LANCOM SD-WAN Gateways

Sicherheitsrelevante Einstellungen

06/2025

LANCOM SYSTEMS

Inhalt

1 LCOS-Version und -Syntaxbeschreibung

Dieses Dokument beschreibt die sicherheitsrelevanten Einstellungen LCOS-basierter SD-WAN Gateways. Es dient als Nachschlagewerk für die Geräte-Administration und den sicheren Betrieb von LANCOM SD-WAN Gateways.

Die beschriebenen Einstellungen gelten für Geräte mit mindestens LCOS-Version 10.90. Um insbesondere im Bereich der zentralen Administratorenverwaltung eine umfassende Absicherung zu gewährleisten, sind die Funktionen dieser LCOS-Version erforderlich.

Für alle aufgeführten Konfigurationsparameter werden der zugehörige Kommandozeilenpfad, die erforderlichen Befehle zur Parametereinstellung sowie eine Übersicht der möglichen Werte dargestellt.

Beispielhaft angeführte Skripte sind in der Regel auf die zum Verständnis relevanten Spalten reduziert.

2 Management

2.1 Passwortqualität

Die Sicherheit des Passwortschutzes hängt maßgeblich von der Komplexität und Zufälligkeit des gewählten Passworts ab. LCOS erlaubt Passwörter für lokale Administratoren-Accounts mit einer Länge von bis zu 128 Zeichen.

Das Passwort sollte zufällig generiert sein und mindestens acht Zeichen umfassen. Dabei sollten mindestens drei der folgenden vier Zeichenklassen enthalten sein: Kleinbuchstaben, Großbuchstaben, Ziffern und Sonderzeichen.

CLI-Einstellung für Root-Passwort

```
passwd                  change password
passwd -n new [old]     change password (no prompt)
```

2.2 Brute-Force-Schutz

Der Passwortschutz bei lokaler Authentifizierung wird durch einen Brute-Force-Schutz zusätzlich verstärkt. Wiederholt fehlerhafte Passworteingaben führen zu einer Sperrung des Zugriffs für eine definierbare Dauer.

Pfad

```
/Setup/Config
/Setup/Voice-Call-Manager/General
```

Kommando

```
set /Setup/Config/Login-Errors 5
set /Setup/Config/Lock-Minutes 5
set /Setup/Voice-Call-Manager/General/Login-Errors 5
set /Setup/Voice-Call-Manager/General/Lock-Minutes 5
```

Mögliche Einträge

```
Login-Errors            : 2 chars from: 1234567890
Lock-Minutes            : 2 chars from: 1234567890
```

2.3 SSH-Parameter

Im folgenden Menü werden die sicherheitsrelevanten Parameter für die Verwendung von SSH konfiguriert.

Pfad

```
/Setup/Config/SSH
```

Kommando

```
set cipher-algorithms aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305,
    aes128-gcm,aes256-gcm
set DH-Groups Group-14,Group-15,Group-16,Group-17,Group-18
set Elliptic-Curves nistp256,nistp384,nistp521
set Signing-Hostkey-Algorithms ssh-ed25519,ssh-ed448,ecdsa-sha2,rsa-sha2-256,rsa-sha2-512
```

```
set Key-Exchange-Algorithms diffie-hellman-group-exchange-sha256,ecdh-sha2,curve25519-sha256,curve448-sha512,
    sntrup761x25519-sha512,diffie-hellman-group14-sha256,diffie-hellman-group15-sha512,
    diffie-hellman-group16-sha512
set MAC-Algorithms hmac-sha2-256,hmac-sha2-512,hmac-sha2-256-etm,hmac-sha2-512-etm
set Max-Hostkey-Length 8192
set Min-Hostkey-Length 2048
```

Mögliche Einträge

```
[  1] Cipher-Algorithms             : Bitmask: 3des-cbc (1), 3des-ctr (2), arcfour (4), arcfour128 (8),
                                               arcfour256 (16), blowfish-cbc (32), blowfish-ctr (64),
                                               aes128-cbc (128), aes192-cbc (256), aes256-cbc (512),
                                               aes128-ctr (1024), aes192-ctr (2048), aes256-ctr (4096),
                                               chacha20-poly1305 (8192), aes128-gcm (16384),
                                               aes256-gcm (32768)
[  2] MAC-Algorithms                : Bitmask: hmac-md5-96 (1), hmac-md5 (2), hmac-sha1-96 (4), hmac-sha1 (8),

                                               hmac-sha2-256-96 (16), hmac-sha2-256 (32),
                                               hmac-sha2-512-96 (64), hmac-sha2-512 (128),
                                               hmac-md5-96-etm (256), hmac-md5-etm (512),
                                               hmac-sha1-96-etm (1024), hmac-sha1-etm (2048),
                                               hmac-sha2-256-96-etm (4096), hmac-sha2-256-etm (8192),
                                               hmac-sha2-512-96-etm (16384), hmac-sha2-512-etm (32768)
[  3] Key-Exchange-Algorithms       : Bitmask: diffie-hellman-group1-sha1 (1),
                                               diffie-hellman-group14-sha1 (2),
                                               diffie-hellman-group-exchange-sha1 (4),
                                               diffie-hellman-group-exchange-sha256 (8), ecdh-sha2 (16),
                                               curve25519-sha256 (32), curve448-sha512 (64),
                                               sntrup761x25519-sha512 (128),
                                               diffie-hellman-group14-sha256 (256),
                                               diffie-hellman-group15-sha512 (2048),
                                               diffie-hellman-group16-sha512 (512),
                                               diffie-hellman-group17-sha512 (4096),
                                               diffie-hellman-group18-sha512 (8192),
                                               sntrup4591761x25519-sha512 (1024)
[  7] DH-Groups                     : Bitmask: Group-1 (1), Group-5 (2), Group-14 (4), Group-15 (8),
                                               Group-16 (16), Group-17 (32), Group-18 (64)
[  8] Compression                   : No (0), Yes (1)
[  9] Elliptic-Curves               : Bitmask: nistp256 (1), nistp384 (2), nistp521 (4)
[ 10] SFTP-Server                   : try 'set SFTP-Server ?'
[ 11] Keepalive-Interval            : 5 chars from 1234567890
[ 12] Operating                     : Bitmask: No (0), Yes (1)
[ 13] Port                          : 5 chars from 1234567890
[ 14] Authentication-Methods        : try 'set Authentication-Methods ?'
[ 15] Signing-Hostkey-Algorithms    : Bitmask: ssh-ed25519 (8), ssh-ed448 (64), ecdsa-sha2 (4), ssh-rsa (1),
                                               rsa-sha2-256 (16), rsa-sha2-512 (32), ssh-dss (2)
[ 16] Verifyable-Hostkey-Algorithms : Bitmask: ssh-ed25519 (8), ssh-ed448 (64), ecdsa-sha2 (4), ssh-rsa (1),
                                               rsa-sha2-256 (16), rsa-sha2-512 (32), ssh-dss (2)
[ 17] Min-RSA-Hostkey-Length        : 5 chars from 1234567890
[ 18] Max-RSA-Hostkey-Length        : 5 chars from 1234567890
[ 19] Nonauth-Disconnect-Time       : 5 chars from 1234567890
[ 20] Max-Auth-Tries                : 5 chars from 1234567890
```

2.3.1 SSH-Schlüsselerzeugung unter LCOS

Zur Erzeugung eines individuellen Schlüsselpaares – bestehend aus einem öffentlichen und einem privaten Schlüssel – gehen Sie wie folgt vor:

Kommando

```
sshkeygen [-q] [-t dsa|rsa|ecdsa|ed25519|ed448] [-b bits] [-f output-file]
```

Mögliche Parameter

```
[-t dsa|rsa|ecdsa|ed25519|ed448]
```

Dieser Parameter bestimmt den Typ des zu erzeugenden Schlüssels. Insgesamt unterstützt SSH folgende Schlüsseltypen:

- **RSA**-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis 16.384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 3.072 Bit.
- **DSA**-Schlüssel folgen dem Digital Signature Standard (DSS) des National Institute of Standards and Technology (NIST) und werden z. B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. Sie haben stets eine Länge von 1.024 Bit, sind jedoch langsamer als vergleichbare RSA-Schlüssel.

- **ECDSA**-Schlüssel sind eine Variante der DSA-Schlüssel, bei der elliptische Kurven (Elliptic Curve Cryptography, ECC) zur Schlüsselerzeugung verwendet werden. ECC ist eine Alternative zu klassischen Signatur- und Schlüsselaustauschverfahren wie RSA oder Diffie-Hellman. Der Hauptvorteil elliptischer Kurven liegt in der Möglichkeit, mit kürzeren Schlüsseln die gleiche Sicherheit zu erreichen. Weitere Informationen finden Sie in *RFC 5656* und *RFC 4492*.
- **Ed25519** ist ein Verfahren auf Basis des Edwards-curve Digital Signature Algorithm (EdDSA), beschrieben in *RFC 8709*.
- **Ed448** ist ein weiteres EdDSA-Verfahren, das ebenfalls auf elliptischen Kurven basiert und in *RFC 8709* spezifiziert ist.

Wenn Sie keinen Typ angeben, wird standardmäßig ein RSA-Schlüssel erzeugt.

```
-b <Bits>
```

Dieser Parameter legt die Schlüssellänge in Bit für RSA-Schlüssel fest. Wird keine Länge angegeben, erzeugt das Kommando einen 1.024-Bit-Schlüssel.

```
-f <OutputFile>
```

Mit diesem Parameter legen Sie den Dateinamen der erzeugten Schlüsseldatei im Dateisystem des Geräts fest. Der Dateiname hängt vom gewünschten Schlüsseltyp ab. Zur Auswahl stehen:

- `ssh_rsakey` für RSA-Schlüssel
- `ssh_dsakey` für DSA-Schlüssel
- `ssh_ecdsakey` für ECDSA-Schlüssel
- `ssl_privkey` für SSL-RSA-Schlüssel
- `ssh_ed25519key` für Ed25519-Schlüssel
- `ssh_ed448key` für Ed448-Schlüssel

```
-q
```

Dieser Parameter aktiviert den „Quiet"-Modus bei der Schlüsselerzeugung. Bereits vorhandene RSA- oder DSA-Schlüssel werden ohne Rückfrage überschrieben und es erfolgt keine Fortschrittsanzeige. Verwenden Sie diesen Parameter z. B. in Skripten, um interaktive Rückfragen zu vermeiden.

2.4 Zentrale Authentisierung

In Installationen mit mehreren zuständigen Administratoren sollte die lokale Verwaltung von Administrator-Accounts nach Möglichkeit vermieden werden.

Bei aktivierter zentraler Authentisierung stehen keine zusätzlichen lokalen Accounts zur Verfügung!

Zur Sicherstellung eines funktionalen Desaster-Recovery kann optional ein Fallback auf den lokalen Root-Account konfiguriert werden. In diesem Fall ist besonders auf die Qualität und Sicherheit des Root-Passworts zu achten.

Pfad

```
/Setup/TACACS+
/Setup/TACACS+/Server
/Setup/Config/Authentication
```

Kommando

```
set /Setup/Config/Authentication
set /Setup/TACACS+/Shared-Secret "***"
set /Setup/TACACS+/Encryption activated
set /Setup/TACACS+/Connection-Timeout 5
set /Setup/TACACS+/Fallback-to-local-users allowed
```

Mögliche Einträge

```
Authentication           : Intern (0), Radius (1), Tacacs+ (2)
Authorisation            : deactivated (0), activated (1)
Shared-Secret            : 31 chars from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                          bcdefghijklmnopqrstuvwxyz `
Encryption               : deactivated (0), activated (1)
Fallback-to-local-users  : allowed (0), prohibited (1)
```

Kommando

```
cd /Setup/Tacacs+/Server
tab Server-Address Loopback-Address Compatibility-Mode
add "10.2.3.4"     "INTRANET"       deactivated
cd /
```

Mögliche Einträge

```
[1] Server-Address       : 31 chars from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
[2] Loopback-Address     : 16 chars from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789-
[3] Compatibility-Mode   : deactivated (0), activated (1)
```

2.5 Optionale Ausnahmen von TACACS+ Autorisierung und Accounting

LCOS bietet eine Option, mit der sich Befehle, die über die Cron-Tabelle (`/Setup/Config/Cron-Table`), die Aktionstabelle (`/Setup/WAN/Action-Table`) oder den Befehl `beginscript` ausgeführt werden, von den TACACS+-Funktionen Autorisierung und Accounting ausnehmen lassen.

Bei aktivierter TACACS+-Integration ist der Zugriff auf diese Option sowie – bei gesetztem Schaltzustand `deactivated (0)` – der Zugriff auf die Cron-Tabelle, die Aktionstabelle und den Befehl `beginscript` besonders restriktiv zu handhaben. Andernfalls könnten Administratoren ungewollte Umgehungsmöglichkeiten zur Konfigurationsänderung erhalten.

Es wird empfohlen, den Zugriff auf diesen Mechanismus ausschließlich auf Administratoren oder automatisierte Prozesse zu beschränken, die bereits über Root-Rechte verfügen.

Pfad

```
/Setup/TACACS+
```

Kommando

```
set /Setup/TACACS+/ Bypass-Tacacs-for-CRON/scripts/action-table activated
```

Mögliche Einträge

```
Bypass-Tacacs-for-CRON/scripts/action-table: deactivated (0),activated (1)
```

2.6 SNMP-Get-Requests von TACACS+ Autorisierung und Accounting ausnehmen

Die TACACS+-Funktionen Autorisierung und Accounting für SNMP-GET-REQUESTs können in SNMP-überwachten Netzwerken zur Entlastung der TACACS+-Server entweder auf den Setup-Pfad beschränkt oder vollständig deaktiviert werden.

Der Status-Pfad enthält keine benutzerspezifischen Informationen. Dennoch sollte im Projektkontext eine Bewertung der Unbedenklichkeit dieser Statusdaten erfolgen.

Eine vollständige Deaktivierung der Überwachungsfunktionen für SNMP-GET-REQUESTs wird nicht empfohlen.

Um ungewollte Zugriffe per SNMP zu verhindern, sollte der Zugriff auf diese Einstellung streng kontrolliert und ausschließlich Administratoren mit Root-Rechten vorbehalten sein.

Pfad

```
/Setup/TACACS+
```

Kommando

```
set /Setup/Tacacs+/ SNMP-GET-Requests-Authorisation only_for_SETUP_tree
set /Setup/Tacacs+/ SNMP-GET-Requests-Accounting only_for_SETUP_tree
```

Mögliche Einträge

```
SNMP-GET-Requests-Authorisation: only_for_SETUP_tree (0), all (1), none (2)
SNMP-GET-Requests-Accounting: only_for_SETUP_tree (0), all (1), none (2)
```

2.7 SNMPv3

Mit der Version 3 wurde die Protokollstruktur von SNMP grundlegend überarbeitet. SNMPv3 ist in mehrere Module mit klar definierten Schnittstellen unterteilt, die miteinander interagieren.

Die drei zentralen Komponenten von SNMPv3 sind:

- „Message Processing and Dispatch (MPD)" – zuständig für die Verarbeitung und Weiterleitung von SNMP-Nachrichten.
- „User-based Security Model (USM)" – definiert Authentifizierung und Verschlüsselung auf Benutzerbasis.
- „View-based Access Control Mechanism (VACM)" – regelt den Zugriff auf MIB-Objekte anhand vordefinierter Sichten (Views).

2.7.1 Erlaube Admins

Standardmäßig ist diese Option aktiviert, sodass registrierte Administratoren Zugriff über SNMPv3 erhalten.

Pfad

```
/Setup/SNMP
```

Kommando

```
set /Setup/SNMP/Allow-Admins YES
```

2.7.2 Zugelassene Protokolle

Aktivieren Sie hier die SNMP-Versionen, die das Gerät für SNMP-Anfragen und SNMP-Traps unterstützen soll.

Es wird empfohlen, ausschließlich SNMPv3 zu verwenden (Standardeinstellung).

Pfad

```
/Setup/SNMP
```

Kommando

```
set /Setup/SNMP/Admitted-Protocols SNMPv3
```

2.7.3 SNMPv3-Admin-Authentifizierung

Dieser Parameter definiert die Authentifizierungsmethode für Administratoren bei SNMPv3.

Die Methode ist fest auf **HMAC-SHA256** eingestellt und kann nicht geändert werden.

2.7.4 SNMPv3-Admin-Verschlüsselung

Dieser Parameter definiert die Verschlüsselungseinstellungen für Administratoren bei SNMPv3.

Die Verschlüsselung ist fest auf **AES256** eingestellt und kann nicht geändert werden.

2.7.5 Benutzer

Wenn einzelnen Benutzern – abweichend von den Administratoren – SNMPv3-Zugriff gewährt werden soll, können diese zusätzlich angelegt werden. Für jeden Benutzer lassen sich Authentifizierungs- und Verschlüsselungsmethode individuell konfigurieren.

Pfad

```
/Setup/SNMP/Users
```

Kommando

```
cd /Setup/SNMP/Users
tab User-Name Authentication-Protocol Authentication-Password Privacy-Protocol Privacy-Password Status
set "User1" "HMAC-SHA256" "9kuufgz76zzh56hft54gjf7" "AES256" "9kuufgz76zzh56hft54gjf7" "active"
```

Mögliche Einträge

```
[ 2] User-Name               : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                              9abcdefghijklmnopqrstuvwxyz`
[ 5] Authentication-Protocol : None (1), HMAC-MD5 (2), HMAC-SHA (3), HMAC-SHA224 (4), HMAC-SHA256 (5),
                                HMAC-SHA384 (6), HMAC-SHA512 (7)
[ 6] Authentication-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                              6789abcdefghijklmnopqrstuvwxyz `
[14] Authentication-Key      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                              6789abcdefghijklmnopqrstuvwxyz `
[ 8] Privacy-Protocol        : None (1), DES (2), AES128 (4), AES192 (20), AES256 (21)
[ 9] Privacy-Password        : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                              6789abcdefghijklmnopqrstuvwxyz `
[15] Privacy-Key             : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345
                                              6789abcdefghijklmnopqrstuvwxyz `
[13] Status                  : active (1), inactive (2)
```

2.7.6 Gruppen

In der Gruppenkonfiguration lassen sich ReadOnly- und ReadWrite-Communities für SNMPv3 definieren.

Pfad

```
/Setup/SNMP/Groups
```

Kommando

```
cd /Setup/SNMP/Groups
tab Security.Model Security-Name Group-Name Status
set "SNMPv3(USM)" "User1" "SNMPv3-ReadOnly" "active"
```

Mögliche Einträge

```
[1] Security-Model       : SNMPv1 (1), SNMPv2 (2), SNMPv3(USM) (3)
[2] Security-Name        : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcde
                                         fghijklmnopqrstuvwxyz`
[3] Group-Name           : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcd
```

```
                                        efghijklmnopqrstuvwxyz`
[5] Status               : active (1), inactive (2)
```

2.8 Lokale Verwaltung der Konfigurationsprotokolle

Das LCOS unterstützt eine Vielzahl von Protokollen für das Management und Monitoring der enthaltenen Funktionen. Die Verwendung der Konfigurationsprotokolle kann zentral für LAN-, WAN- und ggf. WLAN-Verbindungen konfiguriert werden.

Um die Konfigurationsdaten vor unbefugtem Zugriff zu schützen, sollten ausschließlich verschlüsselte Konfigurationsprotokolle zum Einsatz kommen. LCOS unterstützt hierfür SSH, SSL, Telnet über SSL und HTTPS.

Unverschlüsselte Protokolle wie Telnet, HTTP und TFTP sollten deaktiviert werden oder ausschließlich über vertrauenswürdige Verbindungen, z. B. IPSec-VPN-Strecken, verwendet werden.

SNMPv1 und SNMPv2 (zusammengefasst unter der Einstellung „SNMP“) sollten vollständig deaktiviert werden.

2.8.1 IPv4

Pfad

```
/Setup/Config/Access-Table
```

Kommando

```
cd /Setup/Config/Access-Table
tab Ifc. Telnet TFTP HTTP SNMP HTTPS Telnet-SSL SSH Config-Sync SNMPv3
set LAN No No No No Yes Yes Yes Yes Yes
set WAN No No No No Yes Yes Yes No Yes
set WLAN No No No No Yes Yes Yes No Yes
cd /
```

Mögliche Einträge für columns in Access-Table

```
[  1] Ifc.         : value fixed
[  2] Telnet       : VPN (16), Yes (1), Read (4), No (0)
[  3] TFTP         : VPN (16), Yes (1), Read (4), No (0)
[  4] HTTP         : VPN (16), Yes (1), Read (4), No (0)
[  5] SNMP         : VPN (16), Yes (1), Read (4), No (0)
[  6] HTTPS        : VPN (16), Yes (1), Read (4), No (0)
[  7] Telnet-SSL   : VPN (16), Yes (1), Read (4), No (0)
[  8] SSH          : VPN (16), Yes (1), Read (4), No (0)
[ 10] Config-Sync : VPN (16), Yes (1), Read (4), No (0)
[  9] SNMPv3       : VPN (16), Yes (1), Read (4), No (0)
```

2.8.2 IPv6

In der IPv6-Inbound-Firewall existiert eine Regel „DENYALL“, die sämtlichen eingehenden Traffic von außerhalb blockiert. Stellen Sie sicher, dass diese Regel auf Ihrem Gerät aktiviert ist.

Pfad

```
/Setup/IPv6/Firewall/Inbound-Rules
```

Kommando

```
cd /Setup/IPv6/Firewall/Inbound-Rules
tab  Name         Action         Services  Source-Stations  Active  Prio  Src-Tag  Comment
add  "DENY-ALL"   "REJECT-SNMP"  "ANY"     "ANYHOST"        Yes     0     0        "reject all communication
                                                                                    to the device"
cd /
```

Mögliche Einträge

```
[ 1] Name            : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 5] Action          : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 7] Services        : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 8] Source-Stations : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 2] Active          : Yes (0), No (1)
[ 3] Prio            : 4 chars from 1234567890
[11] Src-Tag         : 5 chars from 1234567890
[10] Comment         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdef
                                     ghijklmnopqrstuvwxyz `
```

3 SSL Protokoll-Versionen festlegen

3.1 SSL Protokoll-Version für HTTPS-Verbindungen

Pfad

```
/Setup/HTTP/SSL
```

Kommando

```
cd /Setup/HTTP/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[3] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.2 SSL Protokoll-Version für Telnet-Verbindungen

Pfad

```
/Setup/Config/Telnet-SSL
```

Kommando

```
cd /Setup/Config/Telnet-SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[2] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.3 SSL Protokoll-Version für das CPE WAN Management Protocol, TR-069

Pfad

```
/Setup/CWMP/SSL
```

Kommando

```
cd /Setup/CWMP/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1.2 (8), TLSv1.3 (16)
```

3.4 SSL Protokoll-Version für RADSEC

Pfad

```
/Setup/RADIUS/RADSEC
```

Kommando

```
cd /Setup/RADIUS/RADSEC
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.5 SSL Protokoll-Version für die Aktions-Tabelle

Pfad

```
/Setup/WAN/SSL-for-Action-Table
```

Kommando

```
cd /Setup/WAN/SSL-for-Action-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.6 SSL Protokoll-Version für Seitentabelle im Public Spot-Modul

Pfad

```
/Setup/Public-Spot-Module/SSL-for-Page-Table
```

Kommando

```
cd /Setup/Public-Spot-Module/SSL-for-Page-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.7 SSL Protokoll-Version für E-Mail2SMS-Authentifizierung

Pfad

```
/Setup/Public-Spot-Module/Authentication-Modules/e-mail2Sms-Authentication/SSL
```

Kommando

```
cd /Setup/Public-Spot-Module/Authentication-Modules/e-mail2Sms-Authentication/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.8 SSL Protokoll-Version für RADIUS-Server-Authentifizierung

Pfad

```
/Setup/Public-Spot-Module/Authentication-Modules/Radius-Server/SSL
```

Kommando

```
cd /Setup/Public-Spot-Module/Authentication-Modules/Radius-Server/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.9 SSL Protokoll-Version für das Laden von Firmware, Konfiguration oder Skripten über das Netzwerk

Pfad

```
/Setup/Autoload/Network/SSL
```

Kommando

```
cd /Setup/Autoload/Network/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.10 SSL Protokoll-Version für das zentrale Firmware Management

Pfad

```
/Setup/WLAN-Management/Central-Firmware-Management/SSL
```

Kommando

```
cd /Setup/WLAN-Management/Central-Firmware-Management/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.11 SSL Protokoll-Version für den Rollout-Agent

Pfad

```
/Setup/Config/Rollout-Agent/SSL
```

Kommando

```
cd /Setup/Config/Rollout-Agent/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.12 SSL Protokoll-Version für den Rollout-Wizard

Pfad

```
/Setup/HTTP/Rollout-Wizard/SSL
```

Kommando

```
cd /Setup/HTTP/Rollout-Wizard/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.13 SSL Protokoll-Version für den SYSLOG-Server

Pfad

```
/Setup/SYSLOG/SSL
```

Kommando

```
cd /Setup/SYSLOG/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1.2 (8), TLSv1.3 (16)
```

3.14 SSL Protokoll-Version für CRON-Tabelle

Pfad

```
/Setup/Config/SSL-for-Cron-Table
```

Kommando

```
cd /Setup/Config/SSL-for-Cron-Table
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.15 SSL Protokoll-Version für Mail

Pfad

```
/Setup/Mail/SSL
```

Kommando

```
cd /Setup/Mail/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.16 SSL Protokoll-Version für SCEP-Client

Pfad

```
/Setup/Certificates/SCEP-Client/SSL
```

Kommando

```
cd /Setup/Certificates/SCEP-Client/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.17 SSL Protokoll-Version für ACME-Client

Pfad

```
/Setup/Certificates/ACME-Client/SSL
```

Kommando

```
cd /Setup/Certificates/ACME-Client/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.18 SSL Protokoll-Version für IoT

Pfad

```
/Setup/IoT/Wireless-ePaper/SSL
```

Kommando

```
cd /Setup/IoT/Wireless-ePaper/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.19 SSL Protokoll-Version für WLAN-Management

Pfad

```
/Setup/WLAN-Management/Central-Firmware-Management/SSL
```

Kommando

```
cd /Setup/WLAN-Management/Central-Firmware-Management/SSL
set Versions TLSv1.2,TLSv1.3
cd /
```

Mögliche Einträge

```
[1] Versions : Bitmask: TLSv1 (2), TLSv1.1 (4), TLSv1.2 (8), TLSv1.3 (16)
```

3.20 Rücksetzen der SSL-Einstellungen auf Standardwerte

Mit dem Kommandozeilenbefehl `ssldefaults` können die SSL-Einstellungen entweder im jeweiligen Konfigurationspfad (z. B. `/Setup/Public-Spot-Module/SSL-for-Page-Table`) oder global im Root-Pfad auf die Standardwerte zurückgesetzt werden.

Nach dem Zurücksetzen sind standardmäßig folgende Protokolle aktiviert:

- TLS 1.2
- TLS 1.3

Kommando

```
ssldefaults
```

3.21 Lokale Verwaltung der Administratoren- und Funktionsrechte

Beim lokalen Rechtemanagement können neben dem Root-User weitere Administratoren angelegt werden, um Administratoren mit unterschiedlichen Berechtigungen zu definieren. Diese lokalen Administratoren stehen für sämtliche unterstützten Konfigurationsprotokolle zur Verfügung.

Pfad

```
/Setup/Config/Admins
```

Kommando

```
cd /Setup/Config/Admins
tab Administrator Password
add "admin"       "********!"
tab Encrypted-Password
add "$6$2x4/JZ0hJbbkPWgW$TrQ3.dplvHeE/yZQ9ohxDab4W0GfOJqx3M1mO0EsBnLYwUVMcymlzWqv5rCnDQDJlLonryzhLdCK0T.wOaozQ1"
tab Active Access-Rights  Function-Rights SNMP-Encrypted-Password
add Yes    Admin-RO-Limit 0              "7BAC1CBBEED062F29D5B5CDDC81D6D60EBDFBF6B03FB102300544D2D69691C96"
cd /
```

Im Beispielskript wird ein Administrator eingerichtet, der über Leserechte verfügt, jedoch aufgrund von Einschränkungen keine Trace-Funktionen (Limit) und keine Wizards (Funktionsrechte) ausführen darf.

Read-Only-Administratoren ist das Auslesen von Passwortfeldern innerhalb der Konfiguration nicht gestattet.

Bei Verwendung einer zentralen Authentisierung für Administratoren können keine zusätzlichen lokalen Administrator-Accounts genutzt werden.

Mögliche Einträge

```
[1] Administrator           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/;<=>?[\]^_.0123456789ab
                                            cdefghijklmnopqrstuvwxyz`
[2] Password                : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[6] Encrypted-Password      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[4] Active                  : No (1), Yes (0)
[5] Access-Rights           : none (0), Admin-RO-Limit (8388608), Admin-RW-Limit (8388864),
                              Admin-RO (16777216), Admin-RW (16777472), Supervisor (4294967295)
[3] Function-Rights         : Bitmask: Basic-Wizard (0x1), Security-Wizard (0x2), Internet-Wizard (0x4),
                                       RAS-Wizard (0x10), Provider-Selection (0x8), LANLAN-Wizard (0x20),
                                       Time-Setting (0x40), Device-Search (0x80), Rollout-Wizard (0x2000),
                                       Public-Spot-Wizard (0x800), Dynamic-DNS-Wizard (0x4000),
                                       VoIP-CallManager-Wizard (0x8000), SSH-Command (0x20000),
                                       CF-Profile-Wizard (0x40000), Public-Spot-Xml-Interface (0x80000),
                                       Public-Spot-User-Management-Wizard (0x100000),
                                       Public-Spot-Configuration-Wizard (0x200000),
                                       Prepare-VoIP-Provider-Access (0x800000), CA-Web-Interface (0x1000000),
                                       User-Wizard-1 (0x2000000), User-Wizard-2 (0x4000000),
                                       User-Wizard-3 (0x8000000), User-Wizard-4 (0x10000000),
                                       Telekom-Internet-Protect-Pro-Wizard (0x20000000)
[7] SNMP-Encrypted-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
```

3.22 IPv4-Zugangsliste

Über die TCP-Zugangsliste können die Quelladressen von Administratoren pro Routing-Kontext (Rtg-Tag) eingeschränkt werden. Nur vertrauenswürdige Quellnetze innerhalb von Verwaltungsnetzen sollten für den Konfigurationszugriff freigegeben werden.

Pfad

```
/Setup/TCP-IP/Access-List
```

Kommando

```
cd /Setup/TCP-IP/Access-List
tab IP-Address  IP-Netmask  Rtg-tag  Comment
add 10.0.0.0    255.0.0.0   1
cd /
```

Werden keine Adressen in der Zugangsliste definiert, ist der Zugriff aus beliebigen Quelladressen erlaubt!

Mögliche Einträge

```
[1] Administrator           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/;<=>?[\]^_.0123456789ab
                                            cdefghijklmnopqrstuvwxyz`
[2] Password                : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[6] Encrypted-Password      : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                             89abcdefghijklmnopqrstuvwxyz `
[4] Active                  : No (1), Yes (0)
[5] Access-Rights           : none (0), Admin-RO-Limit (8388608), Admin-RW-Limit (8388864),
                              Admin-RO (16777216), Admin-RW (16777472), Supervisor (4294967295)
[3] Function-Rights         : Bitmask: Basic-Wizard (0x1), Security-Wizard (0x2), Internet-Wizard (0x4),
                                       RAS-Wizard (0x10), Provider-Selection (0x8), LANLAN-Wizard (0x20),
                                       Time-Setting (0x40), Device-Search (0x80), Rollout-Wizard (0x2000),
                                       Public-Spot-Wizard (0x800), Dynamic-DNS-Wizard (0x4000),
                                       VoIP-CallManager-Wizard (0x8000), SSH-Command (0x20000),
                                       CF-Profile-Wizard (0x40000), Public-Spot-Xml-Interface (0x80000),
```

```
                                    Public-Spot-User-Management-Wizard (0x100000),
                                    Public-Spot-Configuration-Wizard (0x200000),
                                    Prepare-VoIP-Provider-Access (0x800000), CA-Web-Interface (0x1000000),
                                    User-Wizard-1 (0x2000000), User-Wizard-2 (0x4000000),
                                    User-Wizard-3 (0x8000000), User-Wizard-4 (0x10000000),
                                    Telekom-Internet-Protect-Pro-Wizard (0x20000000)
[7] SNMP-Encrypted-Password : 128 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.01234567
                                          89abcdefghijklmnopqrstuvwxyz `
```

3.23 IPv6-Zugangsliste

Pfad

```
/Setup/IPv6/Firewall/Inbound-Rules
```

Kommando

```
cd /Setup/IPv6/Firewall/Inbound-Rules
tab Name       Action        Services Source-Stations Active Prio Src-Tag Comment
add "DENY-ALL" "REJECT-SNMP"  ANY"    "ANYHOST"       Yes    0    0       "reject all communication to the
                                                                           device"
cd /
```

Mögliche Einträge

```
[ 1] Name            : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 5] Action          : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 7] Services        : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 8] Source-Stations : 64 chars from  ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                     case characters are converted to upper case)
[ 2] Active          : Yes (0), No (1)
[ 3] Prio            : 4 chars from 1234567890
[11] Src-Tag         : 5 chars from 1234567890
[10] Comment         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdef
                                     ghijklmnopqrstuvwxyz `
```

3.24 Session-Management

Um zu verhindern, dass Konfigurationsverbindungen unbefugt übernommen werden, sollte die zulässige Leerlaufdauer (Idle Time) einer Konfigurationssitzung begrenzt werden.

Pfad

```
/Setup/Config
```

Kommando

```
set /Setup/Config/Config-Aging-Minutes 15 (für TCP basierte Verbindungen)
set /Setup/Config/Outband-Aging-Minutes 5 (für serielle Verbindung)
```

4 Layer-2-Management

Das LCOS unterstützt für den Fall eines Desaster-Recovery das LANCOM Layer-2-Management-Protokoll (LL2M), um Geräte ohne direkten physikalischen Zugang über Ethernet authentifiziert umzukonfigurieren oder auf die Werkseinstellungen zurückzusetzen.

Soll diese Funktion nicht genutzt werden, ist sie zu deaktivieren. Bei aktiviertem Layer-2-Management empfiehlt sich eine Einschränkung des Zugriffs auf einen konfigurierbaren Zeitraum in Sekunden, der nach dem Neustart des jeweiligen Geräts für Layer-2-Management-Zugriffe zur Verfügung steht.

Pfad

```
/Setup/Config/LL2M
```

Kommando

```
set /Setup/Config/LL2M/Operating No
set /Setup/Config/LL2M/Time-Limit 0
```

Mögliche Einträge

```
[1] Operating         : No (0), Yes (1), Client-Only (2)
[2] Time-Limit        : 10 chars from 1234567890
[3] Crypto-Algorithms : Bitmask: Simple (2), SHA256 (4), SHA512 (8)
```

5 Diebstahlschutz

Der Betrieb des IP-Routers kann an eine Standortüberprüfung gekoppelt werden. Diese Diebstahlschutzfunktion schränkt den Betrieb des LANCOM Routers auf fest definierte Standorte ein.

Der Betrieb eines entwendeten LANCOM Routers wird dadurch erheblich erschwert oder sogar vollständig verhindert. Zur Standortüberprüfung steht – je nach Gerätetyp – die GPS-Funktion in absteigender Sicherheitsstufe zur Verfügung.

Pfad

```
/Setup/Config/Anti-Theft-Protection
```

Kommando

```
set /Setup/Config/Anti-Theft-Protection/Enabled No
set /Setup/Config/Anti-Theft-Protection/Deviation 50
set /Setup/Config/Anti-Theft-Protection/Get-GPS-Position No
set /Setup/Config/Anti-Theft-Protection/Latitude 12.3456789
set /Setup/Config/Anti-Theft-Protection/Longitude 1.2345678
```

Mögliche Einträge

```
[ 1] Enabled          : No (0), Yes (1)
[ 8] Deviation[m]     : 4 chars from 1234567890
[ 9] Longitude[deg]   : 12 chars from +-.0123456789
[10] Latitude[deg]    : 11 chars from +-.0123456789
[12] Get-GPS-position : No (0), Yes (1)
```

5.1 Offline-Konfigurationen

Die Konfiguration von LCOS-basierten Geräten kann zur Offline-Bearbeitung und zur Archivierung ausgelesen werden. Hierfür stehen zwei Formate zur Verfügung: die LANconfig-Konfiguration im Format „.lcf“ sowie die LANCOM Script-Konfiguration im Format „.lcs“.

Die LANconfig-Konfiguration stellt ein vollständiges Abbild der Gerätekonfiguration dar. Sie enthält insbesondere das Root-Konfigurationspasswort im Klartext, sofern die Datei nicht verschlüsselt heruntergeladen wurde. Daher wird dringend empfohlen, LANconfig-Konfigurationsdateien stets verschlüsselt herunterzuladen.

Die LANCOM Script-Konfigurationen enthalten nach dem Auslesen alle Passwörter mit Ausnahme des Root-Konfigurationspassworts im Klartext.

Kommando

```
Readconfig (LANconfig File Format)
Reascript (LANCOM Script Format)
```

Die Kommandos sind jeweils über TFTP, serielle Konsole, HTTP, HTTPS, Telnet, Telnet SSL und SSH ausführbar.

Das Auslesen vollständiger Konfigurationen über diese Befehle ist ausschließlich Administratoren mit Supervisor-Rechten gestattet.

Alle LANCOM Konfigurationsdateien sind als sicherheitsrelevant zu betrachten und entsprechend geschützt zu archivieren!

6 Interne Dienste und Logging

6.1 Dienstaktivierung

Das LCOS stellt eine Vielzahl interner Dienste bereit. Um potenziellem Missbrauch vorzubeugen, sollten nicht benötigte Dienste konsequent deaktiviert werden. Eine Übersicht der aktuell konfigurierten Dienste finden Sie im Status-Baum.

Pfad

```
/Status/config/services
```

6.1.1 DHCP

Wenn die dynamische IP-Adressvergabe durch den DHCP-Dienst des LCOS nicht genutzt werden soll, kann diese Funktion für jeden ARF-Kontext separat deaktiviert werden.

Pfad

```
/Setup/DHCP/Network-list
```

Kommando

```
cd /Setup/DHCP/Network-list
tab Network-name Start-Address-Pool End-Address-Pool Netmask Broadcast-Address Gateway-Address DNS-Default
add "INTRANET"   172.16.0.1         172.16.0.254     0.0.0.0 0.0.0.0           0.0.0.0         0.0.0.0
tab DNS-Backup Operating Broadcast-Bit Master-Server 2nd-Master-Server 3rd-Master-Server 4th-Master-Server
add 0.0.0.0    Yes       No            0.0.0.0       0.0.0.0           0.0.0.0           0.0.0.0
tab Loopback-Address Cache Adaption Cluster Max.-Lease Def.-Lease Suppress-ARP-check
add ""               No    No       Yes     0          0          No
cd /
```

Mögliche Einträge

```
[ 1] Network-name       : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789
                                        (lower case characters are converted to upper case)
[ 2] Start-Address-Pool : 15 chars from 1234567890.
[ 3] End-Address-Pool   : 15 chars from 1234567890.
[ 4] Netmask            : 15 chars from 1234567890.
[ 5] Broadcast-Address  : 15 chars from 1234567890.
[ 6] Gateway-Address    : 15 chars from 1234567890.
[ 7] DNS-Default        : 15 chars from 1234567890.
[ 8] DNS-Backup         : 15 chars from 1234567890.
[11] Operating          : No (0), Yes (1), Auto (2), Stateless-Relay (8), Relay (16), Client (4)
[12] Broadcast-Bit      : No (0), Yes (1)
[13] Master-Server      : 15 chars from 1234567890.
[17] 2nd-Master-Server  : 15 chars from 1234567890.
[18] 3rd-Master-Server  : 15 chars from 1234567890.
[19] 4th-Master-Server  : 15 chars from 1234567890.
[22] Loopback-Address   : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[14] Cache              : No (0), Yes (1)
[15] Adaption           : No (0), Yes (1)
[16] Cluster            : No (0), Yes (1)
[20] Max.-Lease         : 5 chars from 1234567890
[21] Def.-Lease         : 5 chars from 1234567890
[23] Suppress-ARP-check : No (0), Yes (1)
```

6.1.2 DNS

Der DNS-Server des LCOS kann sowohl statisch konfigurierte Namen als auch über DHCP erlernte Namen auflösen. Wenn diese Funktion nicht benötigt wird, sollte der Dienst deaktiviert werden.

Das DNS-Forwarding an einen definierten DNS-Server bleibt davon unberührt.

Pfad

```
/Setup/DNS
```

Kommando

```
set /Setup/DNS/Operating No
```

Mögliche Einträge

```
Operating : No (0), Yes (1)
```

6.2 Quellrouten-Überprüfung

Die internen Dienste im LCOS sind in der Lage, eine Überprüfung der Quellrouten durchzuführen. In den Standardeinstellungen akzeptiert das LCOS Zugriffe auf interne Dienste unabhängig von der Quelladresse.

Dies ermöglicht die Remote-Administration eines LANCOM Geräts auch ohne konfigurierte Rückroute. Soll die Administration ausschließlich aus explizit im Routing definierten Quellnetzen möglich sein, ist die Quellrouten-Überprüfung für interne Dienste zu aktivieren (Src-check: strict).

Pfad

```
/Setup/TCP-IP/Network-list
```

Kommando

```
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask    VLAN-ID Interface Src-check Type     Rtg-tag Comment
add "INTRANET"   172.16.0.1 255.255.255.0 1       LAN-1     strict    Intranet 1       "local intranet"
cd /
```

Mögliche Einträge

```
[1] Network-name : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower case
                                 characters are converted to upper case)
[2] IP-Address   : 15 chars from 1234567890.
[3] IP-Netmask   : 15 chars from 1234567890.
[4] VLAN-ID      : 4 chars from 1234567890
[5] Interface    : LAN-1 (256), LAN-2 (257), LAN-3 (258), LAN-4 (259), LAN-5 (260), LAN-6 (261), LAN-7 (262),
                   GRE-TUNNEL-1 (2304), GRE-TUNNEL-2 (2305), GRE-TUNNEL-3 (2306), GRE-TUNNEL-4 (2307),
                   GRE-TUNNEL-5 (2308), GRE-TUNNEL-6 (2309), GRE-TUNNEL-7 (2310), GRE-TUNNEL-8 (2311),
                   BUNDLE-1 (2048), BUNDLE-2 (2049), L2TP-ETHERNET-1 (2560), L2TP-ETHERNET-2 (2561),
                   L2TP-ETHERNET-3 (2562), L2TP-ETHERNET-4 (2563), L2TP-ETHERNET-5 (2564),
                   L2TP-ETHERNET-6 (2565), L2TP-ETHERNET-7 (2566), L2TP-ETHERNET-8 (2567),
                   L2TP-ETHERNET-9 (2568), L2TP-ETHERNET-10 (2569), L2TP-ETHERNET-11 (2570),
                   L2TP-ETHERNET-12 (2571), L2TP-ETHERNET-13 (2572), L2TP-ETHERNET-14 (2573),
                  L2TP-ETHERNET-15 (2574), L2TP-ETHERNET-16 (2575), BRG-1 (1536), BRG-2 (1537), BRG-3 (1538),

                   BRG-4 (1539), BRG-5 (1540), BRG-6 (1541), BRG-7 (1542), BRG-8 (1543), any (65535)
[6] Src-check    : strict (1), loose (0)
[7] Type         : Disabled (0), Intranet (1), DMZ (2)
[8] Rtg-tag      : 5 chars from 1234567890
[9] Comment      : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghij
                                 klmnopqrstuvwxyz `
```

6.3 Zeiteinstellungen

Um Statusinformationen im zeitlichen Zusammenhang auswerten zu können, sollte auf dem Gerät eine Zeitsynchronisation über den NTP-Dienst eingerichtet sein. Erfolgen Authentifizierungen über digitale Zertifikate, ist eine synchronisierte Uhrzeit im LCOS zwingend erforderlich.

Pfad

```
/Setup/Time
/Setup/NTP
/Setup/NTP/RQ-Address
```

Kommando

```
cd /Setup/NTP/RQ-Address
tab RQ-Address                Loopback-Addr. Authentication-Enabled Key-ID
add "NTPS1-0.CS.TU-BERLIN.DE" "INTRANET"     No                     1
add "NTPS1-1.CS.TU-BERLIN.DE" "INTRANET"     No                     1
cd /
```

Der LANCOM Router kann pro Netzwerk die Zeit als Zeitserver intern bereitstellen. Soll dieser Dienst nicht genutzt werden, ist der Zeitserver zu deaktivieren.

Pfad

```
/Setup/NTP/Networklist
```

Kommando

```
cd /Setup/NTP/Networklist
tab Network-name Server-Operating
add "INTRANET"   Yes
cd /
```

6.3.1 MD5-Authentifizierung für NTP-Server

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

Pfad

```
/Setup/NTP
```

Kommando

```
set /Setup/NTP/Server-Authentication Yes
```

MD5-Schlüssel

Der Eintrag enthält den Wert des/der Schlüssel.

Pfad

```
/Setup/NTP/Authentication-Keys
```

Kommando

```
cd /Setup/NTP/Authentication-Keys
tab Key-ID Key               Key-Type
add 1      "dsajfndyjkvhfhgh" MD5
cd /
```

Mögliche Einträge

```
[1] Key-ID   : 10 chars from 1234567890
[2] Key      : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefghijklmn
                             opqrstuvwxyz `
[3] Key-Type : MD5 (0), AES-CMAC-128 (1)
```

Vertrauenswürdige Schlüssel

Enthält eine kommaseparierte Liste der vertrauenswürdigen Schlüssel (Schlüsselnummern).

Pfad

```
/Setup/NTP/Server-Trusted_Keys
```

Kommando

```
set /Setup/NTP/Server-Trusted_Keys [0-9,..]
```

6.3.2 MD5-Authentifizierung für NTP-Client

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

Pfad

```
/Setup/NTP/RQ-Address
```

Kommando

```
cd /Setup/NTP/RQ-Address
cd <List entry>
set Authentication-Enabled yes
```

Schlüsselnummer

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

Pfad

```
/Setup/NTP/RQ-Address
```

Kommando

```
cd /Setup/NTP/RQ-Address
cd <List entry>
set Key-ID [1…65535]
```

Mögliche Einträge

```
[1] RQ-Address: 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789abcdefghijklmnop
                              qrstuvwxyz`
[2] Loopback-Addr.: 39 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+,/:;<=>?[\]^_.0123456789
[3] Authentication-Enabled: No (0), Yes (1)
[4] Key-ID: 10 chars from 1234567890
```

6.4 Internes und externes Event-Logging

Zur umfassenden Dokumentation interner Abläufe im LCOS sollten Syslog-Ereignisse sowohl lokal als auch auf einem externen Server aufgezeichnet werden. Um die Informationsmenge überschaubar zu halten, ist es empfehlenswert, Quellen und Prioritäten gezielt auf den jeweiligen Verwendungszweck abzustimmen.

Der Parameter `Log-CLI-Changes` aktiviert die Protokollierung von Kommandozeilenbefehlen. Ist dieser Parameter aktiv, wird bei der Ausführung eines Befehls über die Kommandozeile des Geräts automatisch ein Eintrag im internen Syslog-Speicher erzeugt.

Pfad

```
/Setup/SYSLOG
/Setup/SYSLOG/Server
```

Kommando

```
set /Setup/SYSLOG/Operating Yes
set /Setup/SYSLOG/ Log-CLI-Changes Yes

cd /Setup/SYSLOG/Server
tab Idx.   IP-Address  Port Protocol RFC5424-Format Source Level Loopback-Addr. Filter-Policy Filter-Name
add "0002" "10.1.1.11" 514  UDP      No             ff     07    "INTRANET"     Allow         ""
add "0001" "127.0.0.1" 514  UDP      No             ff     07    "INTRANET"     Allow         ""
cd /
```

Das Beispielscript aktiviert Syslog Nachrichten aus allen Quellen mit Level ab Warnung, sowohl intern (127.0.0.1) als auch extern (10.1.1.11).

7 IP und Routing

7.1 Loopback-Adressen

Wenn LANCOM Router zusätzlich zu den interfacegebundenen IP-Adressen über separate Management-IP-Adressen erreichbar sein sollen, können benannte Loopback-Adressen konfiguriert werden. Diese lassen sich sowohl für die aktive als auch passive Kommunikation des Routers verwenden.

Die Loopback-Adressen müssen im Routing des Netzwerks berücksichtigt werden. Sie können internen Diensten des Routers als Absenderadresse zugewiesen werden. Über das Routing-Tag werden die Loopback-Adressen den jeweiligen ARF-Kontexten zugeordnet.

Pfad

```
/Setup/TCP-IP/Loopback-List
```

Kommando

```
cd /Setup/TCP-IP/Loopback-List
tab Name          Loopback-Addr.  Rtg-tag
add "MANAGEMENT"  10.1.2.3        1
cd /
```

Internen Diensten, die aktiv kommunizieren, kann eine Loopback-Adresse als Absenderadresse zugewiesen werden.

7.2 Definition virtueller Router

Abhängig vom Gerätetyp stellt LCOS zwei bis zu 256 virtuelle Router bereit, die über sogenannte Routing-Tags voneinander getrennt werden können.

Diese virtuellen Router – auch ARF-Kontexte genannt – lassen sich physikalischen Interfaces und / oder VLANs zuweisen. Gleiche Routing-Tags ermöglichen das Routing zwischen den zugehörigen Netzen, während unterschiedliche Routing-Tags die Netze strikt voneinander trennen.

Das Routing-Tag wirkt als Filter auf die Routing-Tabelle und bestimmt damit, welche Routen einem bestimmten ARF-Kontext zur Verfügung stehen.

Pfad

```
/Setup/TCP-IP/Network-list
```

Kommando

```
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask  VLAN-ID Interface Src-check Type     Rtg-tag Comment
add "INTRANET-1" 10.1.1.11  255.255.0.0 1       LAN-1     loose     Intranet 1
add "INTRANET-2" 10.2.1.11  255.255.0.0 2       LAN-1     loose     Intranet 1
add "OFFICE"     10.5.1.11  255.255.0.0 5       LAN-1     loose     Intranet 5
cd /
```

Die Zuordnung von ARF-Netzen zu VLANs und Interfaces lässt sich mit folgendem Befehl überprüfen:

```
Ifc.: LAN-1
INTRANET 10.1.1.11 255.255.0.0 1
OFFICE   10.5.1.11 255.255.0.0 5
```

Im gezeigten Beispiel werden drei Netze eingerichtet. INTRANET-1 und INTRANET-2 teilen sich das gleiche Routing-Tag und sind damit untereinander routbar. Das Netz OFFICE hingegen wird durch ein abweichendes Routing-Tag logisch separiert.

Stellen Sie sicher, dass Netze, die voneinander isoliert bleiben sollen, mit **unterschiedlichen** Routing-Tags konfiguriert werden!

Das Routing-Tag 0 kennzeichnet ein Supervisor-Netz, das uneingeschränkten Zugriff auf alle anderen Netze besitzt. Es sollte daher mit besonderer Sorgfalt verwendet werden!

7.3 Verwendung virtueller Router im Routing

Routing-Tags definieren, welche Routen aus der globalen Routing-Tabelle einem ARF-Kontext (virtueller Router) zur Verfügung stehen. Ein ARF-Kontext kann nur jene Routen verwenden, die mit seinem Routing-Tag übereinstimmen.

Zusätzlich gelten Routen mit dem Routing-Tag **0** als global sichtbar und sind daher für alle Kontexte zugänglich.

Pfad

```
/Setup/IP-Router/IP-Routing-Table
```

Kommando

```
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask   Rtg-tag Admin-Distance Peer-or-IP     Distance Masquerade Active Comment
add 10.11.0.0  255.255.0.0  1       0              "VPN-INTRANET" 0        No         Yes
add 10.15.0.0  255.255.0.0  5       0              "VPN-OFFICE"   0        No         Yes
cd /
```

Stellen Sie sicher, dass das Routing-Tag des jeweiligen ARF-Kontexts mit den ihm zugewiesenen Routen übereinstimmt. Abweichungen können zu unerwünschtem Routing-Verhalten führen.

WAN-seitig empfangene IP-Pakete erhalten standardmäßig das Routing-Tag **0**, wodurch alle lokalen Netze erreichbar sind.

Bei Verwendung von dynamischem Routing kann das Routing-Tag dynamisch gelernter Routen automatisch über die Konfiguration der Gegenstelle vergeben werden.

Pfad

```
/Setup/IP-Router/Tag-Table
```

Kommando

```
cd /Setup/IP-Router/Tag-Table
tab Peer        Rtg-tag  Start-WAN-Pool  End-WAN-Pool  DNS-Default  DNS-Backup
add "OFFICE-*"  5        0.0.0.0         0.0.0.0       0.0.0.0      0.0.0.0
cd /
```

Mögliche Einträge

```
[1] Peer           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789 (lower
                                                    case characters are converted to upper case)
[2] Rtg-tag        : 5 chars from 1234567890
[3] Start-WAN-Pool : 15 chars from 1234567890.
[4] End-WAN-Pool   : 15 chars from 1234567890.
[5] DNS-Default    : 15 chars from 1234567890.
[6] DNS-Backup     : 15 chars from 1234567890.
```

Zur Gruppierung mehrerer Gegenstellen kann das Wildcard-Zeichen * verwendet werden. Gegenstellen mit identischem Namenspräfix erhalten dann das konfigurierte Routing-Tag. Dies ist besonders hilfreich für VPN-Einwahlclients mit individuellen Adresspools.

Das ARF – in seiner Kombination aus Interface-, VLAN- und Routing-Tag-Zuordnung – stellt das zentrale Element zur logischen Trennung oder Verbindung von Netzsegmenten dar. Es muss sichergestellt sein, dass ARF-Kontexte nur mit den vorgesehenen Routen und Gegenstellen über das Routing-Tag verknüpft werden.

Routing-Tags können auch in Firewall-Regeln für Policy-based Routing verwendet werden. Prüfen Sie Firewall-Konfigurationen sorgfältig auf korrekte Behandlung des Routing-Tags, um die Isolation einzelner ARF-Kontexte zu gewährleisten.

7.4 Dynamisches Routing

LCOS unterstützt RIPv2, OSPFv2, BGPv4 und LISP als dynamische Routing Protokolle.

7.4.1 RIPv2

Da RIPv2 keine Authentisierung vorsieht, darf dynamisches Routing ausschließlich in vertrauenswürdigen lokalen Netzen und mit autorisierten Gegenstellen aktiviert werden.

Um eine missbräuchliche Manipulation der Routing-Informationen zu verhindern, ist sicherzustellen, dass RIPv2 keine Informationen von unautorisierten Teilnehmern entgegennimmt oder verbreitet.

Im LAN erfolgt die Kommunikation von RIPv2 auf Multicast-Basis. Es ist daher unerlässlich, dass der physikalische Zugang zum Ethernet ausschließlich autorisierten Netzwerkteilnehmern gewährt wird.

Für WAN-Verbindungen gilt: RIPv2 ist nur für definierte, vertrauenswürdige Gegenstellen zu aktivieren. Es muss gewährleistet sein, dass gerichtete RIP-Unicasts nicht über WAN-Verbindungen weitergeleitet werden.

LAN

Pfad

```
/Setup/IP-Router/RIP/LAN-Sites
```

Kommando

```
cd /Setup/IP-Router/RIP/LAN-Sites
tab Network-name RIP-Type RIP-Send RIP-Accept Propagate Poisoned-Reverse Dft-Rtg-Tag Rtg-Tag-List Ignore-Tags
add "OFFICE"     RIP-2    No       Yes        No        No               0           ""           No
tab Rx-Filter Tx-Filter
add ""        ""
cd /
```

Mögliche Einträge

```
[ 1] Network-name     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[ 2] RIP-Type         : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[12] RIP-Send         : No (0), Yes (1)
[ 3] RIP-Accept       : No (0), Yes (1)
[ 4] Propagate        : No (0), Yes (1)
[ 7] Poisoned-Reverse : No (0), Yes (1)
[ 5] Dft-Rtg-Tag      : 5 chars from 1234567890
[ 6] Rtg-Tag-List     : 33 chars from  ,0123456789
[14] Ignore-Tags      : No (0), Yes (1)
[10] Rx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[11] Tx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
```

WAN

Pfad

```
/Setup/IP-Router/RIP/WAN-Sites
```

Kommando

```
cd /Setup/IP-Router/RIP/WAN-Sites
add "OFFICE-WAN"  RIP-2  No  Yes  auto  No  No  0.0.0.0  ""  0  ""  No  ""  ""
cd /
```

Mögliche Einträge

```
[ 1] Peer             : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789
                                      (lower case characters are converted to upper case)
[ 2] RIP-Type         : Off (0), RIP-1 (1), R1-comp (2), RIP-2 (3)
[12] RIP-Send         : No (0), Yes (1)
[ 3] RIP-Accept       : No (0), Yes (1)
[ 4] Masquerade       : auto (0), on (1), intranet (2)
[ 7] Poisoned-Reverse : No (0), Yes (1)
[ 8] RFC2091          : No (0), Yes (1)
[ 9] Gateway          : 15 chars from 1234567890.
[13] Loopback-Address : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[ 5] Dft-Rtg-Tag      : 5 chars from 1234567890
[ 6] Rtg-Tag-List     : 33 chars from  ,0123456789
[14] Ignore-Tags      : No (0), Yes (1)
[10] Rx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
[11] Tx-Filter        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                      case characters are converted to upper case)
```

7.4.2 OSPFv2

OSPF unterstützt die Authentifizierung auf Interface-Ebene. Es wird empfohlen, den Authentifizierungstyp „Cryptographic-MD5“ zu verwenden. Das Passwort sollte zufällig generiert sein und eine Mindestlänge von acht Zeichen aufweisen.

Pfad

```
/Setup/Routing-Protocols/OSPF/Interfaces
```

Kommando

```
cd /Setup/Routing-Protocols/OSPF/Interfaces
add "INTRANET" "DEFAULT" 0.0.0.0 Broadcast 1 5 1 1 10 40 Cryptographic-MD5 "********" No No
cd /
```

Mögliche Einträge für Interfaces

```
[ 1] Interface            : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                          (lower case characters are converted to upper case)
[ 2] OSPF-Instance        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                          (lower case characters are converted to upper case)
[ 3] Area-ID              : 15 chars from 1234567890.
[ 4] Type                 : Broadcast (0), NBMA (2), Point-To-Point (1), Point-To-Multipoint (3)
[ 5] Output-Cost          : 10 chars from 1234567890
[ 6] Rxmt-Interval        : 10 chars from 1234567890
[ 7] Inf-Trans-Delay      : 10 chars from 1234567890
[ 8] Router-Priority      : 3 chars from 1234567890
[ 9] Hello-Interval       : 10 chars from 1234567890
[10] Router-Dead-Interval : 10 chars from 1234567890
[11] Authentication-Type  : Null (0), Simple-Password (1), Cryptographic-MD5 (2)
[12] Authentication-Key   : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                          bcdefghijklmnopqrstuvwxyz `
[13] Passive              : No (0), Yes (1)
[14] MTU-Ignore           : No (0), Yes (1)
```

Wenn virtuelle Links (Transit-Areas) verwendet werden, um andere Areas mit der Backbone-Area zu verbinden, sollte auch für den virtuellen Link der Authentifizierungstyp „Cryptographic-MD5“ konfiguriert werden.

Pfad

```
/Setup/Routing-Protocols/OSPF/Virtual-Links
```

Kommando

```
cd /Setup/Routing-Protocols/OSPF/Virtual-Links
tab OSPF-Instance Transit-Area-ID Router-ID Rxmt-Interval Hello-Interval Router-Dead-Interval
add "DEFAULT"     1.2.3.4         1.1.1.1   5            10             40
tab Authentication-Type Authentication-Key
add Cryptographic-MD5   "********"
cd /
```

Mögliche Einträge für Virtual-Links

```
[1] OSPF-Instance        : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[2] Transit-Area-ID      : 15 chars from 1234567890.
[3] Router-ID            : 15 chars from 1234567890.
[6] Rxmt-Interval        : 10 chars from 1234567890
[7] Hello-Interval       : 10 chars from 1234567890
[8] Router-Dead-Interval : 10 chars from 1234567890
[4] Authentication-Type  : Null (0), Simple-Password (1), Cryptographic-MD5 (2)
[5] Authentication-Key   : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789ab
                                         cdefghijklmnopqrstuvwxyz `
```

7.4.3 BGPv4

Sie haben die Möglichkeit, Ihre BGP-Nachbarn mit einem Passwort zu authentifizieren. Das Passwort sollte zufällig gewählt sein und mindestens acht Zeichen lang sein.

Pfad

```
/Setup/Routing-Protocols/BGP/Neighbors
```

Kommando

```
cd /Setup/Routing-Protocols/BGP/Neighbors
tab IP-Address    Port Loopback-Address Rtg-tag Remote-AS Name Operating Password   Neighbor-Profile
add "10.10.10.10" 179  "65000"          0       0         ""   Yes       "********" "DEFAULT"
tab Connection-Mode Connection-Delay Instance-Name Inbound-Policy Outbound-Policy Route-Reflector-Client
add Active          120              "DEFAULT"     ""             ""              No
tab BFD-Profile Comment
add ""          ""
cd /
```

Mögliche Einträge

```
[ 1] IP-Address             : 56 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 2] Port                   : 5 chars from 1234567890
[ 3] Loopback-Address       : 56 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 4] Rtg-tag                : 5 chars from 1234567890
[ 5] Remote-AS              : 10 chars from 1234567890
[ 6] Name                   : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[ 7] Operating              : No (0), Yes (1)
[ 8] Password               : 16 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                                             9abcdefghijklmnopqrstuvwxyz `
[ 9] Neighbor-Profile       : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[10] Connection-Mode        : Active (0), Passive (1), Delayed (2)
[11] Connection-Delay       : 5 chars from 1234567890
[12] Instance-Name          : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[13] Inbound-Policy         : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[14] Outbound-Policy        : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz
[16] Route-Reflector-Client : No (0), Yes (1)
[17] BFD-Profile            : 16 chars from -0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ_abcdefghijklmnopqrstuvwxyz

[15] Comment                : 254 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.01234567
                                              89abcdefghijklmnopqrstuvwxyz`
```

7.5 Proxy ARP

Der Mechanismus Proxy ARP wird verwendet, um entfernte Netze und IP-Adressen, die innerhalb eines lokal definierten IP-Netzes liegen, über WAN-Verbindungen einzubinden.

Sofern dieser Mechanismus nicht ausdrücklich benötigt wird und lokale IP-Adressen ausschließlich innerhalb des lokalen Ethernet-Netzes verwendet werden sollen, ist Proxy ARP zu deaktivieren.

Pfad

```
/Setup/IP-Router
```

Kommando

```
set /Setup/IP-Router/Proxy-ARP No
```

Mögliche Einträge

```
Proxy-ARP : No (0), Yes (1)
```

7.6 Stealth-Modus

Eine häufig diskutierte Methode zur Erhöhung der Netzwerksicherheit ist das sogenannte „Verbergen" eines Routers, bei dem dieser eingehende TCP- und UDP-Anfragen ignoriert, anstatt sie gemäß Standard mit einer Ablehnung zu beantworten (Stealth-Modus).

Diese Vorgehensweise ist umstritten, da auch ein Schweigen Hinweise auf die Existenz eines Geräts liefern kann. Ist tatsächlich kein Zielgerät vorhanden, antwortet der vorgelagerte Router mit einer Meldung wie „nicht zustellbar", weil er das Paket nicht weiterleiten kann. Reagiert er hingegen nicht mit einer Ablehnung, war das Ziel für ihn offenbar erreichbar. Unabhängig davon, ob der angefragte Empfänger selbst antwortet, lässt sich daraus auf seine Existenz schließen.

Das Verhalten eines vorgeschalteten Routers lässt sich nicht simulieren, ohne das Gerät tatsächlich offline zu nehmen – was es auch für eigene angeforderte Dienste unerreichbar macht.

Pfad

```
/Setup/IP-Router/Firewall
```

Kommando

```
set /Setup/IP-Router/Firewall/Stealth-Mode WAN
```

Mögliche Einträge

```
Stealth-Mode : off (0), always (1), WAN (2), default-route (3)
```

8 VPN und Firewall

8.1 IKEv2

Unter IKEv2 stehen Ihnen verschiedene Authentisierungsmethoden zur Verfügung:

- PSK – Authentifizierung über einen Pre-Shared Key (vorab vereinbarter geheimer Schlüssel)
- RSA – Zertifikatsbasierte Authentifizierung
- RSASSA-PSS – Zertifikatsbasierte Authentifizierung mit probabilistischem Signaturverfahren
- ECDSA – Zertifikatsbasierte Authentifizierung mit elliptischer Kurven-Kryptographie (probabilistisches Signaturverfahren)
- EdDSA – Zertifikatsbasierte Authentifizierung mit deterministischem Signaturverfahren
- EAP – Authentifizierung über Benutzername/Passwort oder Zertifikate

LANCOM Router unterstützen zudem das ältere, probabilistische Signaturverfahren nach dem Standard `rsassa-pkcs1-v1_5`. LANCOM empfiehlt jedoch die Verwendung modernerer Verfahren wie ECDSA oder EdDSA.

Pfad

```
/Setup/VPN/IKEv2/Auth/Parameter/
/Setup/VPN/IKEv2/Auth/Addit.-Remote-IDs
```

Kommando

```
cd /Setup/VPN/IKEv2/Auth/Parameter/
tab Name  Local-Auth        Local-Dig-Sig-Profile Local-ID-Type Local-ID  Local-Password Remote-Auth
add "VPN" Digital-Signature DEFAULT-ECDSA         Domain-Name   "GATEWAY" ""             Digital-Signature
tab Remote-Dig-Sig-Profile Remote-EAP-Profile Remote-ID-Type Remote-ID Remote-Password PPK-ID
add DEFAULT-ECDSA          ""                 Domain-Name    "PEER"    ""              ""
tab Addit.-Remote-ID-List Local-Certificate Remote-Cert-ID-Check OCSP-Check CRL-Check
add ""                    ""                No                   No         Yes
cd /
```

Mögliche Einträge für Parameter

```
[ 1] Name                   : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 2] Local-Auth             : RSA-Signature (1), PSK (2), ECDSA-256 (9), ECDSA-384 (10), ECDSA-521 (11),
                              Digital-Signature (14)
[13] Local-Dig-Sig-Profile  : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 3] Local-ID-Type          : No-Identity (0), IPv4-Address (1), IPv6-Address (5), Domain-Name (2),
                              Email-Address (3), Distinguished-Name (9), Key-ID (11)
[ 4] Local-ID               : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                                             789abcdefghijklmnopqrstuvwxyz `
[ 5] Local-Password         : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                                            9abcdefghijklmnopqrstuvwxyz `
[ 6] Remote-Auth            : RSA-Signature (1), PSK (2), ECDSA-256 (9), ECDSA-384 (10), ECDSA-521 (11),
                              Digital-Signature (14), EAP (201)
[14] Remote-Dig-Sig-Profile : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[16] Remote-EAP-Profile     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
[ 7] Remote-ID-Type         : No-Identity (0), IPv4-Address (1), IPv6-Address (5), Domain-Name (2),
                              Email-Address (3), Distinguished-Name (9), Key-ID (11)
[ 8] Remote-ID              : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                                             789abcdefghijklmnopqrstuvwxyz `
[ 9] Remote-Password        : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012345678
                                            9abcdefghijklmnopqrstuvwxyz `
[18] PPK-ID                 : 66 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789a
                                            bcdefghijklmnopqrstuvwxyz`
[10] Addit.-Remote-ID-List  : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                            (lower case characters are converted to upper case)
```

```
[11] Local-Certificate      : 254 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.0123456
                                              789abcdefghijklmnopqrstuvwxyz `
[12] Remote-Cert-ID-Check   : No (0), Yes (1)
[15] OCSP-Check             : No (0), Yes (1)
[17] CRL-Check              : No (0), Yes (1)
```

Das ausgewählte Digital-Signature-Profil bestimmt das genutzt Verfahren und die für die Aushandlung zur Auswahl stehenden Hash-Algorithmen.

Pfad

```
/Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles
```

Kommando

```
cd /Setup/VPN/IKEv2/Auth/Digital-Signature-Profiles
tab  Name                  Auth-Method        Hash-Algorithms
add  "DEFAULT-RSA-PSS"     RSASSA-PSS         SHA-512,SHA-384,SHA-256
add  "DEFAULT-RSA-PKCS"    RSASSA-PKCS1-v1_5  SHA-512,SHA-384,SHA-256
add  "DEFAULT-ECDSA"       ECDSA              SHA-512,SHA-384,SHA-256
add  "DEFAULT-EDDSA25519"  EdDSA25519         IDENTITY
add  "DEFAULT-EDDSA448"    EdDSA448           IDENTITY
cd /
```

Mögliche Einträge für Digital-Signature-Profiles

```
[1] Name            : 20 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                    (lower case characters are converted to upper case)
[2] Auth-Method     : RSASSA-PSS (1), RSASSA-PKCS1-v1_5 (2), ECDSA (4), EdDSA25519 (8), EdDSA448 (16)
[3] Hash-Algorithms : Bitmask: IDENTITY (16), SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8)
```

8.1.1 IKEv2-Verschlüsselung

LANCOM empfiehlt die Verwendung aktueller Diffie-Hellman-Gruppen (DH-Gruppen) für den sicheren Schlüsselaustausch. Für die Verschlüsselung und Integritätsprüfung sowohl der IKE_SA- als auch der Child_SA-Verbindungen sollten möglichst starke, moderne Algorithmen eingesetzt werden.

Pfad

```
/Setup/VPN/IKEv2/Encryption
```

Kommando

```
cd /Setup/VPN/IKEv2/Encryption
tab Name      DH-Groups                          PFS IKE-SA-Cipher-List      IKE-SA-Integ-Alg-List
add "DEFAULT" DH30,DH29,DH28,DH21,DH20,DH19,DH16 Yes AES-CBC-256,AES-GCM-256 SHA-512,SHA-384,SHA-256
tab Child-SA-Cipher-List    Child-SA-Integ-Alg-List
add AES-CBC-256,AES-GCM-256 SHA-512,SHA-384,SHA-256
cd /
```

Mögliche Einträge für Encryption

```
[1] Name                    : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                      (lower case characters are converted to upper case)
[2] DH-Groups               : Bitmask: DH32 (4096), DH31 (2048), DH30 (32), DH29 (64), DH28 (128),
                                       DH21 (256),DH20 (512), DH19 (1024), DH16 (1), DH15 (2), DH14 (4),
                                       DH5 (8), DH2 (16)
[3] PFS                     : No (0), Yes (1)
[4] IKE-SA-Cipher-List      : Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8),
                                       AES-GCM-256 (16), AES-GCM-192 (32), AES-GCM-128 (64),
                                       Chacha20-Poly1305 (128)
[5] IKE-SA-Integ-Alg-List   : Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)
[6] Child-SA-Cipher-List    : Bitmask: AES-CBC-256 (1), AES-CBC-192 (2), AES-CBC-128 (4), 3DES (8),
                                       AES-GCM-256 (16), AES-GCM-192 (32), AES-GCM-128 (64),
                                       Chacha20-Poly1305 (128), NULL (256)
[7] Child-SA-Integ-Alg-List : Bitmask: SHA-512 (1), SHA-384 (2), SHA-256 (4), SHA1 (8), MD5 (16)
```

Bei der Verwendung von Zertifikaten sollte auf eine angemessene Gültigkeitsdauer geachtet werden. Es wird empfohlen, ein automatisiertes Zertifikats-Rollout-Verfahren unter Verwendung des SCEP-Protokolls einzusetzen.

8.1.2 Zertifikatsverwaltung

LCOS ermöglicht die Verwaltung von Zertifikaten entweder manuell oder über einen automatisierten Zertifikats-Rollout. Der automatische Rollout erfolgt über das Protokoll SCEP (Simple Certificate Enrollment Protocol).

Zertifikate können initial sowie innerhalb eines definierten Zeitraums vor ihrem Ablauf automatisch vom Gerät abgerufen werden. Neben der automatischen Beantragung bietet SCEP insbesondere den Sicherheitsvorteil, dass der private Schlüssel direkt auf dem Gerät generiert wird und dieses niemals verlässt.

Der private Schlüssel wird in einem nicht auslesbaren Speicherbereich des Geräts abgelegt. In sicherheitskritischen Umgebungen sollte nach Möglichkeit das SCEP-Protokoll verwendet werden.

Pfad

```
/Setup/Certificates/SCEP-Client
```

Kommando

```
set /Setup/Certificates/SCEP-Client/SCEP-Operating Yes
```

Mögliche Einträge

```
SCEP-Operating : No (0), Yes (1)
```

Kommando

```
cd /Setup/Certificates/SCEP-Client/CAs
tab Name     URL                                        DN                                Enc-Alg Identifier
add "VPN_CA" "http://127.0.0.1/cgi-bin/pkiclient.exe" "/CN=SK CA/O=LANCOM SYSTEMS/C=DE" AES256  ""
tab RA-Autoapprove CA-Signature-Algorithm CA-Fingerprint-Algorithm CA-Fingerprint Loopback-Addr.
add Yes            SHA-256                SHA-256                 ""             ""
cd /
```

Mögliche Einträge

```
[ 1] Name                     : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                              9 (lower case characters are converted to upper case)
[ 2] URL                      : 251 chars from abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789
                                               /?.-;:@&=$_+!*'(),%
[ 3] DN                       : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01234
                                               56789abcdefghijklmnopqrstuvwxyz `
[ 4] Enc-Alg                  : DES (0), 3DES (1), BLOWFISH (2), AES128 (3), AES192 (4), AES256 (5)
[ 5] Identifier               : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01234
                                               56789abcdefghijklmnopqrstuvwxyz `
[ 7] RA-Autoapprove           : No (0), Yes (1)
[ 6] CA-Signature-Algorithm   : MD5 (0), SHA1 (1), SHA-256 (2), SHA-384 (3), SHA-512 (4)
[ 8] CA-Fingerprint-Algorithm : off (0), SHA1 (1), MD5 (2), SHA-256 (3), SHA-384 (4), SHA-512 (5)
[ 9] CA-Fingerprint           : 192 chars from 1234567890abcdef:-, (upper case characters are converted to
                                               lower case)
[11] Loopback-Addr.           : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345678
                                              9 (lower case characters are converted to upper case)
```

Kommando

```
cd /Setup/Certificates/SCEP-Client/Certificates
tab Name     CADN                                Subject      ChallengePwd SubjectAltName KeyUsage
add "VPN_CA" "/CN=VPN CA/O=LANCOM SYSTEMS/C=DE" "/CN=VPN_CA" "********"   ""            ""
tab Extended-KeyUsage                           Device-Certificate-Keylength Application
add "serverAuth, critical, 1.3.6.1.5.5.7.3.18" 4096                          VPN1
cd /
```

Mögliche Einträge

```
[1] Name                      : 16 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.012345
                                             6789 (lower case characters are converted to upper case)
[2] CADN                      : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                              23456789abcdefghijklmnopqrstuvwxyz `
[3] Subject                   : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                              23456789abcdefghijklmnopqrstuvwxyz `
[4] ChallengePwd              : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.012
                                              3456789abcdefghijklmnopqrstuvwxyz `
```

```
[5] SubjectAltName               : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[6] KeyUsage                     : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[9] Extended-KeyUsage            : 251 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!"$%&'()*+-,/:;<=>?[\]^_.01
                                                  23456789abcdefghijklmnopqrstuvwxyz `
[7] Device-Certificate-Keylength : 10 chars from 1234567890
[8] Application                  : VPN1 (0), VPN2 (5), VPN3 (6), VPN4 (7), VPN5 (8), VPN6 (9), VPN7 (10),
                                   VPN8 (11), VPN9 (12), WLan-Controller (1), EAP/TLS (3), Default (13),
                                   CA (14), ConfigSync (15), SYSLOG-PKCS12 (24), SYSLOG-CA (25),
                                   ProvSrv (17), OCSP (18), LBS (20), Wireless-ePaper (21), SCEP-TLS (22),
                                   RADSEC (23), WEBconfig (26), unconfigured (4294967295)
```

8.1.3 VPN-Regeln

Sowohl manuell als auch automatisch erzeugte VPN-Regeln müssen mit dem Befehl `show vpn` auf ihre Korrektheit überprüft werden.

```
> show vpn

VPN SPD and IKE configuration:

# of connections = 1

Rule #1          ikev2        0.0.0.0/0 ANY ANY <-> 0.0.0.0/0 ANY ANY
    Name:                       VPN-CONNECTION
    Unique Id:                  IPSEC-0-VPN-CONNECTION-PR0-L0-R0
    Local  Gateway:             IPV6_ADDR(any:0, 2001:4dd0:af17:8e5e:a0:57ff:fe9c:47fe)
    Remote Gateway:             IPV6_ADDR(any:0, 2003:cf:3fff:2243:a0:57ff:feff:9a44)
```

8.1.4 IPv4-Firewall-Strategie

Die IPv4-Firewall des LCOS verfolgt im Auslieferungszustand (Factory Default) eine „allow all"-Strategie. Um ein Höchstmaß an Datensicherheit beim Datenverkehr zu gewährleisten, sollte die Firewall-Strategie zunächst auf das restriktive „deny all"-Prinzip umgestellt werden.

Nur explizit erwünschte Datenkommunikation darf an den Übergängen zwischen vertrauenswürdigen (trusted) und nicht vertrauenswürdigen (untrusted) Netzwerken erlaubt werden.

Pfad

```
/Setup/IP-Router/Firewall/Rules
```

Kommando

```
cd /Setup/IP-Router/Firewall/Rules
tab Name      Prot. Source    Destination Action            Firewall
add "DENYALL" "ANY" "ANYHOST" "ANYHOST"   "%Lcds0 %R %Lcd0" Yes
cd /
```

Mögliche Einträge

```
[ 1] Name          : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[ 2] Prot.         : 10 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 3] Source        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 4] Destination   : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 7] Action        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[16] LB-Policy     : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[17] LB-Switchover : No (0), Yes (1)
[ 8] Linked        : No (0), Yes (1)
[ 9] Prio          : 4 chars from 1234567890
[10] Firewall-Rule : No (1), Yes (0)
[12] Stateful      : No (1), Yes (0)
[15] Src-Tag       : 5 chars from 1234567890
[14] Rtg-tag       : 5 chars from 1234567890
```

```
[13] Comment       : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefgh
                                   ijklmnopqrstuvwxyz
```

8.1.5 IPv6-Firewall-Strategie

Die IPv6-Firewall des LCOS verfolgt im Auslieferungszustand (Factory Default) eine „deny all"-Strategie, um ein Höchstmaß an Datensicherheit beim Datenverkehr zu gewährleisten.

Nur ausdrücklich gewünschte Datenkommunikation darf an den Übergängen zwischen vertrauenswürdigen (trusted) und nicht vertrauenswürdigen (untrusted) Netzwerken zugelassen werden.

Pfad

```
/Setup/IPv6/Firewall/Forwarding-Rules
```

Kommando

```
cd /Setup/IPv6/Firewall/Forwarding-Rules
tab Name      Action        Services Source-Stations
add "DENYALL" "REJECT-SNMP" "ANY"    "ANYHOST"
cd /
```

Mögliche Einträge

```
[ 1] Name                : 36 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 5] Action              : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 7] Services            : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 8] Source-Stations     : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 9] Destination-Stations : 64 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[12] LB-Policy           : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789
                                         (lower case characters are converted to upper case)
[ 2] Flags               : Bitmask: none (0), deactivated (1), linked (4), stateless (8), LB-Switchover (16)
[ 3] Prio                : 4 chars from 1234567890
[11] Src-Tag             : 5 chars from 1234567890
[ 4] Rtg-tag             : 5 chars from 1234567890
[10] Comment             : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789a
                                         bcdefghijklmnopqrstuvwxyz `
```

8.1.6 Firewall Session Management, IDS und DoS

Die LCOS-Firewall arbeitet als Stateful Inspection Firewall. Um potenzielle Angriffe über zugelassene Protokolle zu verhindern, sollten Firewall-Regeln grundsätzlich zustandsbehaftet (stateful) definiert sein.

Darüber hinaus analysiert LCOS den aktuellen Zustand von IP-Verbindungen, um Portscans und Denial-of-Service-Angriffe (DoS) zu erkennen und zu blockieren. Damit dieser Schutz wirksam ist, müssen die Aktionen der IDS- und DoS-Module auf „Zurückweisen" oder „Verwerfen" konfiguriert sein.

Die jeweiligen Schwellenwerte sind an die spezifische Netzwerkumgebung anzupassen.

Pfad

```
/Setup/IP-Router/Firewall
/Setup/IP-Router/Firewall/Rules
```

Kommando

```
set /Setup/IP-Router/Firewall/Max.-Half-Open-Conns. 100
```

Mögliche Einträge

```
Max.-Half-Open-Conns. : 4 chars from: 1234567890
```

Kommando

```
set /Setup/IP-Router/Firewall/DoS-Action "%d%n"
```

Mögliche Einträge

```
DoS-Action : 29 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopq
                           rstuvwxyz`
```

Kommando

```
set /Setup/IP-Router/Firewall/Port-Scan-Threshold 50
```

Mögliche Einträge

```
Port-Scan-Threshold : 4 chars from: 1234567890
```

Kommando

```
set /Setup/IP-Router/Firewall/IDS-Action "%d%n"
```

Mögliche Einträge

```
IDS-Action : 29 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefghijklmnopq
                           rstuvwxyz`
```

Kommando

```
cd /Setup/IP-Router/Firewall/Rules
tab Name        Prot. Source Destination Action LB-Policy LB-Switchover Linked Prio Firewall-Rule Stateful
add "ALLOW-XYZ" ""    ""     ""          "%A"   ""        No            No     0    Yes           Yes
tab Src-Tag Rtg-tag Comment
add 0       0       ""
cd /
```

Mögliche Einträge

```
[ 1] Name          : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[ 2] Prot.         : 10 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 3] Source        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 4] Destination   : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[ 7] Action        : 40 chars from  #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789abcdefgh
                                    ijklmnopqrstuvwxyz`
[16] LB-Policy     : 32 chars from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()+-,/:;<=>?[\]^_.0123456789 (lower
                                   case characters are converted to upper case)
[17] LB-Switchover : No (0), Yes (1)
[ 8] Linked        : No (0), Yes (1)
[ 9] Prio          : 4 chars from 1234567890
[10] Firewall-Rule : No (1), Yes (0)
[12] Stateful      : No (1), Yes (0)
[15] Src-Tag       : 5 chars from 1234567890
[14] Rtg-tag       : 5 chars from 1234567890
[13] Comment       : 64 chars from #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{|}~!$%&'()*+-,/:;<=>?[\]^_.0123456789abcdefgh
                                   ijklmnopqrstuvwxyz `
```

Als Aktionen stehen die folgenden grundlegenden Parameter zur Verfügung:

```
ACCEPT %A
DROP   %D
REJECT %R
```

Die effektiv vom Router ausgewerteten Firewall-Regeln sind mit den folgenden Hilfsmitteln zu kontrollieren:

Kommando

```
show filter

Filter 0001 from Rule DENYALL:
  Protocol: 0
  Src: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
```

```
Dst: 00:00:00:00:00:00 0.0.0.0 0.0.0.0 0-0
use routing tag 0000
Limit per conn.: after transmitting or receiving of 0 kilobits per second
actions after exceeding the limit:
    reject
Limit per conn.: after transmitting or receiving of 0 kilobits
actions after exceeding the limit:
    accept
```

In den Statusinformationen der Firewall lässt sich die korrekte Funktionsweise der Filterregeln überprüfen. Dazu sollten gezielt die gewünschten IP-Verbindungen aufgebaut werden. Die Übersicht der offenen IP-Verbindungen in der Firewall zeigt, welche Firewall-Regel auf die jeweilige Verbindung angewendet wurde.

Pfad

```
/Status/IP-Router/Connection-List
```

Um zu verhindern, dass etablierte IP-Verbindungen missbräuchlich weiterverwendet werden, entfernt das LCOS die entsprechenden Einträge aus der Verbindungsliste nach dem regulären Verbindungsabschluss oder nach Ablauf eines definierten Leerlauf-Timeouts. Eine IP-Verbindung muss anschließend gemäß Standard neu aufgebaut werden.

Die Timeouts können über die folgenden Einstellungen an die jeweiligen Applikationen angepasst werden.

Zur Vermeidung von Angriffen durch nicht standardkonform fragmentierte Pakete sollten IP-Fragmentierungen vom LCOS korrekt reassembliert werden.

Pfad

```
/Setup/IP-Router/1-N-NAT
```

Kommando

```
set /Setup/IP-Router/1-N-NAT/TCP-Aging-Seconds 300
set /Setup/IP-Router/1-N-NAT/UDP-Aging-Seconds 120
set /Setup/IP-Router/1-N-NAT/ICMP-Aging-Seconds 10
set /Setup/IP-Router/1-N-NAT/Fragments Reassemble
set /Setup/IP-Router/1-N-NAT/Fragment-Aging-Seconds 5
set /Setup/IP-Router/1-N-NAT/IPSec-Aging-Seconds 2000
```

In den Statusinformationen der Firewall lässt sich die korrekte Funktionsweise der Filterregeln nachvollziehen. Dazu müssen die entsprechenden IP-Verbindungen hergestellt werden. Die Übersicht der aktiven IP-Verbindungen zeigt an, welche Firewall-Regel auf die jeweilige Verbindung angewendet wurde.

Mögliche Einträge

```
TCP-Aging-Seconds      : 5 chars from: 1234567890
UDP-Aging-Seconds      : 5 chars from: 1234567890
ICMP-Aging-Seconds     : 5 chars from: 1234567890
Fragments              : Filter (0), Route (1), Reassemble (2)
Fragment-Aging-Seconds : 3 chars from: 1234567890
IPSec-Aging-Seconds    : 5 chars from: 1234567890
IPSec-Table            : try 'set IPSec-Table ?'
```