

# LCOS 10.80

## Addendum

05/2024



**LANCOM**  
SYSTEMS

# Inhalt

<b>1 Addendum zur LCOS-Version 10.80.....</b>	<b>5</b>
<b>2 Diagnose.....</b>	<b>6</b>
2.1 Tracen auf ein angeschlossenes USB-Laufwerk.....	6
2.2 Capture-Daten auf ein USB-Laufwerk ausgeben.....	7
2.2.1 Ergänzungen im Setup-Menü.....	7
<b>3 Sicherheit.....</b>	<b>10</b>
3.1 Länge des Hauptgerätepassworts.....	10
3.1.1 Ergänzungen im Setup-Menü.....	10
<b>4 Routing und WAN-Verbindungen.....</b>	<b>12</b>
4.1 DPS-Switchover kann nun Leitungsprioritäten berücksichtigen.....	12
4.1.1 Ergänzungen im Setup-Menü.....	13
4.2 Priority Bit bei WAN-Verbindung.....	14
4.2.1 Ergänzungen im Setup-Menü.....	14
4.3 Automatischer APN.....	15
4.3.1 Ergänzungen im Setup-Menü.....	16
4.4 Automatischer WWAN-Verbindungsaufbau bei unkonfigurierten Geräten.....	17
4.5 Parameter LTE-Anmeldung entfernt.....	17
4.6 Mobilfunk Cold Standby.....	18
4.6.1 Ergänzungen im Setup-Menü.....	18
<b>5 IPv6.....</b>	<b>20</b>
5.1 Mehrere DHCPv6-Relay-Ziele.....	20
5.1.1 Ergänzungen im Setup-Menü.....	21
5.2 Weitere Optionen für den DHCPv6-Client.....	25
5.2.1 Ergänzungen im Setup-Menü.....	26
5.3 DS-Lite-Tunnel mit Ziel-Interface.....	28
5.3.1 Ergänzungen im Setup-Menü.....	29
<b>6 Firewall.....</b>	<b>30</b>
6.1 Manuelle Ausführung von Aktionen der Aktionstabelle.....	30
6.1.1 Ergänzungen im Setup-Menü.....	30
<b>7 Virtual Private Networks – VPN.....</b>	<b>32</b>
7.1 LANCOM Trusted Access.....	32
7.1.1 Ergänzungen im Setup-Menü.....	33
<b>8 WLAN-Management.....</b>	<b>38</b>
8.1 Kanal-Profil im WLC.....	38
8.1.1 Ergänzungen im Setup-Menü.....	39
8.2 LACP-Konfiguration via WLC.....	41
8.2.1 Ergänzungen im Setup-Menü.....	42
<b>9 Backup-Lösungen.....</b>	<b>44</b>
9.1 Unterstützung von vRouter-Redundanz in Amazon AWS.....	44

<b>10 Weitere Dienste.....</b>	<b>45</b>
10.1 DHCPv4-Client Optionen.....	45
10.1.1 Ergänzungen im Setup-Menü.....	45
10.2 Accounting.....	48
10.2.1 Arbeitsweise.....	49
10.2.2 Ein- bzw. Ausschalten des Accountings im laufenden Betrieb.....	49
10.2.3 Zählung des Datenverkehrs.....	49
10.2.4 Weitere Änderungen beim Accounting.....	50
10.2.5 Ergänzungen im Setup-Menü.....	51
10.3 Neuer Netflow-Parameter „Active-Flow-Timeout“.....	52
10.3.1 Ergänzungen im Setup-Menü.....	52
10.4 PON-Passwort in hexadezimalen Format.....	53
10.4.1 Ergänzungen im Setup-Menü.....	53
10.5 ACME-Client.....	54
10.5.1 ACME-Client konfigurieren.....	55
10.5.2 Ergänzungen im Setup-Menü.....	56
10.6 Aktionen auf eingehende SMS ausführen.....	67
10.6.1 Ergänzungen im Setup-Menü.....	68
<b>11 Ergänzungen im Menüsystem.....</b>	<b>72</b>
11.1 Ergänzungen im Setup-Menü.....	72
11.1.1 Msg-Authenticator-erforderlich.....	72
11.1.2 L2TP-Msg-Authenticator-erforderlich.....	72
11.1.3 LB-Policy.....	73
11.1.4 Vordefinierte-Selektoren.....	73
11.1.5 Msg-Authenticator-erforderlich.....	74
11.1.6 Konfigurationshochladeprüfung.....	74
11.1.7 Msg-Authenticator-erforderlich.....	75
11.1.8 Backup-Msg-Authenticator-erforderlich.....	75
11.1.9 Msg-Authenticator-erforderlich.....	76
11.1.10 Roaming-PDP-Typ.....	76
11.1.11 Datenroaming.....	77
11.1.12 Syslog.....	77
11.1.13 Msg-Authenticator-erforderlich.....	78
11.1.14 Msg-Authenticator-erforderlich.....	78
11.1.15 Msg-Authenticator-erforderlich.....	79
11.1.16 Blockierte-Gegenstellen.....	79
11.1.17 LCOSCap-WAN-Zugriff.....	80
11.1.18 RPCap-WAN-Zugriff.....	80
11.1.19 LB-Policy.....	81
11.1.20 Aktiv.....	81

# Copyright

© 2024 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS) finden Sie auf der WEBconfig des Geräts unter dem Menüpunkt „Extras > Lizenzinformationen“. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage über einen Download-Server bereitgestellt.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde ([www.openssl.org](http://www.openssl.org)).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen

Deutschland

[www.lancom-systems.de](http://www.lancom-systems.de)

# 1 Addendum zur LCOS-Version 10.80

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 10.80 gegenüber der vorherigen Version.

## 2 Diagnose

### 2.1 Tracen auf ein angeschlossenes USB-Laufwerk

Ab LCOS 10.80 ist es möglich, Traces auf ein angeschlossenes USB-Laufwerk, z. B. einen USB-Stick, im Hintergrund zu speichern. Eine aktive Konsolensitzung ist dazu nicht erforderlich, da die Aufzeichnung im Hintergrund durchgeführt wird.

Auf die Datei kann nach Abschluss der Aufzeichnung zugegriffen werden, in dem der USB-Stick an einen Computer angeschlossen wird. Alternativ kann remote per SCP auf das Gerät auf das Verzeichnis /usb/ zugegriffen werden.

Das USB-Laufwerk muss dazu FAT32-formatiert sein. Das Gerät schreibt so lange auf den USB-Stick, bis dieser voll ist, danach stoppt die Aufzeichnung.

 Es ist nicht möglich, eine Datei auf den internen Flash des Geräts zu schreiben oder von dort zu laden.

Ein ICMP-Trace auf der Konsole wird z. B. wie folgt auf ein USB-Laufwerk umgeleitet:

```
Trace # ICMP > /usb/file.lct
```

Der ICMP-Trace wird wie folgt gestoppt:

```
Trace # ICMP > /usb/file.lct bzw. Trace - all > /usb/file.lct
```

Das Show-Kommando „show trace-file“ zeigt aktive Trace-Sitzungen auf USB an.

Ein `Trace - all` beendet nicht die laufenden Sitzungen, die auf USB aufgezeichnet werden, sondern nur die aktiven Traces der aktiven Konsolensitzung.

```
root@lc1900ef-aa:/
> tr # icmp >/usb/my
created trace session for '/usb/my.lct'
/usb/my.lct:
ICMP                ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                ON

root@lc1900ef-aa:/
> tr # tcp >/usb/my
/usb/my.lct:
TCP                  ON

root@lc1900ef-aa:/
> show trace-file

/usb/my.lct:
  ICMP                ON
  TCP                  ON

root@lc1900ef-aa:/
> tr - all >/usb/my
/usb/my.lct:
remove trace session for '/usb/my.lct'
```

## 2.2 Capture-Daten auf ein USB-Laufwerk ausgeben

Ab LCOS 10.80 können Wireshark-Captures im Hintergrund vom Router auf ein angeschlossenes USB-Laufwerk, z. B. einen USB-Stick geschrieben werden. Eine aktive Management-Session vom Computer auf das Gerät ist dazu nicht erforderlich.

Auf die Datei kann nach Abschluss der Aufzeichnung zugegriffen werden, indem der USB-Stick an einen Computer angeschlossen wird. Alternativ kann remote per SCP auf das Gerät auf das Verzeichnis /usb/ zugegriffen werden.

Das USB-Laufwerk muss dazu FAT32-formatiert sein. Das Gerät schreibt so lange auf den USB-Stick, bis dieser voll ist, danach stoppt die Aufzeichnung.



Es ist nicht möglich, eine Datei auf den internen Flash des Geräts zu schreiben oder von dort zu laden.

Den Dateinamen und alle weiteren notwendigen Angaben machen Sie über die Kommandozeile in der Tabelle **Setup > Paket-Capture > Capturing-auf-Datei > Dateien**.

### 2.2.1 Ergänzungen im Setup-Menü

#### Capturing-auf-Datei

In diesem Menü finden Sie die Einstellungen zur Aufzeichnung des Netzwerk-Datenverkehrs auf ein angeschlossenes USB-Laufwerk im Format PCAP. Dieses Format wird z. B. von Wireshark verwendet.

##### SNMP-ID:

2.63.20

##### Pfad Konsole:

**Setup > Paket-Capture**

##### Dateien

In dieser Tabelle konfigurieren Sie die Wireshark-Traces auf ein angeschlossenes USB-Laufwerk.

##### SNMP-ID:

2.63.20.1

##### Pfad Konsole:

**Setup > Paket-Capture > Capturing-auf-Datei**

##### Name

Name des Eintrags.

##### SNMP-ID:

2.63.20.1.1

**Pfad Konsole:**

**Setup > Paket-Capture > Capturing-auf-Datei > Dateien**

**Mögliche Werte:**

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

**In-Betrieb**

Definiert ob der Konfigurationseintrag aktiv oder inaktiv ist.

**SNMP-ID:**

2.63.20.1.2

**Pfad Konsole:**

**Setup > Paket-Capture > Capturing-auf-Datei > Dateien**

**Mögliche Werte:**

nein  
ja

**Dateiname**

Vollständiger Pfad und Name der Wireshark-Capture-Datei, z. B. `/usb/capture.pcap`.

**SNMP-ID:**

2.63.20.1.3

**Pfad Konsole:**

**Setup > Paket-Capture > Capturing-auf-Datei > Dateien**

**Mögliche Werte:**

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

**Schnittstelle**

Name des logischen Interfaces auf dem der Wireshark-Capture ausgeführt werden soll, z. B. DSL-1, LAN-1 etc.

**SNMP-ID:**

2.63.20.1.4

**Pfad Konsole:**

**Setup > Paket-Capture > Capturing-auf-Datei > Dateien**



**Mögliche Werte:**

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

**MAC-Adresse**

MAC-Adresse auf der die Aufzeichnung eingeschränkt werden soll, formatiert ohne Trennzeichen wie „-“ oder „:“.

**SNMP-ID:**

2.63.20.1.5

**Pfad Konsole:**

**Setup > Paket-Capture > Capturing-auf-Datei > Dateien**

**Mögliche Werte:**

max. 17 Zeichen aus `[0-9a-e]`


## 3 Sicherheit

### 3.1 Länge des Hauptgerätepassworts

Ab LCOS 10.80 wurde die maximale Länge des Hauptgerätepassworts auf 128 Zeichen erhöht. Dies wurde auch für die weiteren Administratoren und SNMP-Benutzer angepasst.

Besondere Beachtung gilt dem WLC mit verwalteten Access Points im Falle der Passwortsynchronisierung. Sollte hier das längere Passwort auf dem WLC verwendet werden, so müssen alle verwalteten Access Points ebenfalls auf LCOS 10.80 betrieben werden. Eine lokale Anmeldung ist in diesem Fall auf Access Points mit einer Version kleiner LCOS 10.80 nicht mehr möglich.

Die oben genannten Hinweise gelten nur in dem Fall, falls die neue Möglichkeit von mehr als 16 Zeichen beim Passwort verwendet wird.

 Bitte beachten Sie, dass ein Firmware-Downgrade auf eine Version kleiner LCOS 10.80 mit Passwörtern mit mehr als 16 Zeichen nicht unterstützt wird.

#### 3.1.1 Ergänzungen im Setup-Menü

##### Authentifizierungs-Passwort

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

**SNMP-ID:**

2.9.32.6

**Pfad Konsole:**

Setup > SNMP > Benutzer

**Mögliche Werte:**

max. 128 Zeichen aus [A-Z] [a-z] [0-9] #@{|}~!\$%&'()\*+,-./:;<=>?[\]^\_`~

**Default-Wert:**

leer

##### Verschlüsselungs-Passwort

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

**SNMP-ID:**

2.9.32.9

**Pfad Konsole:**

Setup > SNMP > Benutzer

**Mögliche Werte:**

max. 128 Zeichen aus [A-Z] [a-z] [0-9] #@{|}~!\$%&'()\*+,-./:;<=>?[\]^\_`~`

**Default-Wert:**

*leer*

**Passwort**

Passwort für diesen Eintrag. Dieses wird abhängig von [2.11.89.1 Klartext-behalten](#) geschrieben.

**SNMP-ID:**

2.11.21.2

**Pfad Konsole:**

Setup > Config > Admins

**Mögliche Werte:**

max. 128 Zeichen aus [A-Z] [a-z] [0-9] #@{|}~!\$%&'()\*+,-./:;<=>?[\]^\_`~`

**Default-Wert:**

*leer*

## 4 Routing und WAN-Verbindungen

### 4.1 DPS-Switchover kann nun Leitungsprioritäten berücksichtigen

Ab LCOS 10.80 wird beim DPS-Switchover eine Option unterstützt, über die bei Dynamic Path Selection auch Leitungsprioritäten berücksichtigt werden können.

Zur Konfiguration wechseln Sie in LANconfig zu **IP-Router > Routing > SD-WAN Dynamic Path Selection > Switchover-Profil**.

#### LB-Prio beachten

Dieser Parameter steuert das Verhalten des DPS Session Switchover.

**i** Wenn die Tabelle auf den Default zurückgesetzt wird, erhält die Zeile „AGGRESSIVE-SWITCHOVER“ ein „Ja“, „SOFT-SWITCHOVER“ ein „Nein“.

Mögliche Werte:

#### Ja

Sessions wechseln auch zwischen Interfaces mit gleichem Score, sofern die in [Richtlinien-Zuweisungen](#) vorgegebene Priorisierung eines davon bevorzugt. Passend dazu werden die Ausgabetafeln **Status > Firewall > Dynamic-Path-Selection > IPv4-Preferred-Lines-Log** und **Status > Firewall > Dynamic-Path-Selection > IPv6-Preferred-Lines-Log** in so einem Fall nur noch das höchstpriorisierte Interface als „Preferred“ ausweisen. Das ist auch das Interface, zu dem alle Sessions wechseln, mit einer Geschwindigkeit und in entsprechend vielen Zwischenschritten entsprechend der weiteren Parameter im entsprechenden Switchover-Profil.

**i** Diese Einstellung ist z. B. bei folgendem Szenario sinnvoll: Es wird LTE bzw. 5G zusammen mit VDSL verwendet. In manchen Standorten ist LTE / 5G deutlich besser als VDSL. Es soll aber aus Kostengründen zuerst DSL statt LTE / 5G verwendet werden, da dieses nur als Booster genutzt werden soll. Dies funktioniert z. B. auch mit den Prioritäten des Loadbalancers. Mit dem Defaultverhalten wird aber beim Switchover nicht von der schlechten Leitung zur besseren zurück gewechselt.

**i** Dies ist der Default für neue Einträge.

#### Nein

Das Verhalten des DPS Session Switchover ist, dass dieser nur dann durchgeführt wird, wenn eine andere Leitung tatsächlich besser ist (besserer Score) als die aktuell von der Session verwendete Leitung. Die bei den Load Balancer Policy Assignments mit eintragbarer Priorisierung wird nicht berücksichtigt. Deshalb gibt es keine Switchovers zwischen Interfaces mit identischem Policy-Score.


---

 Dies ist der Default für bereits vor LCOS 10.80 vorhandene Einträge.

## 4.1.1 Ergänzungen im Setup-Menü

### LB-Prio-Beachten

Dieser Parameter steuert das Verhalten des DPS Session Switchover.

 Wenn die Tabelle auf den Default zurückgesetzt wird, erhält die Zeile „AGGRESSIVE-SWITCHOVER“ ein „Ja“, „SOFT-SWITCHOVER“ ein „Nein“.

### SNMP-ID:

2.110.4.32.4


### Pfad Konsole:

**Setup > Firewall > Dynamische-Pfadauswahl > Switchover-Profil**

### Mögliche Werte:

#### Ja

Sessions wechseln auch zwischen Interfaces mit gleichem Score, sofern die in der Tabelle [2.110.4.17 Richtlinien-Zuweisungen](#) vorgegebene Priorisierung eines davon bevorzugt. Passend dazu werden die Ausgabetafeln **Status > Firewall > Dynamic-Path-Selection > IPv4-Preferred-Lines-Log** und **Status > Firewall > Dynamic-Path-Selection > IPv6-Preferred-Lines-Log** in so einem Fall nur noch das höchstpriorisierte Interface als „Preferred“ ausweisen. Das ist auch das Interface, zu dem alle Sessions wechseln, mit einer Geschwindigkeit und in entsprechend vielen Zwischenschritten entsprechend der weiteren Parameter im entsprechenden Switchover-Profil.

 Diese Einstellung ist z. B. bei folgendem Szenario sinnvoll: Es wird LTE bzw. 5G zusammen mit VDSL verwendet. In manchen Standorten ist LTE / 5G deutlich besser als VDSL. Es soll aber aus Kostengründen zuerst DSL statt LTE / 5G verwendet werden, da dieses nur als Booster genutzt werden soll. Dies funktioniert z. B. auch mit den Prioritäten des Loadbalancers. Mit dem Defaultverhalten wird aber beim Switchover nicht von der schlechten Leitung zur besseren zurück gewechselt.

 Dies ist der Default für neue Einträge.

#### Nein

Das Verhalten des DPS Session Switchover ist, dass dieser nur dann durchgeführt wird, wenn eine andere Leitung tatsächlich besser ist (besserer Score) als die aktuell von der Session verwendete Leitung. Die bei den Load Balancer Policy Assignments mit eintragbarer Priorisierung wird nicht berücksichtigt. Deshalb gibt es keine Switchovers zwischen Interfaces mit identischem Policy-Score.

 Dies ist der Default für bereits vor LCOS 10.80 vorhandene Einträge.

### Default-Wert:

Ja

## 4.2 Priority Bit bei WAN-Verbindung

Ab LCOS 10.80 wird das Priority Bit bei WAN-Verbindungen unterstützt.

Dazu wurde der Parameter **VLAN-Prioritätsmapping** erweitert und der neue Parameter **VLAN-Prio-Wert** eingeführt. Beide finden Sie in LANconfig unter **Kommunikation > Gegenstellen > Gegenstellen (DSL)**.

### VLAN-Prioritätsmapping

Dies legt fest, wie die Pakete im VLAN-Prioritätsfeld markiert werden sollen.

#### Wert

Alle Pakete, die auf das WAN geseendet werden, werden mit dem Prioritäts-Tag markiert, das unter **VLAN-Prio-Wert** konfiguriert ist. Das passiert aber nur, wenn auch ein VLAN ungleich 0 konfiguriert ist. Sonst würde es der Einstellung „Aus“ entsprechen.

### VLAN-Prio-Wert

Dieser Wert wird als VLAN-Prioritätswert gesetzt, wenn **VLAN-Prioritätsmapping** auf „Wert“ eingestellt wurde.

### 4.2.1 Ergänzungen im Setup-Menü

#### Prio-Mapping

Dieser Eintrag steuert die Funktionsweise des Prio-Mappings.

#### SNMP-ID:

2.2.19.17

#### Pfad Konsole:

Setup > WAN > DSL-Breitband-Gegenstellen

**Mögliche Werte:****aus**

Prio-Mapping ist deaktiviert.

**1TR-112**

Der Wert „1TR112“ mappt die Precedence (also die obersten 3 Bits) des DSCP in das Feld VLAN-Prio, wenn der DSCP nicht EF ist. Ist er EF, wird die Precedence von CS6 in die VLAN-Prio gemappt (110b).

**DSCP**

Der Wert „DSCP“ mappt die Precedence (also die obersten 3 Bits) des DSCP in das Feld VLAN-Prio.

**Wert**

Alle Pakete, die auf das WAN gegendet werden, werden mit dem Prioritäts-Tag markiert, das unter [2.2.19.20 Prio-Wert](#) auf Seite 15 konfiguriert ist. Das passiert aber nur, wenn auch ein VLAN ungleich 0 konfiguriert ist. Sonst würde es der Einstellung „Aus“ entsprechen.

**Default-Wert:**

aus

**Prio-Wert**

Dieser Wert wird als VLAN-Prioritätswert gesetzt, wenn [2.2.19.17 Prio-Mapping](#) auf Seite 14 auf „Wert“ eingestellt wurde.

**SNMP-ID:**

2.2.19.20

**Pfad Konsole:**

**Setup > WAN > DSL-Breitband-Gegenstellen**

**Mögliche Werte:**

0 ... 7

## 4.3 Automatischer APN

Ab LCOS 10.80 unterstützen Mobilfunk-Router die Möglichkeit, den APN aus der internen Carrier-List des Betriebssystems zu verwenden. Dazu ist es nicht mehr erforderlich, für eine WWAN-Verbindung einen APN manuell zu konfigurieren. Eine manuelle Konfiguration des APNs ist nur noch bei privaten APNs bzw. privaten Mobilfunknetzen nötig. Bei der automatischen Wahl des APNs werden alle gängigen Mobilfunkprovider unterstützt. Hierzu wird der Provider aus der SIM-Karte (MCC/MNC) abgefragt und in der internen Datenbank gesucht.

Dazu gibt es den neuen Parameter **APN-Modus** unter **Schnittstellen > WAN > Mobilfunk-Einstellungen > Mobilfunk-Profile**.

Mobilfunk-Profile - Neuer Eintrag

Name:

PIN:   Anzeigen

APN:

APN-Modus: Automatisch

PDP-Kontext: IPv4

Netz-Auswahl: Automatisch

Netz-Name:

Übertragungs-Betriebsart: Automatisch

Downstream-Rate: 0 kbit/s

Upstream-Rate: 0 kbit/s

Cold-Standby: Nein

5G-/4G-Bänder

Alle

<input type="checkbox"/> 2100 MHz (B1)	<input type="checkbox"/> 1900 MHz (B2)
<input type="checkbox"/> 1800 MHz (B3)	<input type="checkbox"/> 2100 MHz (B4)
<input type="checkbox"/> 850 MHz (B5)	<input type="checkbox"/> 2600 MHz (B7)
<input type="checkbox"/> 900 MHz (B8)	<input type="checkbox"/> 700 MHz (B12)
<input type="checkbox"/> 700 MHz (B13)	<input type="checkbox"/> 800 MHz (B20)
<input type="checkbox"/> 1900 MHz (B25)	<input type="checkbox"/> 800 MHz (B26)
<input type="checkbox"/> 700 MHz (B29)	<input type="checkbox"/> 2300 MHz (B30)
<input type="checkbox"/> 2600 MHz (B41)	

OK Abbrechen

### APN-Modus

Definiert in welchem Modus der APN verwendet werden soll.

- Bei Automatisch wird der APN aus der internen Datenbank der Provider-Einstellungen des Betriebssystems genommen. Hierzu wird der Provider aus der SIM-Karte (MCC/MNC) abgefragt und in der internen Datenbank gesucht. Der Modus „Automatisch“ funktioniert nur bei öffentlichen Provider-APNs und nicht bei privaten APNs. Bei privaten APNs muss der Modus auf "Manuell" gesetzt werden und der APN in das Feld "APN" eingetragen werden.
- Bei Manuell wird der APN aus dem Feld APN verwendet

## 4.3.1 Ergänzungen im Setup-Menü

### APN-Modus

Definiert in welchem Modus der APN verwendet werden soll.

### SNMP-ID:

2.23.41.1.14

### Pfad Konsole:

Setup > Schnittstellen > Mobilfunk > Profile



**Mögliche Werte:****Auto**

Bei Automatisch wird der APN aus der internen Datenbank der Provider-Einstellungen des Betriebssystems genommen. Hierzu wird der Provider aus der SIM-Karte (MCC/MNC) abgefragt und in der internen Datenbank gesucht. Der Modus „Automatisch“ funktioniert nur bei öffentlichen Provider-APNs und nicht bei privaten APNs. Bei privaten APNs muss der Modus auf „Manuell“ gesetzt werden und der APN in das Feld [2.23.41.1.3 APN](#) eingetragen werden.

**Manuell**

Bei Manuell wird der APN aus dem Feld [2.23.41.1.3 APN](#) verwendet.

**Default-Wert:**

Auto

## 4.4 Automatischer WWAN-Verbindungsaufbau bei unkonfigurierten Geräten

Ab LCOS 10.80 ist es möglich, dass Geräte mit WWAN über die Mobilfunkverbindung eine automatische Internetverbindung herstellen können, um damit ein Zero-Touch-Rollout mit der LANCOM Management Cloud durchzuführen. Dazu sind im LCOS neue Default-Einträge für den Aufbau einer WWAN-Gegenstelle vorhanden.

Dazu müssen folgenden Voraussetzungen erfüllt sein:

- Das Gerät muss ab Werk mindestens mit LCOS 10.80 ausgeliefert werden oder per Firmware-Update, z. B. per USB-Stick, auf die notwendige LCOS-Version gebracht werden.
- Die eingesteckte SIM-Karte darf keine PIN haben. Diese kann zuvor z. B. auf einem Mobiltelefon deaktiviert werden.
- Der APN des Providers muss in der internen Carrier-Liste des LCOS vorhanden sein. Nicht unterstützt wird das Szenario mit privaten APNs.
- Der Provider muss IPv4 unterstützen. Ein Zero-Touch-Rollout-Szenario über IPv6-Only-APNs wird derzeit nicht unterstützt.

Clients, die sich im LAN hinter dem Gerät befinden, können in diesem Zustand keine Verbindung ins Internet aufbauen, da das Gerät noch über die automatische LAN-IP-Adresse verfügt, mit der kein Forwarding möglich ist. Dazu muss das Gerät über eine feste IP-Adresse auf dem LAN-Interface verfügen. Dies passiert automatisch, wenn die LMC dem Gerät ein Netzwerk zuweist. Das Gerät selbst kann aber beliebige Ziele im Internet erreichen.

## 4.5 Parameter LTE-Anmeldung entfernt

Ab LCOS 10.80 entfällt der Parameter **LTE-Anmeldung** unter **Setup > Schnittstellen > Mobilfunk > Profile**.

## 4.6 Mobilfunk Cold Standby

Ab LCOS 10.80 gibt es den neuen Parameter **Cold-Standby** unter **Schnittstellen > WAN > Mobilfunk-Profile**.

Mobilfunk-Profile - Neuer Eintrag

Name:

PIN:   Anzeigen

APN:

APN-Modus: Automatisch

PDP-Kontext: IPv4

Netz-Auswahl: Automatisch

Netz-Name:

Übertragungs-Betriebsart: Automatisch

Downstream-Rate: 0 kbit/s

Upstream-Rate: 0 kbit/s

Cold-Standby: Nein

5G-/4G-Bänder

Alle

2100 MHz (B1)  1900 MHz (B2)

1800 MHz (B3)  2100 MHz (B4)

850 MHz (B5)  2600 MHz (B7)

900 MHz (B8)  700 MHz (B12)

700 MHz (B13)  800 MHz (B20)

1900 MHz (B25)  800 MHz (B26)

700 MHz (B29)  2300 MHz (B30)

2600 MHz (B41)

OK Abbrechen

### Cold-Standby

Dieser Parameter definiert, ob das Mobilfunk-Modem im Nicht-Backup-Fall ins Mobilfunknetz eingebucht sein soll. Bei „Ja“ ist das Mobilfunk-Modem im Nicht-Backup-Fall nicht im Mobilfunknetz eingebucht. Im Backup-Fall dauert es entsprechend länger, bis das Modul eine vollständige Backup-Verbindung aufgebaut hat. Diese Funktion wird nur im Zusammenhang mit der Nutzung der Backup-Tabelle unterstützt. Diese Funktion hat keine Auswirkung bzw. ist nicht möglich bei der Verwendung von administrativen Distanzen, da dort das WWAN-Modem immer eine aktive Datenverbindung aufgebaut hat. Default: Nein.

### 4.6.1 Ergänzungen im Setup-Menü

#### Cold-Standby

Definiert, ob das Mobilfunk-Modem im Nicht-Backup-Fall ins Mobilfunknetz eingebucht sein soll. Bei „Ja“ ist das Mobilfunk-Modem im Nicht-Backup-Fall nicht im Mobilfunknetz eingebucht. Im Backup-Fall dauert es entsprechend länger, bis das Modul eine vollständige Backup-Verbindung aufgebaut hat. Diese Funktion wird nur im Zusammenhang mit der Nutzung der Backup-Tabelle unterstützt. Diese Funktion hat keine Auswirkung bzw. ist nicht möglich bei der Verwendung von administrativen Distanzen, da dort das WWAN-Modem immer eine aktive Datenverbindung aufgebaut hat.

#### SNMP-ID:

2.23.41.1.15

**Pfad Konsole:**

Setup > Schnittstellen > Mobilfunk > Profile

**Mögliche Werte:**

Ja  
Nein

**Default-Wert:**

Nein

## 5 IPv6

### 5.1 Mehrere DHCPv6-Relay-Ziele

Ab LCOS 10.80 können im DHCPv6-Relay-Agent mehrere Server-Ziele konfiguriert werden, zu denen der Relay-Agent die Anfragen schickt. Die Anfragen werden immer an alle konfigurierten Server gleichzeitig gesendet.

Außerdem kann eine optionale IPv6-Absendeadresse angegeben werden, die der Relay-Agent für Pakete in Richtung DHCPv6-Server verwendet.

Sie finden die neuen Einstellungen unter **IPv6 > DHCPv6 > Relay-Agent-Interfaces**.

#### Ziel-Adresse

IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse „ff02::1:2“ sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.



Über die Parameter **2. Ziel-Adresse** bis **4. Ziel-Adresse** können Sie weitere Server-Ziele definieren.




Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.

#### Ziel-Interface

Das Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

---

 Über die Parameter **2. Ziel-Interface** bis **4. Ziel-Interface** können Sie weitere Server-Ziele definieren.

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.

#### Absende-Adresse (opt.)


Vergeben Sie hier eine optionale Absendeadresse an, die der Relay-Agent für Pakete in Richtung DHCPv6-Server verwendet.

## 5.1.1 Ergänzungen im Setup-Menü

### Ziel-Adresse

Definieren Sie die IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

---

 Über [2.70.3.3.1.6 Ziel-Adresse-2](#) auf Seite 22, [2.70.3.3.1.8 Ziel-Adresse-3](#) auf Seite 23 und [2.70.3.3.1.10 Ziel-Adresse-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.

#### SNMP-ID:

2.70.3.3.1.4

#### Pfad Konsole:

**Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste**

#### Mögliche Werte:

max. 39 Zeichen aus [A-Z] [a-z] [0-9] :

#### Default-Wert:


ff02::1:2

### Ziel-Interface

Definieren Sie das Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

---

 Über [2.70.3.3.1.7 Ziel-Interface-2](#) auf Seite 22, [2.70.3.3.1.9 Ziel-Interface-3](#) auf Seite 23 und [2.70.3.3.1.11 Ziel-Interface-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.5


**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 16 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default-Wert:***leer***Ziel-Adresse-2**

Definieren Sie hier eine zweite IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

---

 Über [2.70.3.3.1.4 Ziel-Adresse](#) auf Seite 21, [2.70.3.3.1.8 Ziel-Adresse-3](#) auf Seite 23 und [2.70.3.3.1.10 Ziel-Adresse-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.6


**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 39 Zeichen aus `[A-Z][a-z][0-9]:`**Default-Wert:***leer***Ziel-Interface-2**

Definieren Sie hier ein zweites Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

---

 Über [2.70.3.3.1.5 Ziel-Interface](#) auf Seite 21, [2.70.3.3.1.9 Ziel-Interface-3](#) auf Seite 23 und [2.70.3.3.1.11 Ziel-Interface-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.7

**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 16 Zeichen aus `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>[\]^_`~``**Default-Wert:***leer***Ziel-Adresse-3**

Definieren Sie hier eine dritte IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

---

 Über [2.70.3.3.1.4 Ziel-Adresse](#) auf Seite 21, [2.70.3.3.1.6 Ziel-Adresse-2](#) auf Seite 22 und [2.70.3.3.1.10 Ziel-Adresse-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.8


**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 39 Zeichen aus `[A-Z][a-z][0-9]:`**Default-Wert:***leer***Ziel-Interface-3**

Definieren Sie hier ein drittes Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

---

 Über [2.70.3.3.1.5 Ziel-Interface](#) auf Seite 21, [2.70.3.3.1.7 Ziel-Interface-2](#) auf Seite 22 und [2.70.3.3.1.11 Ziel-Interface-4](#) auf Seite 24 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.9


**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 16 Zeichen aus `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]^_`~``**Default-Wert:***leer***Ziel-Adresse-4**

Definieren Sie hier eine vierte IPv6-Adresse des (Ziel-) DHCPv6-Servers, an den der Relay-Agent DHCP-Anfragen weiterleiten soll. Die Adresse kann entweder eine Unicast- oder linklokale Multicast-Adresse sein. Bei Verwendung einer linklokalen Multicast-Adresse muss zwingend das Ziel-Interface angegeben werden, über das der DHCPv6-Server zu erreichen ist. Unter der linklokalen Multicast-Adresse ff02::1:2 sind alle DHCPv6-Server und Relay-Agenten auf einem lokalen Link erreichbar.

---

 Über [2.70.3.3.1.4 Ziel-Adresse](#) auf Seite 21, [2.70.3.3.1.6 Ziel-Adresse-2](#) auf Seite 22 und [2.70.3.3.1.8 Ziel-Adresse-3](#) auf Seite 23 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.


**SNMP-ID:**

2.70.3.3.1.10


**Pfad Konsole:****Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-Liste****Mögliche Werte:**max. 39 Zeichen aus `[A-Z][a-z][0-9]:`**Default-Wert:***leer***Ziel-Interface-4**

Definieren Sie hier ein viertes Ziel-Interface, über das der übergeordnete DHCPv6-Server oder der nächste Relay-Agent zu erreichen ist. Die Angabe ist zwingend erforderlich, wenn unter der Ziel-Adresse eine linklokale Multicast-Adresse konfiguriert wird, da linklokale Multicast-Adressen immer nur auf dem jeweiligen Link gültig sind.

---

 Über [2.70.3.3.1.5 Ziel-Interface](#) auf Seite 21, [2.70.3.3.1.7 Ziel-Interface-2](#) auf Seite 22 und [2.70.3.3.1.9 Ziel-Interface-3](#) auf Seite 23 können Sie weitere Server-Ziele definieren.

---

 Bei mehreren konfigurierten Server-Zielen werden die Anfragen immer an alle konfigurierten Server gleichzeitig gesendet.



**SNMP-ID:**

2.70.3.3.1.11

**Pfad Konsole:**

Setup &gt; IPv6 &gt; DHCPv6 &gt; Relay-Agent &gt; Interface-Liste

**Mögliche Werte:**

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

**Default-Wert:**

leer

**Ziel-Loopback**

Vergeben Sie hier eine optionale Absendeadresse an, die der Relay-Agent für Pakete in Richtung DHCPv6-Server verwendet.

**SNMP-ID:**

2.70.3.3.1.12

**Pfad Konsole:**

Setup &gt; IPv6 &gt; DHCPv6 &gt; Relay-Agent &gt; Interface-Liste

**Mögliche Werte:**

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

**Default-Wert:**

leer

## 5.2 Weitere Optionen für den DHCPv6-Client

Ab LCOS 10.80 können für den DHCPv6-Client bestimmte Optionen konfiguriert werden, die dann übertragen werden. Dies ist erforderlich, wenn der Internet-Provider bestimmte Daten in DHCPv6-Nachrichten erwartet. Die Optionen können in der Tabelle DHCPv6-Optionen unter **IPv6 > DHCPv6 > DHCPv6-Client > Weitere Optionen** frei konfiguriert werden.

The screenshot shows a dialog box titled 'Weitere Optionen - Neuer Eintrag'. It has the following fields and controls:

- Interface-Name:** A dropdown menu with a 'Wählen' button to its right.
- Options-Nummer:** A text input field containing the value '0'.
- Optionstyp:** A dropdown menu with 'String' selected.
- Optionswert:** An empty text input field.
- Option anfragen:** A dropdown menu with 'Nein' selected.
- At the bottom, there are two buttons: 'OK' and 'Abbrechen'.

**Interface-Name**

Interface auf dem der DHCPv6-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv6-LAN-Netzwerk.

**Options-Nummer**

Definiert die vergebene IANA-Nummer der DHCPv6-Option wie diese im RFC definiert ist.

**Optionstyp**

Definiert den Typ der DHCPv6-Option. Mögliche Werte: String, Integer8, Integer16, Integer32, IPv6-Adressen, Domain-List, Hexdump oder Dont-send



Der Options-Typ „Dont-send“ bewirkt, dass kein Optionsinhalt gesendet wird, sondern nur die Optionsnummer im Option-Request, falls im RFC kein Optionswert vorgesehen ist.

**Optionswert**

Definiert den Inhalt der DHCPv6-Option

Dabei kann, außer bei String, auch eine Komma- und / oder Leerzeichen-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene Werte in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: Elapsed-Time, Server-DUID, Reconfigure-Accept und Rapid-Commit.

**Option anfragen**

Definiert, ob die Optionsnummer im DHCPv6-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCPv6-Option definiert. Mögliche Werte: Ja, Nein

## 5.2.1 Ergänzungen im Setup-Menü

**Zusätzliche-Optionen**

In dieser Tabelle können bestimmte Optionen für den DHCPv6-Client konfiguriert werden.

**SNMP-ID:**

2.70.3.2.5

**Pfad Konsole:**

**Setup > IPv6 > DHCPv6 > Client**

**Interface-Name**

Interface auf dem der DHCPv6-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv6-LAN-Netzwerk.

**SNMP-ID:**

2.70.3.2.5.1

**Pfad Konsole:**

**Setup > IPv6 > DHCPv6 > Client > Zusätzliche-Optionen**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Options-Nummer**

Definiert die vergebene IANA-Nummer der DHCP-Option wie diese im RFC definiert ist.

**SNMP-ID:**

2.70.3.2.5.2

**Pfad Konsole:**

**Setup > IPv6 > DHCPv6 > Client > Zusätzliche-Optionen**

**Mögliche Werte:**

max. 5 Zeichen aus [0-9]

**Default-Wert:**

*leer*

**Options-Typ**

Definiert den Typ der DHCPv6-Option.

**SNMP-ID:**

2.70.3.2.5.3

**Pfad Konsole:**

**Setup > IPv6 > DHCPv6 > Client > Zusätzliche-Optionen**

**Mögliche Werte:**

**Integer8**  
**Integer16**  
**Integer32**  
**IPv6-Adressen**  
**Domain-Liste**  
**String**  
**Hexdump**  
**Nicht-Senden**

Dieser Options-Typ bewirkt, dass kein Optionsinhalt gesendet wird, sondern nur die Optionsnummer im Option-Request, falls im RFC kein Optionswert vorgesehen ist.

**Options-Wert**

Definiert den Inhalt der DHCPv6-Option.

Dabei kann, außer bei String, auch eine Komma- und / oder Leerzeichen-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene Werte in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: Elapsed-Time, Server-DUID, Reconfigure-Accept und Rapid-Commit.

**SNMP-ID:**

2.70.3.2.5.4

**Pfad Konsole:**

Setup > IPv6 > DHCPv6 > Client > Zusätzliche-Optionen

**Mögliche Werte:**

max. 254 Zeichen aus [A-Z] [a-z] [0-9] #@{|}~!\$%&'()\*+,-./:;<=>?[\]^\_`~`

**Default-Wert:**

leer

**Option-Anfragen**

Definiert, ob die Optionsnummer im DHCPv6-Option-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCPv6-Option definiert.

**SNMP-ID:**

2.70.3.2.5.5

**Pfad Konsole:**

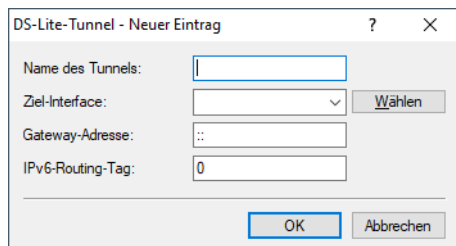
Setup > IPv6 > DHCPv6 > Client > Zusätzliche-Optionen

**Mögliche Werte:**

- Ja
- Nein

### 5.3 DS-Lite-Tunnel mit Ziel-Interface

Ab LCOS 10.80 gibt es die neue Spalte **Ziel-Interface** bei DS-Lite-Tunneln unter LANconfig **IPv4 > Tunnel > DS-Lite-Tunnel**.



**Ziel-Interface**

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET. Max. 16 Zeichen in Großbuchstaben.

### 5.3.1 Ergänzungen im Setup-Menü

**Ziel-Interface**

Name des darunterliegenden WAN-Interface bzw. der darunterliegenden Gegenstelle, z. B. INTERNET.

**SNMP-ID:**

2.2.40.5

**Pfad Konsole:**

**Setup > WAN > DS-Lite-Tunnel**

**Mögliche Werte:**

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

## 6 Firewall

### 6.1 Manuelle Ausführung von Aktionen der Aktionstabelle

Ab LCOS 10.80 können Aktionen der Aktionstabelle manuell ausgeführt werden, indem Ereignisse simuliert werden. Dabei können bestimmte Verbindungsereignisse (z. B. Aufbau, Abbau, Volumen-Budget-Ereignis etc.) ausgelöst werden, ohne dass das Ereignis tatsächlich auftritt. Damit können Einträge der Aktionstabelle getestet werden. Die jeweilige Aktion der Aktionstabelle, auf die das Ereignis zutrifft, wird dabei ausgeführt. Es werden immer alle Einträge ausgeführt, die auf das Ereignis passen.

Unter `/Setup/WAN` gibt es dazu eine neue Kommandozeilenaktion `Manueller-Aktions-Start`.

#### 6.1.1 Ergänzungen im Setup-Menü

##### Manueller-Aktions-Start


Über diese Aktion können Aktionen der Aktionstabelle manuell ausgeführt werden, indem Ereignisse simuliert werden. Dabei können bestimmte Verbindungsereignisse (z. B. Aufbau, Abbau, Volumen-Budget-Ereignis etc.) ausgelöst werden, ohne dass das Ereignis tatsächlich auftritt. Damit können Einträge der Aktionstabelle getestet werden. Die jeweilige Aktion der Aktionstabelle, auf die das Ereignis zutrifft, wird dabei ausgeführt. Es werden immer alle Einträge ausgeführt, die auf das Ereignis passen.

Beispiel: `do Manual-Action-Start internet/establish`

---

 Das Ergebnis der Ausführung kann dabei mit dem Trace „connect“ analysiert werden.

---

 Falls für eine Verbindung mehrere Anweisungs-Ketten (z. B. für verschiedene DynDNS-Hosts) hinterlegt sind, werden immer alle ausgeführt. Ob die Angabe einer IPv6-Adresse erforderlich ist, hängt vom jeweiligen Eintrag in der Aktionstabelle ab. Beim Test von DynDNS-Einträgen bzw. Einträgen, die eine IP-Adresse verwenden, muss in jedem Fall die IP-Adresse per `-4` bzw. `-6` übergeben werden.

##### SNMP-ID:

2.2.64

##### Pfad Konsole:

**Setup > WAN**

##### Mögliche Argumente:

**[-4 <IPv4-Address>]**

Optionale Angabe einer IPv4-Adresse

**[-6 <IPv6-Address>]**

Optionale Angabe einer IPv6-Adresse

**<Connection-Name>/<Condition>]**

<Condition> ist dabei eine der folgenden Bedingungen: ESTABLISH, DISCONNECT, FAILURE, ESTABLISH-FAILURE, VOLUME-BUDGET-EXPIRED, VOLUME-BUDGET-RESET.

Falls keine Bedingung angegeben wird, dann gilt als Default ein Verbindungsaufbau, also die Bedingung ESTABLISH.

# 7 Virtual Private Networks – VPN

## 7.1 LANCOM Trusted Access

Ab LCOS 10.80 wird LANCOM Trusted Access unterstützt, eine Lösung für Cloud-managed Secure Network Access.

LANCOM Trusted Access ist die vertrauenswürdige Network Access Security-Lösung für Unternehmensnetzwerke. Er ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs und schützt damit modernes hybrides Arbeiten von überall und jederzeit. Die LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Ihrer Organisation an und ermöglicht sowohl Cloud-managed VPN-Client-Vernetzung für den Zugriff auf ganze Netze als auch den Umstieg auf eine Zero-Trust-Sicherheitsarchitektur für eine umfassende Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung auf Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip). Bestehende Systeme zur Verwaltung von Benutzern und Benutzergruppen (Active Directory) lassen sich vollständig in die LANCOM Management Cloud (LMC) integrieren. Für kleinere Netzwerke bietet die LMC alternativ eine interne Benutzerverwaltung. LANCOM Trusted Access 100% DSGVO-konform und skaliert für Kleinunternehmen genauso wie für sehr große Netzwerke mit mehreren tausend Benutzern.

### show

Mittels des show-Befehls können Sie die Gruppen und die diesen zugeordneten jeweils gleichrangigen Benutzer („Peers“) anzeigen lassen.

#### Syntax:

```
show lta
Usage:
show lta <option> [<parameter>...]

Options:
groups [group1 ...]: if one or more groups are specified, show the given groups, otherwise show all groups
peers [peer1 ...]  : if one or more peers are specified, show the given peers, otherwise show all peers
help,
?                  : this help
```

#### Beispiel:

```
> l /Status/Firewall/LTA-Database/Groups/
Group-UUID                               IP-Address                               Peer
-----
550e8400-e29b-11d4-a716-446655440000    2001:db8::23                            PEER-1
550e8400-e29b-22d4-a726-446655440000    2001:db8::23                            PEER-1
550e8400-e29b-22d4-a726-446655440000    2001:db8::42                            PEER-2
550e8400-e29b-33d4-a736-446655440000    2001:db8::42                            PEER-2

> l /Status/VPN/LTA/Connections/
Peer                                     Certificate-ID                             User-ID                                     User-Name
-----
                                     Endpoint-ID                               Endpoint-Name
-----
PEER-1                                  11111111-1111-1111-1111-111111111111    22222222-2222-2222-2222-222222222222
TESTER-LTA-USER-NAME
                                     33333333-3333-3333-3333-333333333333    TESTER-LTA-ENDPOINT-NAME
PEER-2                                  11111111-1111-1111-1111-111111111111    22222222-2222-2222-2222-222222222222
TESTER-LTA-USER-NAME

> show lta groups
550e8400-e29b-11d4-a716-446655440000
    PEER-1                                2001:db8::23
550e8400-e29b-22d4-a726-446655440000
```



```

PEER-1                2001:db8::23
PEER-2                2001:db8::42

550e8400-e29b-33d4-a736-446655440000
PEER-2                2001:db8::42

> show lta peers
PEER-1                2001:db8::23
550e8400-e29b-11d4-a716-446655440000
550e8400-e29b-22d4-a726-446655440000

PEER-2                2001:db8::42
550e8400-e29b-22d4-a726-446655440000
550e8400-e29b-33d4-a736-446655440000

```

## 7.1.1 Ergänzungen im Setup-Menü

### Objekt-Tabelle

In der Objekttable werden diejenigen Elemente bzw. Objekte definiert, die in der Regeltabelle der Firewall verwendet werden sollen. Objekte können sein:

- > einzelne Rechner (MAC- oder IP-Adresse, Host-Name)
- > ganze Netze
- > Protokolle
- > Dienste (Ports oder Port-Bereiche, z. B. HTTP, Mail&News, FTP, ...)
- > Verknüpfung von Gruppen-UUIDs des LANCOM Trusted Access mit Stationsnamen

#### SNMP-ID:


2.8.10.1

#### Pfad Konsole:

**Setup > IP-Router > Firewall**

#### Name

Geben Sie hier einen eindeutigen Namen für dieses Objekt an.

-  Die Namen für Objekte des LANCOM Trusted Access beginnen immer mit dem Kürzel „LTA-“ und werden im Normalfall von der LANCOM Management Cloud erzeugt und verwaltet. Über diesen Namen können Sie ein solches LTA-Gruppenobjekt in einer Firewall-Regel als Quelle referenzieren.

#### SNMP-ID:

2.8.10.1.1

#### Pfad Konsole:

**Setup > IP-Router > Firewall > Objekt-Tabelle**

#### Mögliche Werte:

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

#### Default-Wert:


*leer*


**Beschreibung**


Die Elemente der Objekt-Tabelle lassen sich beliebig kombinieren und hierarchisch strukturieren. So können z. B. zunächst Objekte für die Protokolle TCP und UDP definiert werden. Später kann man darauf aufbauend Objekte z. B. für FTP (= TCP + Ports 20 und 21), HTTP (= TCP + Port 80) und DNS (= TCP, UDP + Port 53) anlegen. Diese können dann wiederum zu einem Objekt zusammengefasst werden, das alle Definitionen der Einzelobjekte enthält.

In der Objekttable können die Stationen und Dienste nach folgenden Regeln beschrieben werden:

**Tabelle 1: Objekte für Firewall-Aktionen**

Beschreibung	Objekt-ID	Beispiele und Bemerkungen
lokales Netz	%L	
Gegenstellen	%H	Name muss in DSL- / ISDN- / PPTP- oder VPN-Gegenstellenliste stehen
Hostname	%D	
MAC-Adresse	%E	00:A0:57:01:02:03
IP-Adresse	%A	%A10.0.0.1, 10.0.0.2; %A0 (alle Adressen)
Netzmaske	%M	%M255.255.255.0
Protokoll (TCP/UDP/ICMP etc.)	%P	%P6 (für TCP)
Dienst (Port)	%S	%S20-25 (für Ports 20 bis 25)
LANCOM Trusted Access	%g	 Die UUID für Objekte des LANCOM Trusted Access müssen folgende Kriterien erfüllen: <ul style="list-style-type: none"> <li>&gt; sie dürfen nur Hexadezimalzahlen ('0'...'9', 'a'...'f', 'A'...'F') und das Minus ('-') enthalten</li> <li>&gt; das Minus darf nur an den Positionen 8, 13, 18 und 23 sein</li> <li>&gt; das Minus muss insgesamt 4 Mal auftauchen</li> <li>&gt; die UUID muss 36 Zeichen lang sein</li> </ul> Beispiel: 550e8400-e29b-11d4-a716-446655440000

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

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

**SNMP-ID:**

2.8.10.1.2

**Pfad Konsole:**

Setup > IP-Router > Firewall > Objekt-Tabelle

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Typ**

Bestimmt den Stationstyp. Von der Auswahl hängt ab, welche der nachfolgenden Tabellenspalten ([>Lokales-Netzwerk](#), [Gegenstelle/Host-Name](#) und [Adresse/Praefix](#)) ausgefüllt werden müssen.

**SNMP-ID:**

2.70.5.9.2

**Pfad Konsole:**

**Setup > IPv6 > Firewall > Stationen**

**Mögliche Werte:****Lokales-Netzwerk**

Name eines lokalen Netzwerks z. B. INTRANET.

- > Nur die Spalte [Lokales-Netzwerk](#) ist auszufüllen.
- > Sie kann einen Interface-Namen enthalten, dann besteht die Station aus allen Netzen an diesem Interface.
- > Falls Sie eine Netzwerk-Gruppe eintragen, dann besteht die Station aus allen Präfixen unter [Adressen](#) mit dieser Gruppe.

**Gegenstelle**

Name einer WAN-Gegenstelle z. B. INTERNET.

- > Nur die Spalte [Gegenstelle/Host-Name](#) ist auszufüllen.
- > Sie kann ein WAN-Interface oder ein RAS-Template enthalten und löst zu allen Präfixen / Netzen auf, zu denen eine Route über dieses WAN-Interface oder über ein RAS-Interface zu diesem Template existiert.

**Praefix**

IPv6-Präfix

- > Nur die Spalte [Adresse/Praefix](#) ist auszufüllen.
- > Sie enthält ein IPv6-Präfix, z. B. „2001:db8::/32“.

**Identifizier**

- > Die Spalten [Lokales-Netzwerk](#) und [Adresse/Praefix](#) sind beide auszufüllen
- > [Lokales-Netzwerk](#) enthält ein WAN-Interface oder ein RAS-Template.
- > [Adresse/Praefix](#) enthält einen IPv6-Identifizier. Dies sind die letzten 64 Bit der IPv6-Adresse eines IPv6-Hosts, z. B. „::2a0:57ff:fe1b:3a6a“. Der Wert muss zwei führende Doppelpunkte enthalten.
- > Dieser Identifizier wird mit allen Netzen des Interfaces unter [Lokales-Netzwerk](#) bzw. den Netzwerken des RAS-Interfaces zum angegebenen Template zu einer Adresse kombiniert.
- > Außerdem wird zu jedem dieser Interfaces eine link-lokale Adresse mit diesem Identifizier gebildet.

**IP-Adresse**

- > Nur die Spalte [Adresse/Praefix](#) ist auszufüllen.
- > Sie enthält eine IPv6-Adresse, z. B. „2001:db8::1“

**benannter-Host**

Name eines lokalen IPv6-Hosts bzw. einer lokalen Station.

- Die Spalte *Gegenstelle/Host-Name* ist auszufüllen und enthält einen Hostnamen.
- Die Spalte *Lokales-Netzwerk* ist optional und kann ein LAN-Interface enthalten.
- Der Hostname wird mit Hilfe des DHCPv6-Servers oder des DNS-Servers im Gerät zu einer Hostadresse aufgelöst.
- Wenn ein Interface angegeben wurde, dann wird die Adresse nur genommen, falls sie über dieses Interface erreicht wird.

**MAC-Adresse**

Damit können Regeln für Ressourcen im internen Netzwerk angelegt werden, die anhand ihrer MAC-Adresse identifiziert werden. In Dual-Stack-Netzwerken erleichtert dies die Korrelation zu IPv4-Stationsobjekten, die ebenfalls anhand ihrer MAC-Adresse mit einer IPv4-Regel behandelt werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet.
- Die Spalte *Adresse/Praefix* enthält die MAC-Adresse anhand derer das Objekt identifiziert werden soll.



MAC-Adressen sind nur in Regeln als Quelle erlaubt, nicht jedoch als Ziel.

**Delegiertes-Praefix**

Damit kann insbesondere im Falle eines dynamischen Provider-Präfixes eine Regel für nachgeschaltete Router oder Ressourcen definiert werden.

- Die Spalte *Lokales-Netzwerk* ist optional und kann einen Netzwerknamen enthalten, in dem sich das Stations-Objekt befindet. Dies kann als Einschränkung auf das lokale Netzwerk verwendet werden.
- Die Spalte *Gegenstelle/Host-Name* ist erforderlich und sollte die Gegenstelle enthalten, von der das delegierte Präfix bezogen bzw. abgeleitet wird.
- Die Spalte *Adresse/Praefix* enthält ein Präfix oder eine Adresse, die mit dem vom Provider bezogenen Präfix verknüpft (Oder-Verknüpfung) wird. Wenn sich das Objekt auf das gesamte Präfix beziehen soll, so kann entweder `::/0` konfiguriert werden oder der Eintrag leer gelassen werden.

**Beispiel:** Der Provider delegiert das Präfix `2001:db8:1234::/48` auf der Gegenstelle INTERNET.

- Soll das Subnetz `abcd` verwendet werden, so muss als *Adresse/Praefix* der Wert `0:0:0:abcd::/48` konfiguriert werden.
- Soll nur die Adresse `2001:db8:0:23::dead:beef/128` verwendet werden, so muss als *Adresse/Praefix* `0:0:0:23::dead:beef/128` konfiguriert werden.
- Soll das gesamte Präfix verwendet werden, so muss als *Adresse/Praefix* `::/0` konfiguriert werden oder der Eintrag leer gelassen werden.

**Gruppen-UUID**

Dieser Wert dient zur Konfiguration von LANCOM Trusted Access-Gruppen.

Die Spalte *Gegenstelle/Host-Name* kann die UUID einer LTA-Gruppe enthalten.



Die UUID für Objekte des LANCOM Trusted Access müssen folgende Kriterien erfüllen:

- sie dürfen nur Hexadezimalzahlen ('0'... '9', 'a'... 'f', 'A'... 'F') und das Minus ('-') enthalten
- das Minus darf nur an den Positionen 8, 13, 18 und 23 sein
- das Minus muss insgesamt 4 Mal auftauchen
- die UUID muss 36 Zeichen lang sein

Beispiel: 550e8400-e29b-11d4-a716-446655440000

Die Spalten *Lokales-Netzwerk* und *Adresse/Praefix* müssen leer sein.

Die hier konfigurierten LTA-Gruppenobjekte können in [2.70.5.5 Stations-Liste](#) zu LTA-Gruppen-Listen zusammengefasst werden. Sowohl LTA-Gruppenobjekte als auch LTA-Gruppen-Listen können anschließend in einer Regel ([2.70.5.2 Forwarding-Regeln](#)) als Quelle verwendet werden.

**Default-Wert:**

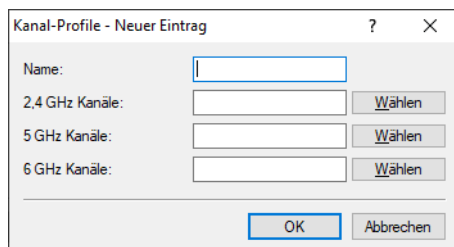
Lokales-Netzwerk

## 8 WLAN-Management

### 8.1 Kanal-Profile im WLC

Ab LCOS 10.80 wurde die Konfiguration der WLAN-Kanäle aus dem physikalischen WLAN-Profil in das neu geschaffene Kanal-Profil verlagert. Innerhalb des Kanal-Profiles können die WLAN-Kanäle je Frequenzband festgelegt werden. Auf diese Weise lassen sich auch Kanäle eindeutig definieren, deren Nummerierung sich in verschiedenen Frequenzbändern wiederholt (z. B. bei 2,4 GHz und 6 GHz).

Die Konfiguration der WLAN-Kanäle erstellen Sie unter **WLAN-Controller > Profile > Erweiterte Profile > Kanal-Profile**.



Kanal-Profile - Neuer Eintrag

Name:

2.4 GHz Kanäle:  Wählen

5 GHz Kanäle:  Wählen

6 GHz Kanäle:  Wählen

OK Abbrechen

#### Name

Name des Profils.

#### 2,4 GHz Kanäle

Wählen Sie die 2,4 GHz-Kanäle für dieses Profil aus.

#### 5 GHz Kanäle

Wählen Sie die 5 GHz-Kanäle für dieses Profil aus.

#### 6 GHz Kanäle

Wählen Sie die 6 GHz-Kanäle für dieses Profil aus.

Verknüpfen Sie das neu erzeugte Kanalprofil anschließend innerhalb des physikalischen WLAN-Profiles unter **WLAN-Controller > Profile > Physikalische WLAN-Parameter**.

### Kanal-Profil

Wählen Sie ein Kanal-Profil aus. Siehe [Kanal-Profil-Tabelle](#).



Das DEFAULT-Profil aktiviert alle erlaubten Kanäle des eingestellten Landes.



Beim Upgrade auf LCOS 10.80 werden die bisherigen Kanaleinstellungen automatisch in ein neues Kanalprofil migriert.

## 8.1.1 Ergänzungen im Setup-Menü

### Kanalprofil

Wählen Sie den Namen eines Kanal-Profiles aus. Siehe [2.37.1.30 Kanalprofile](#) auf Seite 39.



Das DEFAULT-Profil aktiviert alle erlaubten Kanäle des eingestellten Landes.

### SNMP-ID:


2.37.1.2.29

### Pfad Konsole:

**Setup > WLAN-Management > AP-Konfiguration > Radioprofile**

### Kanalprofile

Erstellen Sie in dieser Tabelle die Konfiguration der WLAN-Kanäle. Innerhalb des Kanal-Profiles können die WLAN-Kanäle je Frequenzband festgelegt werden. Auf diese Weise lassen sich auch Kanäle eindeutig definieren, deren Nummerierung sich in verschiedenen Frequenzbändern wiederholt (z. B. bei 2,4 GHz und 6 GHz). Verknüpfen Sie neu erzeugte Kanalprofile anschließend innerhalb des physikalischen WLAN-Profiles.

 Das DEFAULT-Profil aktiviert alle erlaubten Kanäle.

**SNMP-ID:**

2.37.1.30

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration****Name**Name des Profils. Geben Sie diesen in [2.37.1.2.29 Kanalprofil](#) auf Seite 39 an.**SNMP-ID:**

2.37.1.30.1

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Kanalprofile****2.4GHz-Kanaele**

Wählen Sie die 2,4 GHz-Kanäle für dieses Profil aus.

**SNMP-ID:**

2.37.1.30.2

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Kanalprofile****5GHz-Kanaele**

Wählen Sie die 5 GHz-Kanäle für dieses Profil aus.

**SNMP-ID:**

2.37.1.30.3

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Kanalprofile****6GHz-Kanaele**

Wählen Sie die 6 GHz-Kanäle für dieses Profil aus.



**SNMP-ID:**

2.37.1.30.4

**Pfad Konsole:**

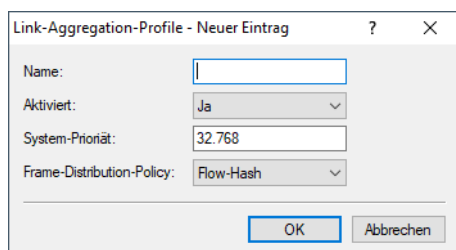
Setup &gt; WLAN-Management &gt; AP-Konfiguration &gt; Kanalprofile

## 8.2 LACP-Konfiguration via WLC

LACP nach IEEE 802.1AX erlaubt es, mehrere Ethernet-Verbindungen in einer sogenannten LAG (Link Aggregation Group) zu bündeln, um innerhalb der LAG den erreichbaren Datendurchsatz zu erhöhen. Hierzu werden auf der sendenden Seite die ausgehenden Pakete anhand der konfigurierten Frame-Distribution-Policy auf die verschiedenen Einzel-Links innerhalb der LAG verteilt.

Die LACP-Konfiguration der verwalteten Access Points kann durch den WLC ab LCOS 10.80 RU1 vorgegeben und konfiguriert werden.

Die Konfiguration der Link-Aggregation-Profiles erstellen Sie unter **WLAN-Controller > Profile > Erweiterte Profile > Link-Aggregation-Profiles**.

**Name**

Der Name dieser LAG (Link Aggregation Group).

**Aktiviert**

Aktiviert bzw. deaktiviert diese LAG (Link Aggregation Group).

**System-Priorität**

Die Systempriorität dieser LAG (Link Aggregation Group).

**Frame-Distribution-Policy**

Frame-Distribution-Policy dieser LAG (Link Aggregation Group). Mögliche Optionen:

**Flow-Hash**

Für ausgehende Pakete wird ein Flow-Hash über die enthaltenen IP-Adressen und TCP/UDP-Ports gebildet und anhand dessen die Pakete auf die einzelnen Links der LAG verteilt. Hiermit erreicht man eine Verteilung auf Session-Ebene, so dass auch Sessions eines einzelnen Clients auf mehrere Links verteilt werden können. Diese Einstellung wird für die meisten Szenarien empfohlen.

**Quell-Ziel-MAC**

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

## 8.2.1 Ergänzungen im Setup-Menü

### Linkaggregierungsprofile

LACP nach IEEE 802.1AX erlaubt es, mehrere Ethernet-Verbindungen in einer sogenannten LAG (Link Aggregation Group) zu bündeln, um innerhalb der LAG den erreichbaren Datendurchsatz zu erhöhen. Hierzu werden auf der sendenden Seite die ausgehenden Pakete anhand der konfigurierten Frame-Distribution-Policy auf die verschiedenen Einzel-Links innerhalb der LAG verteilt.

**SNMP-ID:**

2.37.1.29

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration****Name**

Der Name dieser LAG (Link Aggregation Group).

**SNMP-ID:**

2.37.1.29.1

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Linkaggregierungsprofile****Mögliche Werte:**max. 31 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()*+,-./:;<=>?[\]^_.`**Default-Wert:***leer***Aktiv**

Aktiviert bzw. deaktiviert diese LAG (Link Aggregation Group).

**SNMP-ID:**

2.37.1.29.2

**Pfad Konsole:****Setup > WLAN-Management > AP-Konfiguration > Linkaggregierungsprofile****Mögliche Werte:****Nein**

Deaktiviert

**Ja**

Aktiviert

**Default-Wert:**

Nein

**Systemprioritaet**

Die Systempriorität dieser LAG (Link Aggregation Group).

**SNMP-ID:**

2.37.1.29.3

**Pfad Konsole:**

**Setup > WLAN-Management > AP-Konfiguration > Linkaggregierungsprofile**

**Mögliche Werte:**

max. 5 Zeichen aus [0-9]

**Default-Wert:**

32768

**Frame-Verteilungs-Regel**

Frame-Distribution-Policy dieser LAG (Link Aggregation Group).

**SNMP-ID:**

2.37.1.29.4

**Pfad Konsole:**

**Setup > WLAN-Management > AP-Konfiguration > Linkaggregierungsprofile**

**Mögliche Werte:****Flow-Hash**

Für ausgehende Pakete wird ein Flow-Hash über die enthaltenen IP-Adressen und TCP/UDP-Ports gebildet und anhand dessen die Pakete auf die einzelnen Links der LAG verteilt. Hiermit erreicht man eine Verteilung auf Session-Ebene, so dass auch Sessions eines einzelnen Clients auf mehrere Links verteilt werden können. Diese Einstellung wird für die meisten Szenarien empfohlen.

**Quell-Ziel-MAC**

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

## 9 Backup-Lösungen

### 9.1 Unterstützung von vRouter-Redundanz in Amazon AWS

Ab LCOS 10.80 können Sie die Unterstützung von vRouter-Redundanz in Amazon AWS auch über LANconfig einrichten.

Konfigurieren Sie die vRouter-Redundanz für AWS in LANconfig unter **Sonstige Dienste > Dienste > Cloud Provider > AWS HA-Redundanz**.

The screenshot shows the 'Cloud Provider' configuration area in LANconfig. It contains a text box with instructions: 'Konfigurieren Sie hier die Parameter, um die Routing-Tabelle bei Cloud-Providem per API im Backup-Fall umzuschreiben.' Below this is a button labeled 'AWS HA-Redundanz...'. Below the button is a dialog box titled 'AWS HA-Redundanz - Neuer Eintrag'. The dialog box has the following fields: 'Profilname:' (text input), 'Route-Tabelle:' (text input), 'CIDR-IP:' (text input), 'ENI:' (text input), 'Region:' (text input), 'Netzwerkname:' (dropdown menu with a 'Wählen' button), and 'Kommentar:' (text input). At the bottom of the dialog are 'OK' and 'Abbrechen' buttons.

#### Profilname

Eindeutiger Name des Profils. Über diesen Namen wird das Profil im Kommando zur Änderung der Route referenziert.

#### Route-Tabelle

Name der Routing-Tabelle die in AWS geändert werden soll, z. B. „rtb-099605ce6cb4ac319“. Diesen Wert erhalten Sie aus der AWS-Management-Oberfläche.

#### CIDR IP

Präfix in der Routing-Tabelle, für das der Next-Hop geändert werden soll, z. B. „0.0.0.0/0“.

#### ENI

Name des AWS-Netzwerkadapters (Elastic Network Interface) der als Next-Hop durch das Kommando gesetzt werden soll, z. B. „eni-00c734d6da1fd8968“. Diesen Wert erhalten Sie aus der AWS-Management-Oberfläche.

#### Region

Region, in der sich die AWS Routing-Tabelle befindet, z. B. „eu-central-1“

#### Netzwerkname

Name des Interfaces bzw. der Gegenstelle im vRouter über die der vRouter die AWS-API erreichen kann, z. B. „INTERNET“.

#### Kommentar

Vergeben Sie einen aussagekräftigen Kommentar für diesen Eintrag.

## 10 Weitere Dienste

### 10.1 DHCPv4-Client Optionen

Ab LCOS 10.80 können für den DHCPv4-Client bestimmte Optionen konfiguriert werden, die dann übertragen werden. Dies ist erforderlich, wenn der Internet-Provider bestimmte Daten in DHCP-Nachrichten erwartet. Die Optionen können in der Tabelle DHCP-Optionen unter **IPv4 > DHCPv4 > DHCP-Client > DHCP-Optionen** frei konfiguriert werden.

#### Interface

Interface auf dem der DHCPv4-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv4-LAN-Netzwerk.

#### Options-Nummer

Definiert die vergebene IANA-Nummer der DHCP-Option wie diese im RFC definiert ist.

#### Options-Typ

Definiert den Typ der DHCP-Option. Mögliche Werte: String, Integer8, Integer16, Integer32 oder IP-Adresse

#### Options-Wert

Definiert den Inhalt der DHCP-Option

Dabei kann, außer bei String, auch eine Komma- und/oder Space-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen, für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57) und end (255).

#### Request-Liste

Definiert, ob die Optionsnummer im DHCP-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCP-Option definiert. Mögliche Werte: Ja, Nein

#### 10.1.1 Ergänzungen im Setup-Menü

##### Client

Hier finden Sie alle Einstellungen zum DHCP-Client für IPv4.

**SNMP-ID:**

2.10.40

**Pfad Konsole:****Setup > DHCP****Zusaetzliche-Optionen**

In dieser Tabelle können bestimmte Optionen für den DHCPv4-Client konfiguriert werden.

**SNMP-ID:**

2.10.40.5

**Pfad Konsole:****Setup > DHCP > Client****Interface**

Interface auf dem der DHCPv4-Client diese Option verwenden soll, z. B. WAN-Gegenstelle oder IPv4-LAN-Netzwerk.

**SNMP-ID:**

2.10.40.5.1

**Pfad Konsole:****Setup > DHCP > Client > Zusaetzliche-Optionen****Mögliche Werte:**max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Default-Wert:***leer***Options-Nummer**

Definiert die vergebene IANA-Nummer der DHCP-Option wie diese im RFC definiert ist.

**SNMP-ID:**

2.10.40.5.2

**Pfad Konsole:****Setup > DHCP > Client > Zusaetzliche-Optionen****Mögliche Werte:**max. 3 Zeichen aus `[0-9]`

**Default-Wert:***leer***Options-Typ**

Definiert den Typ der DHCP-Option.

**SNMP-ID:**

2.10.40.5.3

**Pfad Konsole:****Setup > DHCP > Client > Zusätzliche-Optionen****Mögliche Werte:**

**String**  
**Integer8**  
**Integer16**  
**Integer32**  
**IP-Adresse**

**Options-Wert**

Definiert den Inhalt der DHCP-Option

Dabei kann, außer bei String, auch eine Komma- und/oder Space-separierte Liste angegeben werden. Für Integerwerte gelten die C-Codierungen, für Zahlen, d. h. 0x ergibt einen Hexwert und wenn die Zahl mit 0 beginnt ist es ein Oktal-Wert. Zusätzlich kann beim Typ Integer8 auch ein einzelner Hex-String (mit gerader Länge) ohne Separator angegeben werden. Vorhandene in den Standard-Optionen können überschrieben werden. Die folgenden Optionen können nicht überschrieben bzw. konfiguriert werden: padding (0), overload (52), message-type (53), server-id (54), request-list (55), message-size (57) und end (255).

**SNMP-ID:**

2.10.40.5.4

**Pfad Konsole:****Setup > DHCP > Client > Zusätzliche-Optionen****Mögliche Werte:**max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`**Default-Wert:***leer***Request-Liste**

Definiert, ob die Optionsnummer im DHCP-Request angefragt werden soll. Das Verhalten wird über das jeweilige RFC der DHCP-Option definiert.

**SNMP-ID:**

2.10.40.5.5

**Pfad Konsole:****Setup > DHCP > Client > Zusätzliche-Optionen****Mögliche Werte:**nein  
ja

## 10.2 Accounting

Ab LCOS 10.80 wurde das Accounting erweitert. Neben der Unterstützung für IPv6 ist eine Funktion zur Darstellung des aktuellen Datendurchsatzes von einzelnen Stationen oder logischen Schnittstellen im Netzwerk neu hinzugekommen. Diese Funktion ist besonders zu Analysezwecken geeignet, wenn geprüft werden soll, welche Station im Netzwerk zur aktuellen Zeit welchen Datenverkehr verursacht. Damit können z. B. Stationen identifiziert werden, die die Internetverbindung auslasten oder über welche Schnittstelle wie viel Datenverkehr zum aktuellen Zeitpunkt läuft.

Aus Performance-Gründen wird empfohlen, diese Funktion nur zur Zeit der laufenden Analyse zu aktivieren und danach wieder zu deaktivieren. Für eine umfangreichere Überwachung des Datenverkehrs wird Netflow in Zusammenhang mit einem externen Collector empfohlen.

Um die Analyse-Funktion zu nutzen, verwenden Sie die Kommandozeile und setzen unter /setup/accounting den Schalter „Aktiv“ auf „Ja“. Setzen Sie das „Intermittent-Reporting-Intervall“ auf einen kleinen Wert in Sekunden, z. B. 5 Sekunden.

Um die Funktion nach der Analyse wieder zu deaktivieren, setzen Sie den Schalter „Aktiv“ auf „Nein“.

Verwenden Sie zur Anzeige des aktuellen Durchsatzes pro Benutzer das Kommando „show accounting users“.

```
show accounting users
```

Username	Interface	Rx-Total	Tx-Total	Rx-IPv4	Tx-IPv4	Rx-IPv6	Tx-IPv6
192.168.1.7	INTERNET	0 Bit/s	115 Bit/s	0 Bit/s	115 Bit/s	0 Bit/s	0 Bit/s
192.168.1.9	INTERNET	9.38 KBit/s	3.92 KBit/s	9.38 KBit/s	3.92 KBit/s	0 Bit/s	0 Bit/s

```
Next update of accounting bandwidth data in: 3s
```

Alternativ zum Show-Kommando kann auch die Status-Tabelle /status/accounting/benutzer-bandbreitenverbrauch aufgerufen werden.

Das Show-Kommando hat mehrere Optionen, die mit ? angezeigt werden können:

```
> show accounting ?
```

Anzeige von Kurzzeit-Bandbreiten-Statistikdaten des Accountings.

HINWEIS: Das Accounting muss eingeschaltet und das Intermittent-Reporting-Intervall gesetzt sein. Alle Bandbreiten-Daten werden in diesem Intervall aktualisiert.

VERWENDUNG:

```
show accounting-bandwidth <BEFEHL> [FLAGS]:
```

BEFEHLE:

interfaces: Im Accounting aufgezeichneter Bandbreitenverbrauch, aufgeschlüsselt nach Interfaces

users: Im Accounting aufgezeichneter Bandbreitenverbrauch, aufgeschlüsselt nach Benutzern und Interfaces

FLAGS:

-bps: Gibt alle Werte in der Einheit Bit/s ohne Nachkommastellen aus

-kpbs: Gibt alle Werte in der Einheit KBit/s mit 3 festen Nachkommastellen aus

-mbps: Gibt alle Werte in der Einheit MBit/s mit 3 festen Nachkommastellen aus

-gbps: Gibt alle Werte in der Einheit GBit/s mit 3 festen Nachkommastellen aus

HINWEIS: Nur eines der Einheiten-Flags kann gleichzeitig angegeben werden. Wird keines angegeben, wird die Einheit automatisch bestimmt und die Ausgabe erfolgt mit 3 signifikanten Stellen.

-compact: Beschränkt die Ausgabe auf den Gesamt-Bandbreitenverbrauch je Übertragungsrichtung



```
-totals-only:      (nur fuer Befehl 'users') Zeigt die Benutzer-Bandbreiten nicht fuer jedes Interface
gesondert an, sondern aufsummiert
```

Beispiele:

„show accounting interfaces“ zeigt die Auslastung bzw. aktuellen Datendurchsatz der Interfaces an. Diese Information findet sich auch in der Tabelle /Status/Accounting/Interface-Bandbreitenverbrauch.

Mit dem Befehl „repeat 5 show accounting users“ auf der Konsole können Sie das Kommando alle 5 Sekunden automatisch anzeigen lassen.

## 10.2.1 Arbeitsweise

Accounting-Benutzer werden über ihren Benutzernamen identifiziert. Potentielle Accounting-Benutzer sind:

- > Alle Stationen im LAN (Benutzername ist ihre IPv4 oder IPv6-Adresse, oder, sofern er dem Router über DNS bekannt ist, der Hostname der Station)
- > Alle VPN-Gegenstellen (Benutzername ist der Gegenstellenname)
- > Alle ausgewählten RAS-Clients (Benutzername ist die RAS-Client-ID; Mehrfacheinwahlen werden der selben ID zugeordnet)

Der vom Accounting gezählte Datenverkehr ist jeder Datenverkehr, der zwischen einem Benutzer und einer IP-Adresse hinter einem der folgenden Interfacetypen stattfindet (unabhängig ob Rx- oder Tx-Traffic):

- > WAN
- > RAS
- > VPN

Bei einer Verbindung von z. B. VPN zu VPN wird der Traffic gezählt und für beide VPN-Benutzer getrennt verbucht.

Das Accounting zeichnet für jeden Benutzer den Datenverkehr mit jeder Gegenstelle separat auf. Das heißt: Datenverkehr von z. B. VPN zu WAN1 und Datenverkehr von VPN zu WAN2 sind separate Datensätze.

Das Accounting zeichnet jeweils aus Sicht des Benutzers sowohl eingehende und ausgehende Daten als auch IPv4- und IPv6-Traffic getrennt auf. Das bedeutet, dass ein IPv6-Datenpaket von z. B. VPN1 zu VPN2 für VPN1 als IPv6-Tx, und für VPN2 als IPv6-Rx gezählt wird.

Außerdem zeichnet das Accounting die Anzahl der aufgetretenen Datenströme (Sessions) auf, diese allerdings nicht getrennt nach Rx und Tx.

Bidirektionaler Datenverkehr wird als 2 Sessions gezählt, da 2 Datenströme vorliegen. Je ein aus Benutzersicht eingehender und ein ausgehender Datenstrom.

## 10.2.2 Ein- bzw. Ausschalten des Accountings im laufenden Betrieb

Die Prüfung, ob eine Datenverbindung vom Accounting gezählt wird, wird mit dem Aufbau der Verbindung (erstes Datenpaket) getroffen. Datenverbindungen, die bereits bestehen, wenn das Accounting eingeschaltet wird, werden vom Accounting nicht betrachtet.

Wird das Accounting im laufenden Betrieb ausgeschaltet, so werden die Datenverbindungen, die aktuell laufen, nicht mehr in die Accounting-Daten aufgenommen.

## 10.2.3 Zählung des Datenverkehrs

In der Standardeinstellung wird Traffic immer dann beim Accounting gemeldet, wenn eine Datenverbindung (in Form einer Firewallsession) endet, also etwa nach einem Timeout innerhalb der Firewall oder beim Schließen einer TCP-Verbindung. Bei lange laufenden Verbindungen kann das zu einer erheblichen Verzögerung führen, bis Datenverkehr tatsächlich in den Accounting-Statustabellen erscheint. Um dieses Problem zu behandeln, wurde eine Zwischenmeldungs-Funktionalität namens „Intermittent-Reporting“ in das Accounting integriert, welche Teilaufzeichnungen in festen Intervallen beim Accounting einträgt. Wie oft dies passiert, wird über das Intermittent-Reporting-Intervall konfiguriert. Im Default ist dies auf 0 eingestellt; d. h. die Funktionalität ist deaktiviert. Wird dort ein Wert zwischen 1

und 30 eingetragen, so definiert diese Einstellung das Intervall in Sekunden, in dem Datenverbindungs-Zwischenmeldungen beim Accounting eingehen.

Die Zwischenmeldungen erhöhen die Systemlast abhängig von der Anzahl der aktiven Datenverbindungen. Die Zwischenmeldungen der Datenverbindungen werden unabhängig voneinander durchgeführt (also nicht alle auf einmal), um Lastspitzen zu vermeiden.

Das Intermittent Reporting kann bei laufendem Accounting jederzeit eingeschaltet werden, die erste Zwischenmeldung enthält dann den kompletten bis zum Einschaltzeitpunkt gemessenen Datenverkehr der einzelnen Datenflüsse.

## 10.2.4 Weitere Änderungen beim Accounting

Bei der Konfiguration des Accounting ist der Parameter **Unterscheidungskriterium** entfallen.

### Entfallene Menüeinträge

Entfernt wurden die folgenden Menüeinträge:

- Sortieren-nach (SNMP ID: 2.18.3)
- Aktuelle-User (SNMP ID: 2.18.4)
  - Username (SNMP ID: 2.18.4.1)
  - MAC-Adresse (SNMP ID: 2.18.4.2)
  - Gegenstelle (SNMP ID: 2.18.4.3)
  - Verbindungs-Typ (SNMP ID: 2.18.4.4)
  - Rx-KBytes (SNMP ID: 2.18.4.5)
  - Tx-KBytes (SNMP ID: 2.18.4.6)
  - Gesamt-Zeit (SNMP ID: 2.18.4.8)
  - Verbindungen (SNMP ID: 2.18.4.9)
- Accounting-Liste (SNMP ID: 2.18.5)
  - Username (SNMP ID: 2.18.5.1)
  - MAC-Adresse (SNMP ID: 2.18.5.2)
  - Gegenstelle (SNMP ID: 2.18.5.3)
  - Verbindungs-Typ (SNMP ID: 2.18.5.4)
  - Rx-KBytes (SNMP ID: 2.18.5.5)
  - Tx-KBytes (SNMP ID: 2.18.5.6)
  - Gesamt-Zeit (SNMP ID: 2.18.5.8)
  - Verbindungen (SNMP ID: 2.18.5.9)
- Loeschen-Accounting-Liste (SNMP ID: 2.18.6)
- Schnappschuss-erstellen (SNMP ID: 2.18.7)
- Letzter-Schnappschuss (SNMP ID: 2.18.9)
  - Username (SNMP ID: 2.18.9.1)
  - MAC-Adresse (SNMP ID: 2.18.9.2)
  - Gegenstelle (SNMP ID: 2.18.9.3)
  - Verbindungs-Typ (SNMP ID: 2.18.9.4)

- > Rx-KBytes (SNMP ID: 2.18.9.5)
- > Tx-KBytes (SNMP ID: 2.18.9.6)
- > Gesamt-Zeit (SNMP ID: 2.18.9.8)
- > Verbindungen (SNMP ID: 2.18.9.9)
  
- > Diskriminator (SNMP ID: 2.18.10)

## 10.2.5 Ergänzungen im Setup-Menü

### Intermittent-Reporting-Intervall

Definiert in welchem Intervall in Sekunden die Informationen im Show-Kommando „show accounting“ bzw. den entsprechenden Status-Tabellen aktualisiert werden.

**SNMP-ID:**

2.18.16

**Pfad Konsole:**

**Setup > Accounting**

**Mögliche Werte:**

0 ... 30 Sekunden

**Besondere Werte:**

**0**

Ausgeschaltet

### Status-Tabellen-Einträge-Limit

Gibt an, wie viele Einträge das Accounting maximal speichert.

**SNMP-ID:**

2.18.17

**Pfad Konsole:**

**Setup > Accounting**

**Mögliche Werte:**

0 ... 999.999 Einträge

**Besondere Werte:**

**0**

Unbegrenzt

## 10.3 Neuer Netflow-Parameter „Active-Flow-Timeout“

Ab LCOS 10.80 können Sie unter **Meldungen/Monitoring > Protokolle** im Abschnitt **NetFlow / IPFIX** den neuen Parameter **Active-Flow-Timeout** setzen.

### Active-Flow-Timeout

Definiert das Intervall in Sekunden nachdem ein laufender Datenstrom per Netflow exportiert wird. Damit ist es möglich, länger laufende Sessions, z. B. große Downloads, schon während der Laufzeit zu exportieren. Der weitere Datenverkehr wird dann als ein neuer Datenfluss gewertet und die Aufzeichnung des Datenverkehrs für die Meldung beim Collector beginnt von neuem.

Mögliche Werte: 60-1800 Sekunden (0 schaltet die Funktion aus)

### 10.3.1 Ergänzungen im Setup-Menü

#### Active-Flow-Timeout

Definiert das Intervall in Sekunden nachdem ein laufender Datenstrom per Netflow exportiert wird. Damit ist es möglich, länger laufende Sessions, z. B. große Downloads, schon während der Laufzeit zu exportieren. Der weitere Datenverkehr wird dann als ein neuer Datenfluss gewertet und die Aufzeichnung des Datenverkehrs für die Meldung beim Collector beginnt von neuem.

#### SNMP-ID:

2.109.5

#### Pfad Konsole:

Setup > NetFlow

#### Mögliche Werte:

60 ... 1800 Sekunden

#### Besondere Werte:

0

Ausgeschaltet

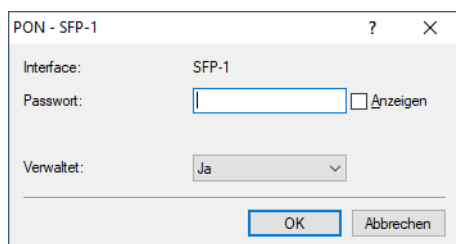
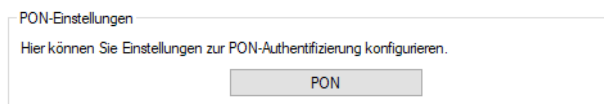
#### Default-Wert:

1800

## 10.4 PON-Passwort in hexadezimalen Format

Ab LCOS 10.80 können Sie das PON-Passwort neben der bisherigen Darstellung mit 10 ASCII-Zeichen nun auch als 20 hexadezimale Zeichen eingeben.

Die Einstellung für das PON-Passwort finden Sie wie bisher in LANconfig unter **Interfaces > WAN > PON** oder in der Konsole unter **Setup > Schnittstellen > PON > Password**.



### Passwort

Geben Sie hier das PON-Passwort ein, falls Ihr Provider eine Authentifizierung per Passwort durchführt. Andere Begriffe für PON-Passwort sind „ONT-Installationskennung“ oder „PLOAM-Passwort“. Das Passwort muss aus exakt 10 (für ASCII) oder 20 Zeichen (für hexadezimale Darstellung) bestehen, ohne das führende Präfix 0x für hexadezimale Darstellungen. Verwendet der Provider z. B. nur 14 Zeichen, so muss das Passwort durch manuelles Anhängen von Nullen (0) aufgefüllt werden. Das Passwort ist im Default leer.

Das PON-Passwort für Ihren Anschluss erhalten Sie von Ihrem Internet-Provider.

### 10.4.1 Ergänzungen im Setup-Menü

#### Passwort

Geben Sie hier das PON-Passwort ein, falls Ihr Provider eine Authentifizierung per Passwort durchführt. Andere Begriffe für PON-Passwort sind „ONT-Installationskennung“ oder „PLOAM-Passwort“. Das Passwort muss aus exakt 10 (für ASCII) oder 20 Zeichen (für hexadezimale Darstellung) bestehen, ohne das führende Präfix 0x für hexadezimale Darstellungen. Verwendet der Provider z. B. nur 14 Zeichen, so muss das Passwort durch manuelles Anhängen von Nullen (0) aufgefüllt werden. Das Passwort ist im Default leer.

Das PON-Passwort für Ihren Anschluss erhalten Sie von Ihrem Internet-Provider.

#### SNMP-ID:

2.23.23.3

#### Pfad Konsole:

**Setup > Schnittstellen > PON**

#### Mögliche Werte:

Entweder 10 ASCII oder 20 hexadezimale Zeichen aus

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

**Default-Wert:***leer*

## 10.5 ACME-Client

Ab LCOS 10.80 wird der Automatic Certificate Management Environment (ACME) Client nach [RFC 8555](#) für Let's Encrypt Zertifikate unterstützt. [Let's Encrypt](#) ist eine freie und offene Zertifizierungsstelle, die es ermöglicht, kostenfreie SSL- / TLS-Zertifikate zu beziehen. Die Zertifikate können für die WEBconfig sowie für den Public Spot verwendet werden.

Voraussetzung für die Nutzung von Let's Encrypt ist, dass das Gerät über einen öffentlich auflösbaren Domain-Namen, z. B. DynDNS, verfügt. Für eine korrekte Nutzung der Zertifikate muss die WEBconfig des Geräts über den Domain-Namen aufgerufen werden und nicht über die IP-Adresse. Bei Aufruf der WEBconfig über die IP-Adresse schlägt die Zertifikatsprüfung fehl, da Let's Encrypt-Zertifikate auf Domain-Namen und nicht auf IP-Adressen ausgestellt werden.

Bei Let's Encrypt werden Zertifikate ausgestellt, wenn ein Gerät beweisen kann, dass es den Domain-Namen unter Kontrolle hat. Dazu stellt Let's Encrypt eine sogenannte „Challenge“, die das Gerät erfüllen muss. Diesen Prozess führt der ACME-Client im Gerät automatisch durch. Ebenso erneuert der ACME-Client automatisch das Zertifikat vor einer definierten Ablauffrist des Zertifikats.


In der Konfiguration muss zunächst ein Domain-Name konfiguriert werden. Das Gerät stellt dann automatisch einen Zertifikatsantrag bei Let's Encrypt und öffnet temporär z. B. den Port 443 oder 80. Daraufhin überprüft Let's Encrypt, ob das Gerät und die zuvor gestellte Challenge (z. B. Token) unter dem angegebenen Domain-Namen und Port 443 oder 80 erreichbar ist. Ist die Prüfung erfolgreich, so wird das Zertifikat ausgestellt. Das Gerät erneuert automatisch das Zertifikat bevor dieses abläuft. Das Gerät öffnet in diesem Prozess kurzzeitig den Port 80 bzw. 443 für diese Challenge und schließt diesen im zweiten Schritt auch wieder.

In folgenden Szenarien ist ein Einsatz von Let's Encrypt nicht möglich bzw. schlägt fehl:

- Das Gerät verfügt über keine öffentliche IP-Adresse
- Eine vorgeschaltete Firewall blockiert den Zugriff auf Port 443 oder 80 vom Internet aus

Grundsätzlich werden auch mehrere Domain-Namen im SAN-Feld (Subject Alternative Name) des Zertifikats unterstützt.

---

 Standardmäßig wird Port 443 und das Verfahren `tls-alpn-01` für die ACME-Challenge verwendet. Soll das Verfahren `http-01` auf Port 80 verwendet werden, muss in der Konfiguration im LANconfig der Parameter **Allgemein > Admin > Zugriffseinstellungen > HTTP-Zugang von einer WAN-Schnittstelle** auf „Automatisch“ eingestellt sein.

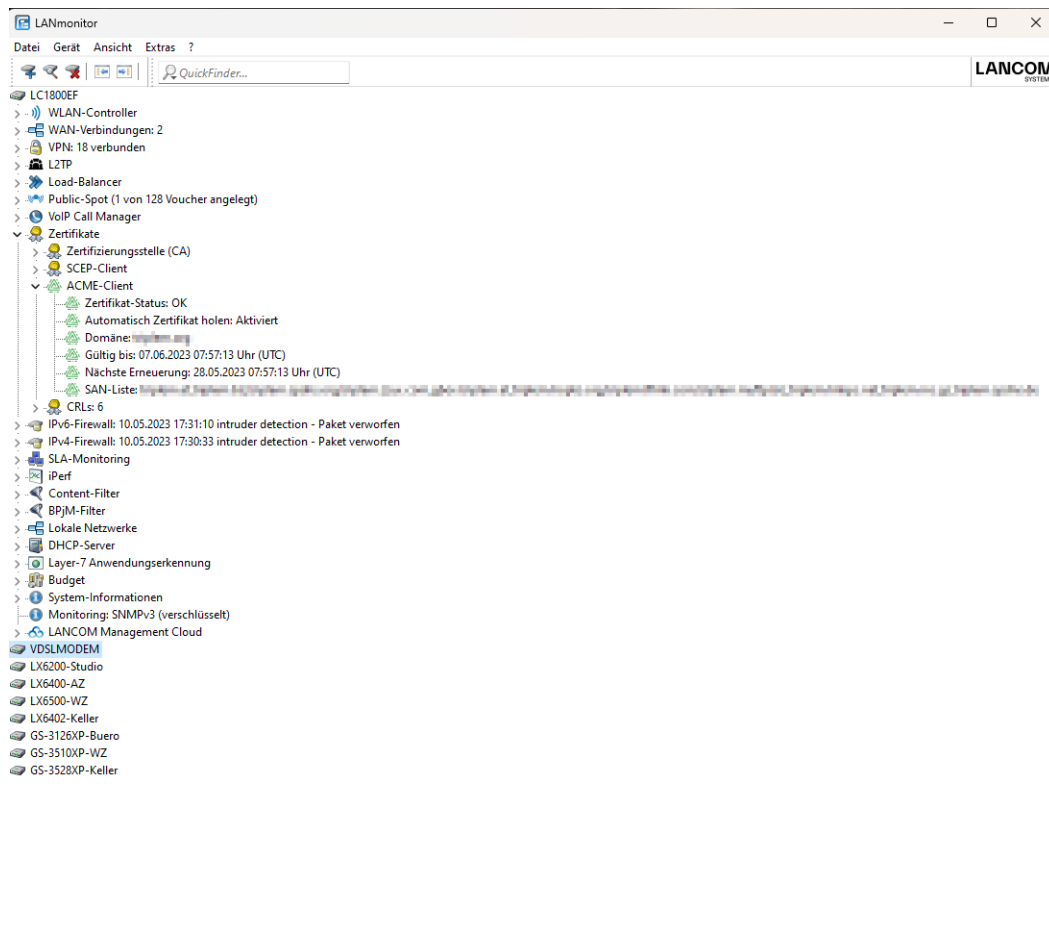
---

 Bitte beachten Sie, dass eine Nutzung des ACME-Clients mit der Authorisierungs-Challenge `tls-alpn-01` sowie ein gleichzeitiges Portforwarding mit Port 443 nicht möglich ist. Das gleiche gilt, falls der ACME-Client über die Methode `http-01` verwendet werden soll für Port 80.

Eine manuelle Anpassung des ACME-Client auf einen beliebigen Port ist laut [RFC 8737](#) im Protokoll nicht möglich.



Informationen zum ACME-Client können Sie im LANmonitor sehen und mit dem Kommandozeilenbefehl `trace # acme` einen Trace starten bzw. auch wieder beenden.



### 10.5.1 ACME-Client konfigurieren

In LANconfig konfigurieren Sie den Automatic Certificate Management Environment (ACME) Client unter **Zertifikate > ACME-Client**.

ACME-Client/Let's Encrypt Client

Mit dem ACME (Automatic Certificate Management Environment) Client können Let's Encrypt Zertifikate automatisch bezogen und regelmäßig erneuert werden.

ACME-Client aktiviert

Domäne:

Kontakt (E-Mail-Adresse):

Zertifikatstyp:

Autorisierungs-Challenge:

Endpoint-Auflösung:

SAN-Liste:

Minimale Zertifikatsgültigkeit:  Tage

Absende-Adresse (optional):

#### ACME-Client aktiviert

Aktiviert bzw. Deaktiviert das automatische Holen und Erneuern des Zertifikats.

**Domäne**

DNS-Domain-Name für die das Zertifikat erstellt werden soll, z. B. „test.example.com“

**Kontakt (E-Mail-Adresse)**

Definiert die Kontaktinformationen für den Zertifikatsantrag, z. B. die E-Mail-Adresse „test@example.com“.

**Zertifikatstyp**

Definiert den Zertifikatstyp inkl. Schlüssellänge.

Mögliche Werte: RSA-2K, RSA-3K, RSA-4K, ECC-256, ECC-384

**Autorisierungs-Challenge**

Definiert über welche Methode die Autorisierungs-Challenge bei Let's Encrypt durchgeführt werden soll.

Mögliche Werte:

- > TLS-alpn-01: Autorisierung wird über TLS und Port 443 durchgeführt
- > http-01: Autorisierung wird über HTTP und Port 80 durchgeführt
- > http-01,tls-alpn-01: Es wird http-01 vor TLS-alpn-01 bevorzugt
- > tls-alpn-01,http-01: Es wird TLS-alpn-01 vor http-01 bevorzugt

**Endpoint-Auflösung**

Definiert unter welchem Protokoll der Endpunkt aufgelöst werden soll. Mögliche Werte:

- > IPv4-Only
- > IPv6-Only
- > IPv6-Or-IPv4

**SAN-Liste**

Definiert welche weiteren Domain-Namen im SAN-Feld (Subject Alternative Name) des Zertifikats eingetragen werden sollen. Möglich ist eine komma-getrennte Liste von Domain-Namen (ohne Leerzeichen).

**Minimale Zertifikatsgültigkeit**

Minimale Anzahl von Tagen bevor das Zertifikat vor Ablauf erneuert wird. Default: 30 Tage

**Absende-Adresse (optional)**

Referenziert eine benannte Loopback-Adresse, die als Absender verwendet wird. Wenn das Feld leer gelassen wird, wählt der Router selbstständig eine Adresse aus.

## 10.5.2 Ergänzungen im Setup-Menü

**ACME-Client**

Diese Tabelle enthält die Einstellungen für den ACME-Client. Der Automatic Certificate Management Environment (ACME) Client nach [RFC 8555](#) wird für Let's Encrypt Zertifikate unterstützt. [Let's Encrypt](#) ist eine freie und offene Zertifizierungsstelle, die es ermöglicht, kostenfreie SSL- / TLS-Zertifikate zu beziehen. Die Zertifikate können für die WEBconfig sowie für den Public Spot verwendet werden.

**SNMP-ID:**

2.39.8

**Pfad Konsole:**

Setup > Zertifikate



**Endpunkt**

Endpunkt bzw. URL unter der der Zertifikatsantrag gestellt werden soll.

**SNMP-ID:**

2.39.8.1

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

max. 100 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

**Default-Wert:**

`https://acme-v02.api.letsencrypt.org/directory`

**Domain**

DNS-Domain-Name für die das Zertifikat erstellt werden soll, z. B. „test.example.com“

**SNMP-ID:**

2.39.8.2

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

max. 100 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

**Default-Wert:**

*leer*

**SAN-Liste**

Definiert welche weiteren Domain-Namen im SAN-Feld (Subject Alternative Name) des Zertifikats eingetragen werden sollen. Möglich ist eine komma-getrennte Liste von Domain-Namen (ohne Leerzeichen).

**SNMP-ID:**

2.39.8.3

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

max. 200 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

**Default-Wert:**

*leer*

**Kontakt**

Definiert die Kontaktinformationen für den Zertifikatsantrag, z. B. die E-Mail-Adresse „test@example.com“.

**SNMP-ID:**

2.39.8.4

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

max. 200 Zeichen aus [A-Z] [a-z] [0-9] #@{|}~!\$%&'()\*+,-./:;<=>?[\]^\_`~

**Default-Wert:**

*leer*

**Endpoint-Auflösung**

Definiert unter welchem Protokoll der Endpoint aufgelöst werden soll.

**SNMP-ID:**

2.39.8.5

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

**nur-IPv4**

**nurIPv6**

**IPv6-oder-IPv4**

**Zertifikats-Typ**

Definiert den Zertifikatstyp inkl. Schlüssellänge.

**SNMP-ID:**

2.39.8.6

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Mögliche Werte:**

RSA-2K  
RSA-3K  
RSA-4K  
ECC-256  
ECC-384

**Default-Wert:**

RSA-2K

**PKCS12-Zieldatei**

Internes Ziel, unter dem das empfangene Zertifikat gespeichert werden soll.

**SNMP-ID:**

2.39.8.7

**Pfad Konsole:**

Setup > Zertifikate > ACME-Client

**Mögliche Werte:**

**ssl\_pkcs12\_int**  
Zertifikatsspeicher für WEBconfig-Zertifikate.

**Default-Wert:**

ssl\_pkcs12\_int

**Autorisierungs-Challenges**

Definiert über welche Methode die Autorisierungs-Challenge bei Let's Encrypt durchgeführt werden soll.

**SNMP-ID:**

2.39.8.8

**Pfad Konsole:**

Setup > Zertifikate > ACME-Client

**Mögliche Werte:**

**http-01**  
Autorisierung wird über HTTP und Port 80 durchgeführt.  
**tls-alpn-01**  
Autorisierung wird über TLS und Port 443 durchgeführt.

**http-01,tls-alpn-01**

Es wird http-01 vor TLS-alpn-01 bevorzugt.

**tls-alpn-01,http-01**

Es wird TLS-alpn-01 vor http-01 bevorzugt.

**Default-Wert:**

tls-alpn-01,http-01

**SSL**

In diesem Menü konfigurieren Sie die Einstellungen für eine SSL/TLS-gesicherte Verbindung zum Let's Encrypt-Server.

**SNMP-ID:**

2.39.8.10

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client**

**Versionen**

Wählen Sie hier die Verschlüsselungsprotokolle für die TLS-Verbindung aus.

**SNMP-ID:**

2.39.8.10.1

**Pfad Konsole:**

**Setup > Zertifikate > ACME-Client > SSL**

**Mögliche Werte:**

SSLv3  
TLSv1  
TLSv1.1  
TLSv1.2  
TLSv1.3

**Default-Wert:**

TLSv1.2

TLSv1.3

**Schlüsselaustausch-Algorithmen**

Wählen Sie hier die Verschlüsselungsverfahren für die SSL/TLS-Verbindung aus.

**SNMP-ID:**

2.39.8.10.2

**Pfad Konsole:**

Setup &gt; Zertifikate &gt; ACME-Client &gt; SSL

**Mögliche Werte:**

RSA  
DHE  
ECDHE

**Default-Wert:**

RSA

DHE

ECDHE

**Krypto-Algorithmen**

Wählen Sie hier die Krypto-Algorithmen für die SSL/TLS-Verbindung aus.

**SNMP-ID:**

2.39.8.10.3

**Pfad Konsole:**

Setup &gt; Zertifikate &gt; ACME-Client &gt; SSL

**Mögliche Werte:**

RC4-40  
RC4-56  
RC4-128  
DES40  
DES  
3DES  
AES-128  
AES-256  
AESGCM-128  
AESGCM-256  
Chacha20-Poly1305

**Default-Wert:**

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Chacha20-Poly1305

### Hash-Algorithmen

Wählen Sie hier die Hash-Algorithmen für die SSL/TLS-Verbindung aus.

#### SNMP-ID:

2.39.8.10.4

#### Pfad Konsole:

Setup > Zertifikate > ACME-Client > SSL

#### Mögliche Werte:

MD5

SHA1

SHA-2-256

SHA2-384

#### Default-Wert:

SHA-2-256

SHA2-384

### PFS-bevorzugen

Bestimmen Sie, ob für die SSL/TLS-gesicherte Verbindung PFS (Perfect Forward Secrecy) aktiviert ist.

#### SNMP-ID:

2.39.8.10.5

#### Pfad Konsole:

Setup > Zertifikate > ACME-Client > SSL

#### Mögliche Werte:

Ja

Nein

#### Default-Wert:

Ja

### Neuverhandlungen

Mit dieser Einstellung steuern Sie, ob der Client eine Neuverhandlung von SSL / TLS auslösen kann.

#### SNMP-ID:

2.39.8.10.6

#### Pfad Konsole:

**Setup > Zertifikate > ACME-Client > SSL**

#### Mögliche Werte:

##### **verboten**

Das Gerät bricht die Verbindung zur Gegenstelle ab, falls diese eine Neuverhandlung anfordert.

##### **erlaubt**

Das Gerät lässt Neuverhandlungen mit der Gegenstelle zu.

##### **ignoriert**

Das Gerät ignoriert die Anforderung der Gegenseite zur Neuverhandlung.

#### Default-Wert:

ignoriert

### Elliptische-Kurven

Legen Sie fest, welche elliptischen Kurven zur Verschlüsselung verwendet werden sollen.

#### SNMP-ID:

2.39.8.10.7

#### Pfad Konsole:

**Setup > Zertifikate > ACME-Client > SSL**

#### Mögliche Werte:

##### **secp256r1**

secp256r1 wird zur Verschlüsselung verwendet.

##### **secp384r1**

secp384r1 wird zur Verschlüsselung verwendet.

##### **secp521r1**

secp521r1 wird zur Verschlüsselung verwendet.

##### **x25519**

x25519 wird zur Verschlüsselung verwendet.

##### **x448**

x448 wird zur Verschlüsselung verwendet.

**Default-Wert:**

secp256r1

secp384r1

secp521r1

x25519

x448

**Signatur-Hash-Algorithmen**

Bestimmen Sie mit diesem Eintrag, mit welchem Hash-Algorithmus die Signatur verschlüsselt werden soll.

**SNMP-ID:**

2.39.8.10.21

**Pfad Konsole:****Setup > Zertifikate > ACME-Client > SSL****Mögliche Werte:****MD5-RSA****SHA1-RSA****SHA224-RSA****SHA256-RSA****SHA384-RSA****SHA512-RSA****MD5-ECDSA****SHA1-ECDSA****SHA224-ECDSA****SHA256-ECDSA****SHA384-ECDSA****SHA512-ECDSA****Default-Wert:**

SHA256-RSA

SHA384-RSA

SHA512-RSA

SHA256-ECDSA

SHA384-ECDSA

SHA512-ECDSA



**Min-DH-Laenge**

Dieser Wert bezieht sich auf das Diffie-Hellman-Agreement, mit dem das Master Secret für den SSL-Tunnel abgeleitet wird, genauer auf den Längenbereich der dafür verwendeten Schlüssel. Sinnvolle Längen sind im Bereich 2048...8192.

**SNMP-ID:**

2.39.8.10.22

**Pfad Konsole:**

Setup > Zertifikate > ACME-Client > SSL

**Mögliche Werte:**

max. 4 Zeichen aus [0-9]

**Default-Wert:**

2048

**Max-DH-Laenge**

Dieser Wert bezieht sich auf das Diffie-Hellman-Agreement, mit dem das Master Secret für den SSL-Tunnel abgeleitet wird, genauer auf den Längenbereich der dafür verwendeten Schlüssel. Sinnvolle Längen sind im Bereich 2048...8192.

**SNMP-ID:**

2.39.8.10.23

**Pfad Konsole:**

Setup > Zertifikate > ACME-Client > SSL

**Mögliche Werte:**

max. 4 Zeichen aus [0-9]

**Default-Wert:**

8192

**Endpoint-Loopback-Adresse**

Geben Sie hier die Loopback-Adresse für den ACME-Client an.

**SNMP-ID:**

2.39.8.11

**Pfad Konsole:**

Setup > Zertifikate > ACME-Client

**Mögliche Werte:**

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

**Default-Wert:***leer***Manuell-Zertifikat-holen**

Mit dieser Aktion lösen Sie ein manuelles Holen des Zertifikats aus.

**SNMP-ID:**

2.39.8.21

**Pfad Konsole:****Setup > Zertifikate > ACME-Client****Automatisch-Zertifikat-holen**

Einstellungen zum automatischen Holen und Erneuern des Zertifikats.

**SNMP-ID:**

2.39.8.22

**Pfad Konsole:****Setup > Zertifikate > ACME-Client****In-Betrieb**

Aktiviert bzw. Deaktiviert das automatische Holen und Erneuern des Zertifikats.

**SNMP-ID:**

2.39.8.22.1

**Pfad Konsole:****Setup > Zertifikate > ACME-Client > Automatisch-Zertifikat-holen****Mögliche Werte:****ja  
nein****Default-Wert:**

nein

**Minimal-Gueltigkeit-Tage**

Minimale Anzahl von Tagen bevor das Zertifikat vor Ablauf erneuert wird.

**SNMP-ID:**

2.39.8.22.2

**Pfad Konsole:**

Setup &gt; Zertifikate &gt; ACME-Client &gt; Automatisch-Zertifikat-holen

**Mögliche Werte:**

max. 5 Zeichen aus [0-9]

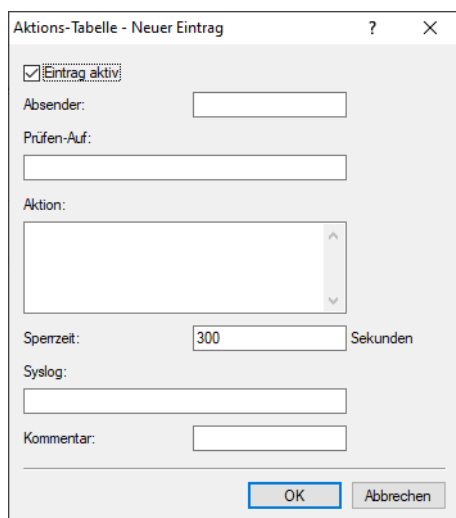
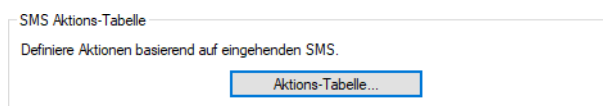
**Default-Wert:**

30

## 10.6 Aktionen auf eingehende SMS ausführen

Ab LCOS 10.80 können Sie bei Routern mit WWAN-Modul auf eingehende SMS mit vordefinierten Aktionen reagieren. Dadurch können Sie bei einer eingehenden SMS (z. B. Datenguthaben aufgebraucht) selber mit einer SMS an den Internetprovider reagieren und darüber neues Datenguthaben hinzubuchen.

In LANconfig konfigurieren Sie dies unter **Meldungen/Monitoring > SMS-Nachrichten > SMS Aktions-Tabelle > Aktions-Tabelle**.

**Eintrag aktiv**

Aktiviert oder Deaktiviert den Tabelleneintrag.

**Absender**

Absendeadresse der eingehenden SMS, auf deren Basis die folgende Aktion ausgeführt werden soll. Z. B. 7277 für die Deutsche Telekom.

**Prüfen-Auf**

Inhalt der eingehenden SMS, auf den geprüft werden soll. Z. B. contains=' aufgebraucht' im Falle eines aufgebrauchten Datenguthabens. Der Text, auf den geprüft wird, ist case-sensitiv!

**Aktion**

Definiert die Aktion, die nach Prüfung der Vorgaben unter **Absender** und **Prüfen-Auf** ausgeführt werden soll. Z. B. `exec:smssend -d 7277 -t "Speed"` zum Buchen eines SpeedOn im Netz der Deutschen Telekom. Mit `exec` wird ein Befehl auf der Konsole ausgeführt, in diesem Fall das Kommando `smssend`.

**Sperrzeit**

Definiert die Sperrzeit in Sekunden, in welcher die Aktion nicht erneut ausgeführt werden darf.

**Syslog**

Freies Textfeld zur Definition der Meldung, die bei Ausführung dieser Aktion in das Syslog geschrieben werden soll.

**Kommentar**

Freies Kommentarfeld.

## 10.6.1 Ergänzungen im Setup-Menü

**Aktions-Tabelle**

Über diese Tabelle können Sie auf eingehende SMS mit vordefinierten Aktionen reagieren. Dadurch können Sie im Falle einer eingehenden SMS (z. B. Datenguthaben aufgebraucht) selber mit einer SMS an den Internetprovider reagieren und darüber neues Datenguthaben hinzubuchen.

**SNMP-ID:**

2.83.11

**Pfad Konsole:**

**Setup > SMS**

**Idx.**

Index zu diesem Eintrag in der Liste.

**SNMP-ID:**

2.83.11.1

**Pfad Konsole:**

**Setup > SMS > Aktions-Tabelle**

**Mögliche Werte:**

max. 6 Zeichen aus `0123456789`

**Default-Wert:**

*leer*

**Aktiv**

Aktiviert oder Deaktiviert den Tabelleneintrag.

**SNMP-ID:**

2.83.11.2

**Pfad Konsole:**

Setup > SMS > Aktions-Tabelle

**Mögliche Werte:****Nein**

Deaktiviert den Tabelleneintrag.

**Ja**

Aktiviert den Tabelleneintrag.

**Default-Wert:**

Ja

**Sender**

Absendeadresse der eingehenden SMS, auf deren Basis die folgende Aktion ausgeführt werden soll. Z. B. 7277 für die Deutsche Telekom.

**SNMP-ID:**

2.83.11.4

**Pfad Konsole:**

Setup > SMS > Aktions-Tabelle

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

**Pruefen-Auf**

Inhalt der eingehenden SMS, auf den geprüft werden soll. Z. B. `contains='aufgebraucht'` im Falle eines aufgebrauchten Datenguthabens. Der Text, auf den geprüft wird, ist case-sensitiv!

**SNMP-ID:**

2.83.11.5

**Pfad Konsole:**

Setup > SMS > Aktions-Tabelle

**Mögliche Werte:**

max. 50 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~`

**Default-Wert:**

*leer*

**Aktion**

Definiert die Aktion, die nach Prüfung der Vorgaben unter [2.83.11.4 Sender](#) auf Seite 69 und [2.83.11.5 Prüfen-Auf](#) auf Seite 69 ausgeführt werden soll. Z. B. `exec:smssend -d 7277 -t "Speed"` zum Buchen eines SpeedOn im Netz der Deutschen Telekom. Mit `exec` wird ein Befehl auf der Konsole ausgeführt, in diesem Fall das Kommando `smssend`.

**SNMP-ID:**

2.83.11.6

**Pfad Konsole:**

**Setup > SMS > Aktions-Tabelle**

**Mögliche Werte:**

max. 250 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+,-./:;<=>?[\]^_`~`

**Default-Wert:**

*leer*

**Sperrzeit**

Definiert die Sperrzeit in Sekunden, in welcher die Aktion nicht erneut ausgeführt werden darf.

**SNMP-ID:**

2.83.11.7

**Pfad Konsole:**

**Setup > SMS > Aktions-Tabelle**

**Mögliche Werte:**

max. 9 Zeichen aus `0123456789`

**Default-Wert:**

300

**Syslog**

Freies Textfeld zur Definition der Meldung, die bei Ausführung dieser Aktion in das Syslog geschrieben werden soll.

**SNMP-ID:**

2.83.11.8

**Pfad Konsole:****Setup > SMS > Aktions-Tabelle****Mögliche Werte:**max. 50 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-/,/:;<=>?[\]^_`~``**Default-Wert:***leer***Kommentar**

Freies Kommentarfeld.

**SNMP-ID:**

2.83.11.10

**Pfad Konsole:****Setup > SMS > Aktions-Tabelle****Mögliche Werte:**max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()+-/,/:;<=>?[\]^_`~``**Default-Wert:***leer*

# 11 Ergänzungen im Menüsystem

## 11.1 Ergänzungen im Setup-Menü

### 11.1.1 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.2.22.28

**Pfad Konsole:**

Setup > WAN > RADIUS

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.2 L2TP-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.2.22.29

**Pfad Konsole:**

Setup > WAN > RADIUS

**Mögliche Werte:**

**nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.



**Default-Wert:**

nein

### 11.1.3 LB-Policy

Definiert ab LCOS 10.80 RU5 die Dynamic Path Selection Policy, die für diese Firewall Regel verwendet wird. Dies kann entweder eine der vordefinierten aus [2.8.20.4 Vordefinierte-Selektoren](#) auf Seite 73 oder eine der selbst erzeugten unter [2.110.4.16 Richtlinien](#) sein.

Die hier genannte Policy wird als Rückfall-Policy genutzt, falls in der Firewall bzw. dem Kommandozeilen-Ping keine Policy oder die Policy DEFAULT (siehe [2.8.20.4 Vordefinierte-Selektoren](#) auf Seite 73) einträgt und gilt für Sessions, die über diesen Loadbalancer senden.

**SNMP-ID:**

2.8.20.2.13

**Pfad Konsole:****Setup > IP-Router > Load-Balancer > Buendel-Gegenstellen****Mögliche Werte:**max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+,/:;<=>?[\]^_.`**Default-Wert:**

leer

### 11.1.4 Vordefinierte-Selektoren

Hier finden Sie einige durch LCOS vordefinierte Load-Balancer-Policies, die unter [2.8.10.2.16 LB-Policy](#) bzw. [2.70.5.2.12 LB-Policy](#) auf Seite 81 verwendet werden können.

Ab LCOS 10.80 RU5 sind die Policies DEFAULT und MOST-USED hinzugefügt worden.

**SNMP-ID:**

2.8.20.4

**Pfad Konsole:****Setup > IP-Router > Load-Balancer****Mögliche Werte:****DEFAULT**

Diese Loadbalancer-Policy hat immer denselben Effekt, wie wenn man keine Policy angibt bzw. die LB-Policy-Spalte leer lässt. In der Firewall und im Kommandozeilen-Ping löst sie einen Rückfall auf die Policy aus der Tabelle [2.8.20.2.13 LB-Policy](#) auf Seite 73 aus. In der Tabelle [2.8.20.2.13 LB-Policy](#) auf Seite 73 löst sie einen Rückfall auf den TRAFFIC-Selektor aus.

**TRAFFIC  
BANDWIDTH  
ROUND-ROBIN  
MOST-USED**

Mit dieser Policy wählt der Loadbalancer denjenigen Kanal, auf dem gerade die meisten Firewall-Sessions (ungeachtet, ob in Sende- oder Empfangsrichtung und ungeachtet, ob IPv4 oder IPv6) liegen. Diese Policy ist nur als Gegenstück zu Dynamic Path Selection sinnvoll, d. h. wenn etwa ein Filialgerät auf dem Loadbalancer Dynamic Path Selection nutzt, dann sollte die Zentrale auf ihrem zugehörigen Loadbalancer MOST-USED nutzen. Das führt effektiv dazu, dass sich die Zentrale an die Dynamic Path Selection-Entscheidungen der Filiale anpasst, ohne dass die Filiale ihre Entscheidung der Zentrale explizit mitteilen müsste.

### 11.1.5 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.11.81.1.10

**Pfad Konsole:****Setup > Config > RADIUS > Server****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.6 Konfigurationshochladepruefung

Definiert, ob das Gerät unbekannte OIDs in hochgeladenen Konfigurationen verarbeiten soll. Dieser Schalter dient hauptsächlich Validierungen und Kompatibilitätsprüfungen. Im Default werden unbekannt OIDs ignoriert und die Konfiguration wird akzeptiert.

**SNMP-ID:**

2.11.97

**Pfad Konsole:****Setup > Config**

**Mögliche Werte:****tolerant**

Unbekannte OIDs werden akzeptiert.

**streng**

Unbekannte OIDs produzieren einen Fehler so dass der Konfigurations-Upload fehlschlägt.

**Default-Wert:**

tolerant

### 11.1.7 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.21

**Pfad Konsole:**

Setup > WLAN > RADIUS-Zugriffspruefung

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.8 Backup-Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.12.29.22

**Pfad Konsole:**

Setup > WLAN > RADIUS-Zugriffspruefung

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.9 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.19.36.9.1.1.11

**Pfad Konsole:****Setup > VPN > IKEv2 > RADIUS > Autorisierung > Server****Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.10 Roaming-PDP-Typ

Definiert mit welchem PDP-Typ (IPv4, IPv6 oder IPv4 und IPv6) die Mobilfunkverbindung im Roaming-Fall aufgebaut werden soll.

**SNMP-ID:**

2.23.41.1.16

**Pfad Konsole:****Setup > Schnittstellen > Mobilfunk > Profile**

**Mögliche Werte:**

IPv4  
IPv6  
IPv4v6

**Default-Wert:**

IPv4

### 11.1.11 Datenroaming

Aktiviert bzw. Deaktiviert die Datenverbindung, falls das Gerät in einem fremden Mobilfunknetz eingebucht ist (Roaming).

**SNMP-ID:**

2.23.41.1.17

**Pfad Konsole:**

Setup > Schnittstellen > Mobilfunk > Profile

**Mögliche Werte:**

Ja  
Nein

**Default-Wert:**

Ja

### 11.1.12 Syslog

Dieses Menü enthält Einträge, die ggf. Syslog-Meldungen auslösen.

**SNMP-ID:**

2.23.41.14

**Pfad Konsole:**

Setup > Schnittstellen > Mobilfunk

#### Syslog-Signal-Hysterese

Definiert bei wie viel dB Unterschied bei Schwankungen im Signallevel (vorheriger Wert zu aktueller Wert) eine Syslog-Meldung generiert werden soll.

**SNMP-ID:**

2.23.41.14.1

**Pfad Konsole:**

**Setup > Schnittstellen > Mobilfunk > Syslog**

**Mögliche Werte:**

max. 4 Zeichen aus [0-9]

**Default-Wert:**

5

### 11.1.13 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.2.6

**Pfad Konsole:**

**Setup > RADIUS > Server > Clients**

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**

Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

**Default-Wert:**

nein

### 11.1.14 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.3.18

**Pfad Konsole:**

**Setup > RADIUS > Server > Weiterleit-Server**

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Default-Wert:**

nein

### 11.1.15 Msg-Authenticator-erforderlich

Neuer Schalter ab LCOS 10.80 RU5. Definiert, ob das Vorhandensein des Message-Authenticator-Attributs in RADIUS-Nachrichten auf Client-Seite erzwingt. Die Client-Seite ist die Seite, die den RADIUS-Accept/Fail empfängt.

**SNMP-ID:**

2.25.10.16.6

**Pfad Konsole:**

Setup > RADIUS > Server > IPv6-Clients

**Mögliche Werte:****nein**

Access-Requests müssen keinen Message-Authenticator enthalten.

**ja**

Access-Requests müssen immer einen Message-Authenticator enthalten.

**Nur-Proxy**

Falls ein Access-Request ein Proxy-State-Attribut enthält, muss ein Message-Authenticator enthalten sein.

**Default-Wert:**

nein

### 11.1.16 Blockierte-Gegenstellen

Der TR069-Server kann meist nicht über jede Internet-Verbindung erreicht werden (z. B. Backup-Verbindungen). Auch kann eine Kommunikation mit dem Server nicht sinnvoll sein, wenn z. B. der Client vom Server über diesen Kommunikationsweg nicht identifiziert werden kann.

Daher können hier ab LCOS 10.80 RU5, Komma-separiert, Gegenstellen eintragen werden, über die kein Kontakt mit dem TR069-Server hergestellt werden darf.

**SNMP-ID:**

2.44.28

**Pfad Konsole:****Setup > CWMP****Mögliche Werte:**

max. 256 Zeichen aus [A-Z] [0-9] @ { | } ~ ! \$ % &amp; ' ( ) + - , / : ; &lt; = &gt; ? [ \ ] ^ \_ .

**Default-Wert:***leer*

### 11.1.17 LCOSCap-WAN-Zugriff

Mit dieser Einstellung regeln Sie den Zugriff auf LCOSCAP aus dem WAN.

**SNMP-ID:**

2.63.5

**Pfad Konsole:****Setup > Paket-Capture****Mögliche Werte:****nein**

Kein Zugriff erlaubt. Dies ist die Voreinstellung bei Neugeräten oder wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird.

**ja**

Zugriff erlaubt. Dies ist die Voreinstellung bei Geräten, welche auf die Version LCOS 10.80 von einer älteren Version aktualisiert wurden.

**nur-VPN**

Zugriff nur über VPN-Verbindungen erlaubt.

**Default-Wert:**

nein

### 11.1.18 RPCap-WAN-Zugriff

Mit dieser Einstellung regeln Sie den Zugriff auf RPCAP aus dem WAN.

**SNMP-ID:**

2.63.14

**Pfad Konsole:****Setup > Paket-Capture**



**Mögliche Werte:****nein**

Kein Zugriff erlaubt. Dies ist die Voreinstellung bei Neugeräten oder wenn das Gerät auf die Werkseinstellungen zurückgesetzt wird.

**ja**

Zugriff erlaubt. Dies ist die Voreinstellung bei Geräten, welche auf die Version LCOS 10.80 von einer älteren Version aktualisiert wurden.

**nur-VPN**

Zugriff nur über VPN-Verbindungen erlaubt.

**Default-Wert:**

nein

## 11.1.19 LB-Policy

Definiert ab LCOS 10.80 RU5 die Dynamic Path Selection Policy, die für diese Firewall Regel verwendet wird. Dies kann entweder eine der vordefinierten aus [2.8.20.4 Vordefinierte-Selektoren](#) auf Seite 73 oder eine der selbst erzeugten unter [2.110.4.16 Richtlinien](#) sein.

**SNMP-ID:**

2.70.5.2.12

**Pfad Konsole:**

**Setup > IPv6 > Firewall > Forwarding-Regeln**

**Mögliche Werte:**

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

**Default-Wert:**

*leer*

## 11.1.20 Aktiv

Aktiviert bzw. deaktiviert das Senden und Empfangen von SMS auf dem Gerät.

**SNMP-ID:**

2.83.10

**Pfad Konsole:**

**Setup > SMS**

**Mögliche Werte:****Nein**

Senden und Empfangen von SMS deaktiviert.

11 Ergänzungen im Menüsystem

**Ja**

Senden und Empfangen von SMS aktiviert.

**Default-Wert:**

Ja