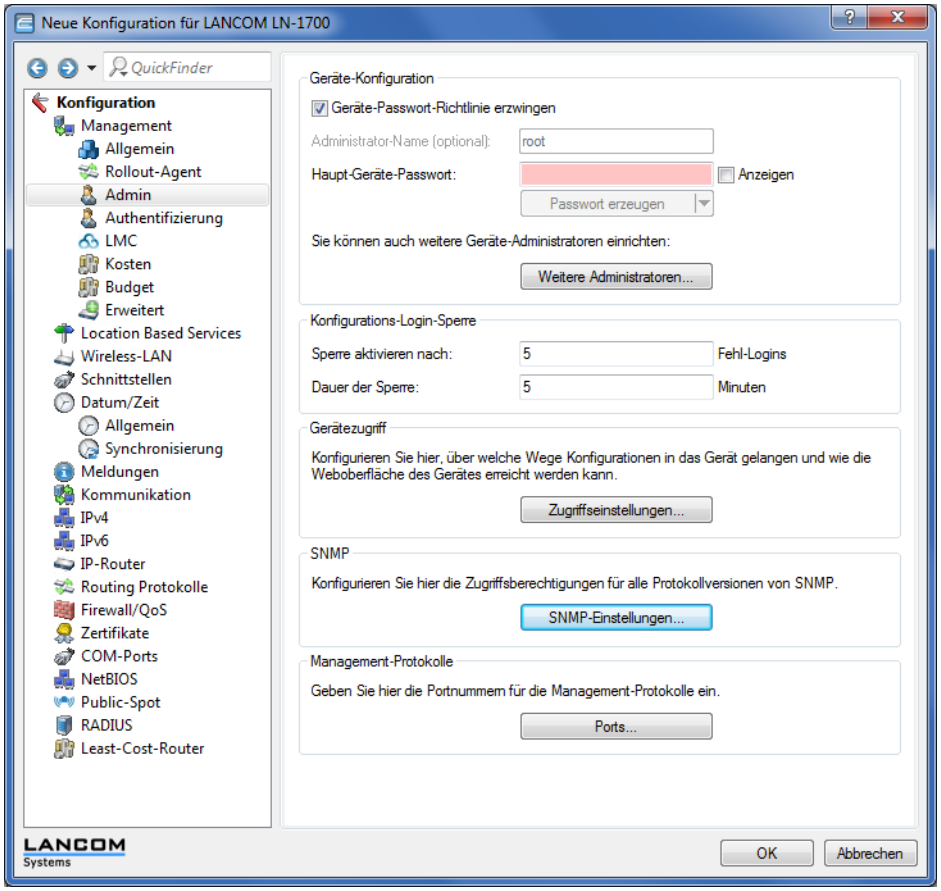
13.2 Simple Network Management Protocol (SNMP)

Ab LCOS-Version 10.12 stehen SNMPv3-Benutzern weitere Authentifizierungs-Algorithmen zur Verfügung.

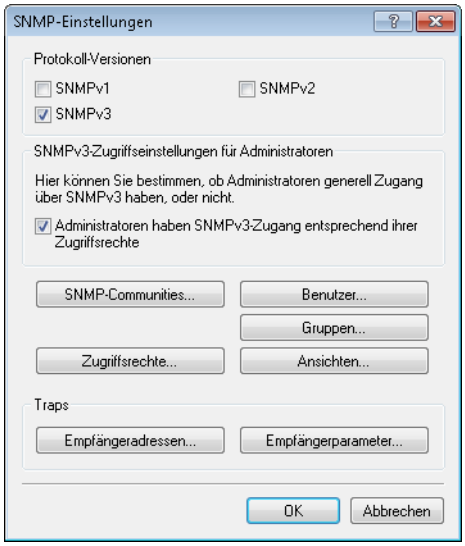
Dies bedeutet ein weiteres Plus an Sicherheit.

13.2.1 SNMP mit LANconfig konfigurieren

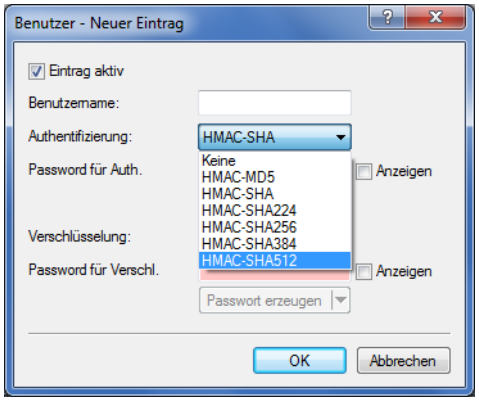
Sie konfigurieren die neuen Features unter **Management** > **Admin** > **SNMP**



im Menü **SNMP-Einstellungen**.



Im Menü **Benutzer** finden Sie die Auswahlliste **Authentifizierung**.



Die neuen Authentifizierungs-Algorithmen:

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

13.2.2 Ergänzungen im Setup-Menü

Authentifizierungs-Protokoll

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss.

Ab LCOS-Version 10.12 stehen Ihnen Hash-Algorithmen mit einer Hash-Länge von 224 Bits und mehr zur Verfügung.

SNMP-ID:

2.9.32.5

Pfad Telnet:

Setup > **SNMP** > **Benutzer**

Mögliche Werte:

None

Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-96 (Hash-Länge 160 Bits).

HMAC-SHA224

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512

Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512(Hash-Länge 512 Bits).

Default-Wert:

HMAC-SHA

14 Appendix

14.1 Die CRON-Syntax

Ein CRON-Job besteht aus sechs Feldern:

```
minute    hour    day of month    month    day of week    command
```

Der Asterix '*' dient als Platzhalter für alle erlaubten Zeichen.

Einige Beispiele für das regelmäßige Ausführen eines Restart-Befehls mit CRON:

Jeden Tag um 13:30:

```
30          13          *           *           *          restart
```

Jeden Tag 30 Minuten nach jeder vollen Stunde:

```
30          *           *           *           *          restart
```

Alle 30 Minuten jeden Tag:

```
*/30        *           *           *           *          restart
```

Jeden Samstag um 20:15 Uhr:

```
15          20          *           *           6          restart
```

Der Sonntag wird wahlweise über die '0' oder die '7' ausgewählt.

Um 00:00 Uhr zum Monatsersten

```
0           0           1           *           *          restart
```