



Addendum LCOS 8.80 RC2



Contents

1 Addendum to LCOS version 8.80 RC2.....	7
2 Configuration.....	8
2.1 Tab command when scripting.....	8
2.2 Setting the device time from GPS.....	9
2.2.1 Additions to the menu system.....	10
3 LCOS.....	12
3.1 Configurable SSH algorithms.....	12
3.1.1 Additions to the Setup menu.....	12
3.1.2 Enhancements to LANconfig.....	17
3.2 File transfer via SCP.....	17
3.3 Displaying status information from the DHCP server.....	20
4 LLDP.....	22
4.1 How it works.....	22
4.2 Structure of LLDP messages.....	23
4.3 Supported operating systems.....	24
4.4 Additions to the menu system.....	25
4.4.1 Additions to the Setup menu.....	25
5 IPv6.....	33
5.1 IPv6 basics.....	33
5.1.1 Why use IPv6-standard IP addresses?.....	33
5.1.2 IP address structure according to the IPv6 standard.....	33
5.1.3 Stages of migration.....	34
5.2 IPv6 tunneling technologies.....	34
5.2.1 6in4 tunneling.....	34
5.2.2 6rd tunneling.....	35
5.2.3 6to4 tunneling.....	35
5.3 DHCPv6.....	36
5.3.1 DHCPv6 server.....	36
5.3.2 DHCPv6 client.....	36
5.4 IPv4 VPN tunnel via IPv6.....	36
5.4 Setup Wizard – Setting up an IPv4 VPN connection via IPv6.....	37
5.5 IPv6 firewall.....	38
5.5.1 Function.....	38
5.5.2 Configuration.....	38
5.5.3 IPv6 firewall table.....	38
5.6 Additions to the Setup menu.....	40
5.6.1 Tunnel.....	40
5.6.2 Router advertisement.....	51
5.6.3 DHCPv6.....	61
5.6.4 Relay agent.....	75

5.6.5 Network.....	77
5.6.6 Firewall.....	81
5.6.7 LAN interfaces.....	103
5.6.8 WAN interfaces.....	107
5.6.9 Operating.....	110
5.6.10 Forwarding.....	110
5.6.11 Router.....	110
5.6.12 IPv6 address.....	113
5.7 Additions to the Status menu.....	113
5.7.1 Log table.....	113
5.8 Additional command-line commands.....	114
5.8.1 IPv6 addresses.....	114
5.8.2 IPv6 prefixes.....	115
5.8.3 IPv6 interfaces.....	115
5.8.4 IPv6 neighbor cache.....	116
5.8.5 IPv6 DHCP server.....	117
5.8.6 IPv6 DHCP client.....	117
5.8.7 IPv6 route.....	117
5.8.8 Release IPv6 address.....	117
5.9 Enhancements to LANconfig.....	118
5.9.1 IPv6 configuration menu.....	118
5.9.2 Settings in the PPP list.....	130
5.9.3 IP routing tables.....	130
5.9.4 Separate views for the IPv4 and IPv6 firewalls.....	132
5.9.5 IPv6 DNS hosts in the DNS list	132
5.9.6 Configuring the IPv6 firewall rules.....	132
5.10 Tutorials.....	143
5.10.1 Setting up IPv6 Internet access.....	143
5.10.2 Setting up a 6to4 tunnel.....	152
6 WLAN.....	159
6.1 Closed-network function: Suppress SSID broadcast.....	159
6.1.1 Additions to the menu system.....	160
6.1.2 Enhancements to LANconfig.....	162
6.2 New parameter for WLAN-client signal strength.....	163
6.2.1 Additions to the menu system.....	163
6.3 Spectral scan.....	164
6.3.1 Functions of the software module.....	164
6.3.2 Spectral scan analysis window.....	167
6.3.3 Enhancements to LANmonitor.....	169
6.3.4 Additions to the Setup menu.....	171
6.4 WLAN band steering.....	174
6.4.1 Enhancements to LANconfig.....	175
6.4.2 Additions to the Setup menu.....	176
6.4.3 Additions to the Status menu.....	177

6.5 STBC / LDPC.....	178
6.5.1 Basics.....	178
6.5.2 Additions to the Setup menu.....	178
6.5.3 Additions to the Status menu.....	179
6.6 LANCOM-specific UUID information element for access points.....	183
6.6.1 UUID info element for LANCOM WLAN access points.....	183
6.7 DFS.....	184
6.7.1 DFS4.....	184
6.7.2 Function and the history of development.....	184
6.8 PMK caching in the WLAN client mode.....	185
6.8.1 Additions to the Setup menu.....	185
6.8.2 Additions to the Status menu.....	186
6.9 Pre-authentication in WLAN-client mode.....	188
6.9.1 Additions to the Setup menu.....	189
6.10 Time-staggered roaming for dual-radio client WLAN modules.....	189
6.10.1 Additions to the menu system.....	189
6.10.2 Enhancements to LANconfig.....	190
6.11 Greenfield mode for access points with IEEE 802.11n.....	191
6.12 Separate RADIUS server for each SSID.....	191
6.12.1 Additions to the menu system.....	191
6.12.2 Enhancements to LANconfig.....	195
7 Public Spot.....	197
7.1 Managing Public Spot users via the web API.....	197
7.1.1 Adding a Public Spot user.....	197
7.2 Public Spot user administration.....	198
7.2.1 Adding new Public Spot users with a single click.....	199
7.3 Set case-sensitive for user names.....	199
7.3.1 RADIUS server.....	199
7.3.2 Public Spot Wizard.....	200
7.3.3 Additions to the Setup menu.....	201
7.4 Delegation of user account creation for Public Spots.....	202
7.4.1 Additions to the Setup menu.....	202
7.4.2 Enhancements to LANconfig.....	209
7.5 DNS snooping.....	211
7.5.1 Additions to the Setup menu.....	212
7.5.2 Additions to the Status menu.....	212
7.6 XML interface.....	213
7.6 Function.....	213
7.6 Setting up the XML interface via WEBconfig.....	214
7.6 Analyzing the XML interface using cURL.....	215
7.6.1 Commands.....	216
7.6.2 Additions to the Setup menu.....	220
7.7 Multiple logins.....	221
7.7.1 Enabling multiple logins in the Public Spot Wizard.....	221

7.7.2 Additions to the Setup menu.....	222
7.8 Wizard for basic Public Spot configuration.....	222
7.8.1 Basic settings.....	222
7.8.2 Tutorials for setting up and using Public Spots.....	223
7.9 Distinct function rights.....	226
7.9.1 Additions to the Setup menu.....	226
7.9.2 Enhancements to LANconfig.....	227
7.10 Additions to the Setup menu.....	227
7.10.1 Free networks.....	227
8 Routing and WAN connections.....	229
8.1 Default mode in the DSLoL interface.....	229
8.1.1 Additions to the Setup menu.....	229
9 Diagnosis.....	230
9.1 SYSLOG accounting is disabled by default.....	230
9.2 Boot-persistent SYSLOG, event log and boot log.....	230
9.2.1 Additions to the Setup menu.....	230
9.2.2 Enhancements to command-line commands	232
9.2.3 Enhancements to LANconfig.....	232
9.3 Logging configuration changes made via the command line.....	232
9.3.1 Additions to the Setup menu.....	233
9.3.2 Enhancements to LANconfig.....	233
9.4 SYSLOG: Change to the default order.....	234
9.4.1 Additions to the Setup menu.....	234
9.4.2 Enhancements to LANconfig.....	235
9.5 Packet capturing.....	235
9.5.1 Enhancements to WEBconfig.....	236
9.6 Trace output for the XML interface.....	236
9.7 Ping command for IPv6.....	237
10 LCMS.....	238
10.1 Enhancements to LANconfig.....	238
10.1.1 Creating a password in LANconfig.....	238
10.1.2 Internal browser in LANconfig.....	239
10.2 Setting the SNMP read-only community 'Public'.....	243
10.3 Enhancements to LANmonitor.....	244
10.3.1 Display local IPv6 addresses.....	244
10.3.2 Displaying PBX lines in the SIP ALG.....	245
10.3.3 Displaying the active Ethernet ports.....	245
10.3.4 Delete all VPN connection failures.....	245
10.3.5 Display of the GPS time.....	246
11 Virtual Private Networks - VPN.....	247
11.1 Deleting all VPN errors with one command.....	247
11.1.1 Additions to the menu system.....	247
11.2 Default proposals for IKE and IPSec.....	247
11.3 Selecting DH group 14 for VPN connections.....	247

11.3.1 Additions to the Setup menu.....	247
11.4 Replay detection	249
11.4.1 Additions to the menu system.....	250
11.5 myVPN.....	250
11.5 Using the Setup Wizard in LANconfig to set up a VPN profile for the LANCOM myVPN app.....	250
11.5 Retrieve the VPN profile with the LANCOM myVPN app.....	253
11.5 Opening and closing the VPN connection on the iOS device.....	260
11.5 Deleting a VPN profile from the iOS device.....	261
11.5.1 Enhancements to LANconfig.....	262
11.5.2 Additions to the menu system.....	263
12 Voice over IP - VoIP.....	269
12.1 Default setting for WAN registration of a SIP user.....	269
12.1.1 Additions to the menu system.....	269
13 LANCOM Content Filter.....	270
13.1 Concurrent user model in the content filter.....	270
13.1.1 General settings.....	270
13.2 New content filter category, Command/Control Server.....	272
13.2.1 Introduction	272
13.3 Additions to the menu system.....	273
13.3.1 Command/Control server	273

1 Addendum to LCOS version 8.80 RC2

The document describes the new functions and changes to LCOS version 8.80 over the previous version.

2 Configuration

2.1 Tab command when scripting

When working with scripts, the `tab` command enables the desired columns for the subsequent `set` command.

When you perform the configuration with a command line tool, you generally supplement the `set` command with the values for the columns of the table.

For example, you set the values for the performance settings of a WLAN interface as follows:

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

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

> set WLAN-1 Yes *
```

In this example the Performance table has three columns:

- Ifc, the desired interface
- Enable or disable QoS
- The desired value for TX bursting

With the command `set WLAN-1 Yes *` you enable the QoS function for WLAN-1, and you leave the value for TX bursting unchanged with the asterisk (*).

Working with the `set` command in this way is adequate for tables with only a few columns. However, tables with many columns can pose a major challenge. For example, the table under **Setup > Interfaces > WLAN > Transmission** contains 22 entries:

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

Possible Entries for columns in Transmission:
[1][Ifc]                : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17),
WLAN-1-4 (18), WLAN-1-5 (19), WLAN-1-6 (20), WLAN-1-7 (21), WLAN-1-8
(22)
[2][Packet-Size]       : 5 Chars from: 1234567890
[3][Min-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6),
6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M
(15)
[9][Max-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6),
6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M
(15)
[4][Basic-Rate]        : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M
(9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[19][EAPOL-Rate]       : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M
(6), 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14),
54M (15), HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),
HT-1-26M (31), HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M
(35), HT-2-13M (36), HT-2-26M (37), HT-2-39M (38), HT-2-52M (39), HT-2-78M
(40), HT-2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]    : 3 Chars from: 1234567890
```



```
[11][Soft-Retries]      : 3 Chars from: 1234567890
[7][11b-Preamble]     : Auto (0), Long (1)
[16][Min-HT-MCS]      : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10
(3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15
(8)
[17][Max-HT-MCS]      : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10
(3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15
(8)
[23][Use-STBC]        : No (0), Yes (1)
[24][Use-LDPC]        : No (0), Yes (1)
[13][Short-Guard-Interval] : Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates] : No (0), Yes (1)
[22][Receive-Aggregates] : No (0), Yes (1)
[20][Max-Aggr.-Packet-Count] : 2 Chars from: 1234567890
[6][RTS-Threshold]    : 5 Chars from: 1234567890
[10][Min-Frag-Len]    : 5 Chars from: 1234567890
[21][ProbeRsp-Retries] : 3 Chars from: 1234567890
```

Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

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

! The asterisks for the values after the column for the short guard interval are unnecessary in this example, as the columns will be ignored when setting the new values.

As an alternative to this rather confusing and error-prone notation, you can use the `tab` command as the first step to determine which columns are changed with the subsequent `set` command:

```
> tab Ifc short guard-Interval
> set WLAN-1-3 No
```

The `tab` command also makes it possible to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for `Use-LDPC` to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
> tab Ifc short guard-Interval Use-LDPC
> set WLAN-1-3 No Yes
```

! The tables may only contain only a selection of the columns, depending on the hardware model. The `tab` command ignores columns which do not exist for that device. This gives you the option to develop unified scripts for different hardware models. The `tab` instructions in the scripts reference the maximum number of required columns. Depending on the model, the script only performs the `set` instructions for the existing columns.

2.2 Setting the device time from GPS

From LCOS 8.80, you have the option of retrieving the time for the device via GPS automatically as an alternative to an NTP server or ISDN. Prerequisites for the obtaining the device time from GPS are:

- The operating mode of the 3G/4G modem is set to WWAN ([2.23.7.2 Operating](#))
- The GPS module is enabled ([2.40.1 Operating](#))
- The Fetch method for the device time is set to GPS ([2.14.1 Fetch method](#))

The current GPS time is to be found in LANmonitor ([Display of GPS time](#)) or the device status area ([1.63.3 Timestamp \(GPS\)](#)).

- ⓘ This feature is available only on devices with internal WWAN module from Sierra. Please check the specifications for your model to see whether your device supports this function.
- ⓘ The retrieval of GPS time requires an active SIM card in the device. The time is only available once the device has successfully gained a GPS fix. This requires the connection to at least four satellites in sufficient quality.
- ⓘ The time received from GPS may differ by a few seconds from the actual time due to run-time variations and the non-observance of leap seconds in the GPS network.

2.2.1 Additions to the menu system

Additions to the Setup menu

Fetch method

Select here if and how the device synchronizes its internal real-time clock.

SNMP ID: 2.14.1

Telnet path: /Setup/Time

Possible values:

- None
- ISDN
- NTP
- GPS

Default: NTP

Operating

Select the operating mode for the interface.

Telnet path: LCOS Menu Tree/Setup/Interfaces/Mobile/Operating

Possible values:

- No
- modem
- UMTS-GPRS
- WWAN

Default: No

Operating

Activate or deactivate the GPS function here. You can activate the GPS module independently of the location verification function, for example to monitor the current positional coordinates with LANmonitor.

SNMP ID: 2.40.1

Telnet path: /Setup/GPS/Operating

Possible values:

- No
- Yes

Default: No

Additions to the Status menu

Timestamp (GPS)

This entry shows the time that was last received from the GPS network.

SNMP ID:

1.63.3

Telnet path:

Status > GPS

3 LCOS

3.1 Configurable SSH algorithms

The SSH implementation in the operating system of your device supports numerous cryptographic methods (algorithms). The devices can optionally restrict the choice of cryptographic methods to the algorithms of your preference.

3.1.1 Additions to the Setup menu

SSH

This item manages the mechanisms used for SSH encryption. You can select which algorithms are supported in both server and client mode.

SNMP ID:

2.11.28

Telnet path:**Setup > Config**

Cipher algorithms

The cipher algorithms are used for encrypting and decrypting data. Select one or more of the available algorithms.

SNMP ID:

2.11.28.1

Telnet path:**Setup > Config > SSH****Possible values:**

3DES-cbc

3DES-ctr

arcfour

arcfour128

arcfour256

blowfish-cbc

blowfish-ctr

aes128-cbc

aes192-cbc

aes256-cbc

aes128-ctr

aes192-ctr

aes256-ctr

Default:

3des-cbc,3des-ctr,arcfour,arcfour128,arcfour256,blowfish-cbc,blowfish-ctr,aes128-cbc,
aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr

MAC algorithms

MAC algorithms are used to check the integrity of messages. Select one or more of the available algorithms.

SNMP ID:

2.11.28.2

Telnet path:

Setup > Config > SSH

Possible values:

hmac-md5-96
hmac-md5
hmac-sha1-96
hmac-sha1
hmac-sha2-256-96
hmac-sha2-256
hmac-sha2-512-96
hmac-sha2-512

Default:

hmac-md5-96,hmac-md5,hmac-sha1-96,hmac-sha1,hmac-sha2-256-96,
hmac-sha2-256,hmac-sha2-512-96,hmac-sha2-512

Key exchange algorithms

The MAC key exchange algorithms are used to negotiate the key algorithm. Select one or more of the available algorithms.

SNMP ID:

2.11.28.3

Telnet path:

Setup > Config > SSH

Possible values:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256

Default:

diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256

Host key algorithms

The host key algorithms are used to authenticate hosts. Select one or more of the available algorithms.

SNMP ID:

2.11.28.4

Telnet path:

Setup > Config > SSH

Possible values:

ssh-rsa
ssh-dss

Default:

ssh-rsa,ssh-dss

Min host key length

This parameter defines the minimum length of your host keys.

SNMP ID:

2.11.28.5

Telnet path:

Setup > Config > SSH

Possible values:

Max. 5 numbers

Default:

512

Max host key length

This parameter defines the maximum length of your host keys.

SNMP ID:

2.11.28.6

Telnet path:

Setup > Config > SSH

Possible values:

Max. 5 numbers

Default:

8192

DH groups

The Diffie-Hellman groups are used for the key exchange. Select one or more of the available groups.

SNMP ID:

2.11.28.7

Telnet path:

Setup > Config > SSH

Possible values:

Group 1
Group 5
Group 14
Group 15

Group 16

Default:

Group 1, group 5, group 14

VPN

This menu contains the configuration of the Virtual Private Network (VPN).

SNMP ID: 2.19

Telnet path: /Setup

Aggressive mode IKE group default

This IKE group is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID: 2.19.11

Telnet path: /Setup/VPN

Possible values:

- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

Main mode IKE group default

This IKE group is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID: 2.19.14

Telnet path: /Setup/VPN

Possible values:

- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

Quick mode PFS group default

This IPsec group is used for simplified dial-in with certificates.

SNMP ID: 2.19.20

Telnet path: /Setup/VPN

Possible values:

- 0: No PFS
- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536

3 LCOS

- 14: MODP-2048

Default: MODP-1024

Layer

Define other parameters for the individual VPN connections here.

SNMP ID: 2.19.7

Telnet path: /Setup/VPN

PFS group

Perfect Forward Secrecy (PFS) is a security feature of encryption algorithms. The PFS group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID: 2.19.7.3

Telnet path: /Setup/VPN/Layer

Possible values:

- 0: No PFS
- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

IKE group

The IKE group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID: 2.19.7.4

Telnet path: /Setup/VPN/Layer

Possible values:

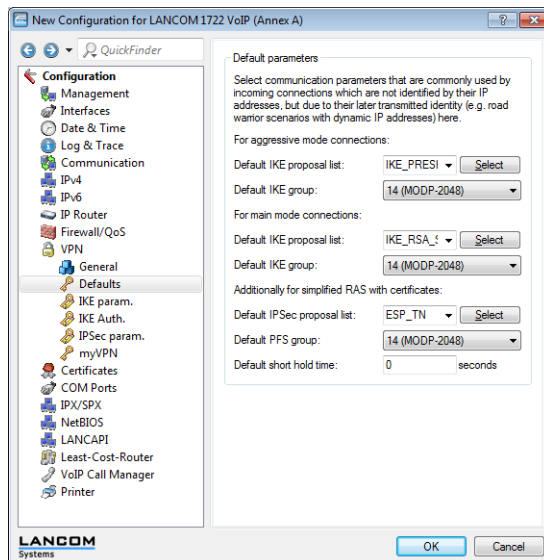
- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

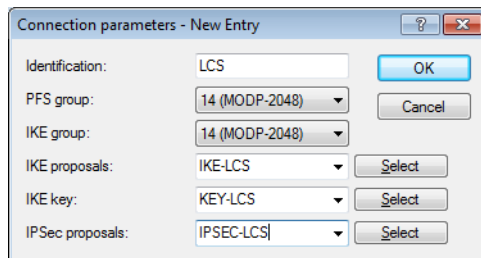
3.1.2 Enhancements to LANconfig

Selecting the IKE group in LANconfig

In LANconfig, the settings for the default IKE groups are located under **VPN > Defaults**:



In LANconfig, the settings for the default IKE groups for VPN connections are located under **VPN > General > Connection parameters**:



3.2 File transfer via SCP

SCP (Secure Copy) is a protocol for the secure transfer of data between two computers in a network. Administrators often use SCP to exchange data between servers or between servers and workstations. With a suitable tool (for example, the Putty add-on pscp.exe on Windows operating systems) you can also exchange data between your PC/notebook and a LANCOM device.

Download pscp.exe from the Putty download page to perform file transfer from a Windows operating system.

Then open a command line window using the command `cmd`.

Change to the directory where you have saved the file pscp.exe and run the following command to transfer a file from your Windows computer to the device. Enter the options `-scp` and `-pw` followed by your password:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw ***** c:\path\myfile.ext
<User>@<IP-address>:target
```

Change the order of the source and destination, to transfer the file from the device to your computer:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw *****
<User>@<IP-address>:target c:\path\myfile.ext
```

Enter the following command to save the configuration from the device to a file named `config.lcs` on your computer:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw *****
root@123.123.123.123:config c:\config.lcs
```

To upload a new firmware file from your computer to the device, enter the following command:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw ***** c:\firmware.upx
root@123.123.123.123:firmware
```

The following table specifically shows which files you can read via SCP from the device and which ones you can write to it:

Table 1: Files for the SCP file transfer

Target	Read	Write	Description
ssl_cert	Yes	Yes	SSL – certificate (*.pem, *.crt, *.cer [BASE64])
ssl_privkey		Yes	SSL – private key (*.key [BASE64 unencrypted])
ssl_rootcert	Yes	Yes	SSL – root CA certificate (*.pem, *.crt, *.cer [BASE64])
ssl_pkcs12		Yes	SSL – container as PKCS#12 file (*.pfx, *.p12)
ssh_rsakey		Yes	SSL – RSA key (*.key [BASE64 unencrypted])
ssh_dsakey		Yes	SSL – DSA key (*.key [BASE64 unencrypted])
ssh_authkeys		Yes	SSH – accepted public key
vpn_rootcert	Yes	Yes	VPN – root CA certificate (*.pem, *.crt, *.cer [BASE64])
vpn_devcert	Yes	Yes	VPN – device certificate (*.pem, *.crt, *.cer [BASE64])
vpn_devprivkey		Yes	SSL – private device key (*.key [BASE64 unencrypted])
vpn_pkcs12		Yes	VPN – container (VPN1) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_2		Yes	VPN – container (VPN2) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_3		Yes	VPN – container (VPN3) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_4		Yes	VPN – container (VPN4) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_5		Yes	VPN – container (VPN5) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_6		Yes	VPN – container (VPN6) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_7		Yes	VPN – container (VPN7) as PKCS#12 file (*.pfx, *.p12)

Target	Read	Write	Description
vpn_pkcs12_8		Yes	VPN – container (VPN8) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_9		Yes	VPN – container (VPN9) as PKCS#12 file (*.pfx, *.p12)
vpn_add_cas		Yes	VPN - add additional CA certificates (*.pfx, *.p12, *.pem, *.crt, *.cer [BASE64])
eaptls_rootcert	Yes	Yes	EAP/TLS – root CA certificate (*.pem, *.crt, *.cer [BASE64])
eaptls_devcert	Yes	Yes	EAP/TLS – device certificate (*.pem, *.crt, *.cer [BASE64])
eaptls_privkey		Yes	EAP/TLS – private device key (*.key [BASE64 unencrypted])
eaptls_pkcs12		Yes	EAP/TLS – container as PKCS#12 file (*.pfx, *.p12)
radsec_rootcert	Yes	Yes	RADSEC – root CA certificate (*.pem, *.crt, *.cer [BASE64])
radsec_devcert	Yes	Yes	RADSEC – device certificate (*.pem, *.crt, *.cer [BASE64])
radsec_privkey		Yes	RADSEC – private device key (*.key [BASE64 unencrypted])
radsec_pkcs12		Yes	RADSEC – container as PKCS#12 file (*.pfx, *.p12)
radius_accnt_total	Yes	Yes	RADIUS server – summary accounting (*.csv)
scep_cert_list	Yes	Yes	SCEP-CA – certificate list
scep_cert_serial	Yes	Yes	SCEP-CA – serial number
scep_ca_backup	Yes		Backup for SCEP-CA – PKCS12 container
scep_ra_backup	Yes		Backup for SCEP-CA – PKCS12 container
scep_ca_pkcs12		Yes	SCEP-CA – PKCS12 container
scep_ra_pkcs12		Yes	SCEP-CA – PKCS12 container
pbspot_template_welcome	Yes	Yes	Public Spot – welcome page (*.html, *.htm)
pbspot_template_login	Yes	Yes	Public Spot – login page (*.html, *.htm)
pbspot_template_error	Yes	Yes	Public Spot – error page (*.html, *.htm)
pbspot_template_start	Yes	Yes	Public Spot – home page (*.html, *.htm)
pbspot_template_status	Yes	Yes	Public Spot – status page (*.html, *.htm)
pbspot_template_logoff	Yes	Yes	Public Spot – logoff page (*.html, *.htm)

3 LCOS

Target	Read	Write	Description
pbspot_template_help	Yes	Yes	Public Spot – help page (*.html, *.htm)
pbspot_template_noproxy	Yes	Yes	Public Spot – no proxy page (*.html, *.htm)
pbspot_template_voucher	Yes	Yes	Public Spot – voucher page (*.html, *.htm)
pbspot_template_agb	Yes	Yes	Public Spot – GTC page (*.html, *.htm)
pbspot_formhdrimg	Yes	Yes	Public Spot – header image pages (*.gif, *.png, *.jpeg)
WLC_Script_1.lcs	Yes	Yes	CAPWAP – WLC_Script_1.lcs
WLC_Script_2.lcs	Yes	Yes	CAPWAP – WLC_Script_2.lcs
WLC_Script_3.lcs	Yes	Yes	CAPWAP – WLC_Script_3.lcs
default_pkcs12		Yes	
rollout_wizard		Yes	
rollout_template		Yes	
rollout_logo		Yes	
hip_cert_0		Yes	
issue	Yes	Yes	Text for display after command-line login (e.g. ASCII logos)
config	Yes	Yes	Device configuration
firmware		Yes	Firmware update

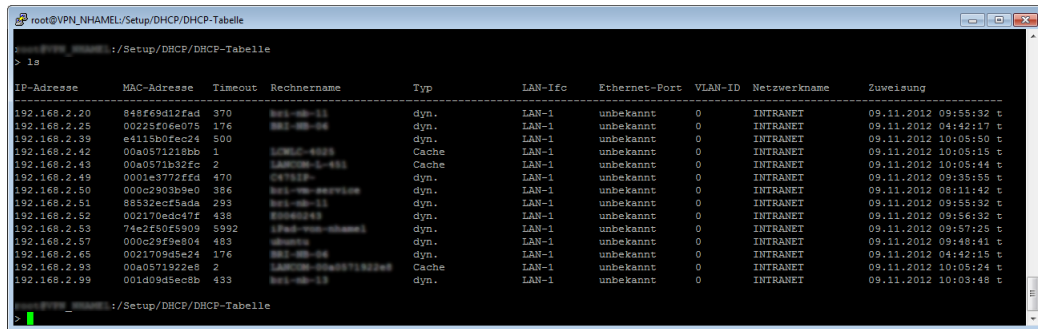
3.3 Displaying status information from the DHCP server

The status table of the DHCP server shows the following information about the devices that to which the DHCP server has assigned IP addresses:

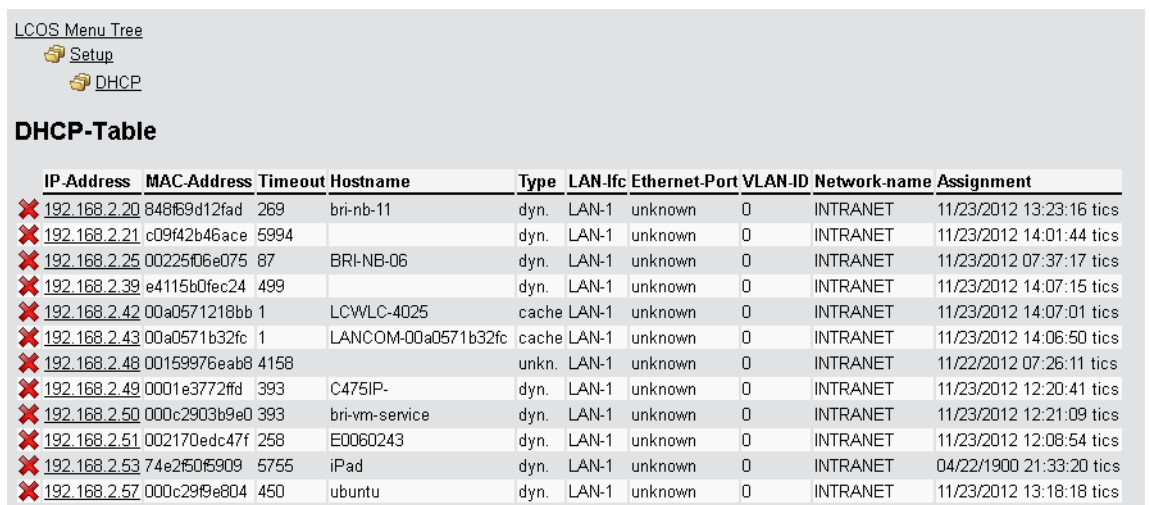
- IP address, which the DHCP server has assigned to the network device
- MAC address of the network device
- Timeout, remaining validity period in minutes
- Computer name
- Type of address assignment, dynamic or from cache
- LAN-Ifc, logical interface over which the DHCP server assigned the IP address to the network device
- Ethernet port, physical interface over which the DHCP server assigned the IP address to the network device
- VLAN ID of the network
- Network name
- Assignment, date and time when the DHCP server assigned the IP address to the network device

You can find the status information for the DHCP server at the following locations:

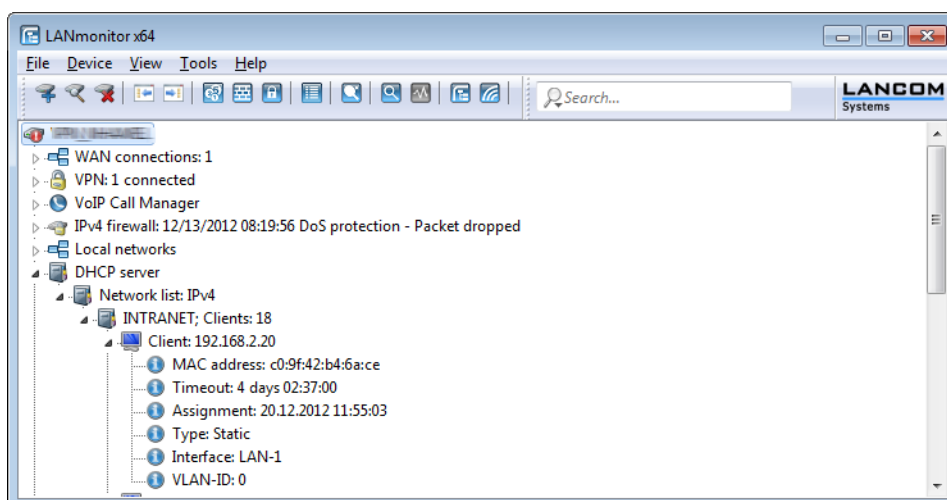
- Telnet: /Setup/DHCP/DHCP-Table



- WEBconfig: /Setup/DHCP/DHCP-Table



- LANmonitor: Broken down by network name under DHCP-server > Network list



4 LLDP

The Link Layer Discovery Protocol (LLDP) provides a simple and reliable way to exchange information between neighboring devices on the network and for determining the topology of networks. LLDP provides discovery functions to identify individual devices and entire network structures using the procedures defined in the IEEE 802.1AB standard. Since the protocol works on Layer 2 (security level) of the OSI layer model and it is, therefore, used for physically addressing devices, its functionality is not limited to logical networks such as IP networks. In principle, LLDP covers all physically accessible devices on the network.

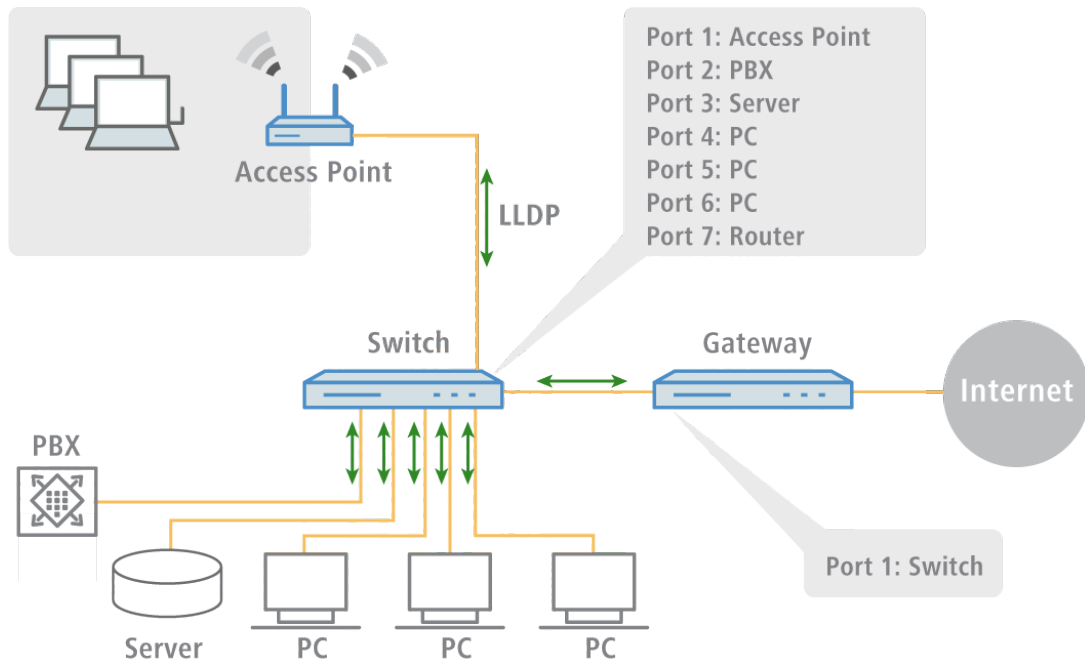
In particular, the vendor-independent LLDP protocol offers many advantages in complex networks:

- It enables the automatic detection of components attached to a network such as routers, switches, and WLAN access points.
- It simplifies the integration of a wide range of different devices, which support the LLDP standard, into an existing network: Using central network management software, and automatic testing and diagnostic processes, the time required for setup, operation and maintenance of a network is reduced.
- The information sent by the individual devices provides an overview of the topology (i.e., structure and arrangement) of the entire network. Central management software provides the administrator with a virtual image of the network, which is automatically updated when there are changes in the topology.
- With the help of management software, the administrator can also easily monitor and manage complex networks. Using this software, he can determine which components and devices are interconnected and can easily locate any faults.
- LLDP can reduce the costs of buying, building or restructuring a network, since companies are no longer dependent on specific manufacturers because of this open standard. Individual network components can be selected based on which one is best for your implementation. This was previously not possible when proprietary protocols were in use.

4.1 How it works

LLDP works on a simple principle: The so-called LLDP agent runs on all devices with LLDP support. On the one hand, this software component sends information to all interfaces of the device at regular intervals. This is done using either Unicast or Multicast, depending on the destination addresses, which you can configure as required. On the other hand,

the LLDP agent is continuously receiving information from neighboring devices. The transmission and reception of the respective data packets is handled independently from each other.



The data packets being sent and received contain information such as the name and the description of the device, the ID and description of ports, the IP address or MAC address of the device, the specific capabilities of the device (e.g., in terms of switching and routing), VLAN identifiers and vendor-specific details. In this case, LLDP defines basic information that a data packet must always include, as well as optional additional information.

The individual devices store the information received locally in a data structure, the so-called MIB (Management Information Base). An MIB therefore contains data from its own LLDP agent and of the detected, direct neighbor agent.

The information exchange provides a continuing identification of the devices within the network, because the devices normally send packets cyclically (i.e. in configurable intervals). Furthermore, the devices also inform their network neighbors when changes occur on the device or in its network connection.

For the actual device identification process it is crucial that each connection point in the topology is clearly identified as a "Media Service Access Point" (MSAP). An MSAP is composed of a device ID (Chassis ID) and a port identification (Port ID). The unique identification or assignment of devices is therefore based on the fact that each MSAP in the monitored network topology may occur only once.

The Administrator can query and capture the data reported by the devices via a central network management software on his computer, where the query of the individual MIBs is performed using the SNMP protocol. The management software thus documents the entire topology of the network and allows automatic display of this topology along with a graphic representation of the current diagnostic data.

4.2 Structure of LLDP messages

Information is exchanged using specific units of data known as LLDP Data Units (LLDPDU). These data unit consists of TLVs (Type-Length-Values), and each TLV field corresponds to a certain type and has a certain length.

In accordance with the LLDP standard IEEE 802.1AB three TLVs are mandatory at the beginning of an LLDPDU in the following order:

- Type 1 = Chassis ID

4 LLDP

- Type 2 = Chassis ID
- Type 3 = Time to live

Following these mandatory TLVs, an LLDPDU can include additional, optional TLVs:

- Type 4 = Port description
- Type 5 = System name
- Type 6 = System description
- Type 7 = System capabilities
- Type 8 = Management address

At the end of an LLDPDU the following TLV is mandatory:

- Type 0 = End of LLDPDU

Tabular overview of the TLVs

TLV	Usage	Name	Example	Function
Type 1	Mandatory	Chassis ID	0018.2fa6.b28c	Identifies the device
Type 2	Mandatory	Port ID	Fi-0/12	Identifies the port
Type 3	Mandatory	Time to live	60 sec	Signals to the receiving device how long the received information should remain valid
Type 4	Optional	Port description	GigabitEthernet0/12	Displays details about the port such as the hardware version
Type 5	Optional	System name	PN-I/O 3	Displays the name given to the device by the administrator
Type 6	Optional	System description	LCOS software, version 8.9.1 SE	Displays details about the device such as the version of the networking software
Type 7	Optional	System capabilities	Router	Displays the primary function and capabilities of the device.
Type 8	Optional	Management address	192,168.0.1	Shows the IP or MAC address of the device
Type 0	Mandatory	End of LLDPDU	-----	Signals the end of the data unit

4.3 Supported operating systems

In principle, LLDP works on all popular systems, provided that LLDP agents or an appropriate software for evaluation of the LLDP packages is available. For Linux there are various open source projects, such as "LLDPD", "Open-LLDP" (with hyphen) or "ladvd", which deploy an LLDP agent.

The project "OpenLLDP" aims to achieve a further dissemination and acceptance of the LLDP protocol (802.1AB). The software supports the transmission and reception of LLDP messages on the Linux, Mac OS X, FreeBSD, and NetBSD platforms. Currently, however, this development seems to be stalled.

Microsoft Windows Vista and Windows 7 contain a proprietary protocol called LLTD (Link Layer Topology Discovery), which is essentially the same functionality as LLDP. On Windows XP, the LLTD component can be installed later as a patch. However, the patch is limited compared to the features implemented in Vista and Windows 7 because the "LLTD Responder" only reports IPv4 addresses, and not IPv6 addresses.

If you want to install LLDP on Windows systems, you can use a shareware called "haneWIN LLDP Agent". Using this, LLDP works on all Windows systems as of Windows 2000, i.e., on both 32-bit and 64-bit systems.

The most widely used free software for evaluation and analysis is Wireshark. The basic version of Wireshark is free of charge and now well-established as a standard. The software supports a wide variety of operating systems and can read and evaluate a wide variety of protocols (including LLDP). However, the focus of the basic version of Wireshark is the analysis of problems within the network. If you need more features (such as the visualization of network traffic in the form of colored graphs), you can purchase add-on modules.

4.4 Additions to the menu system

4.4.1 Additions to the Setup menu

LLDP

This submenu contains the configuration options relating to the Link Layer Discovery Protocol (LLDP). The options are similar to the configuration options according to LLDP MIB. If the information contained here is not sufficient, you can find more details in the IEEE 802.1AB standard.

SNMP ID:

2.38

Telnet path:

Setup > LLDP

Management addresses

In this table, enter the management address(es) that the device transmits via LLDPDUs. Management addresses take their names from the TCP/IP network list. The device only transfers the network and management addresses in this table for the LLDPDUs. A network from this list has the option of using the port list to limit the wider disclosure of the individual device addresses.

SNMP ID:

2.38.7

Telnet path:

Setup > LLDP > Management-Addresses



Defining address bindings limits the disclosure of management addresses regardless of the settings in the port lists. The device only reports a network that is connected to an interface. This is irrespective of the settings of the port list.

Network name

The name of the TCP/IP network, as entered in the TCP-IP network list.

SNMP ID:

2.38.7.1

Telnet path:

Setup > LLDP > Management-Addresses > Network-Name

Possible values:

Max. 16 alphanumerical characters

Default:

Blank

Port list

The list of interfaces and ports belonging to the corresponding management address.

SNMP ID:

2.38.7.2

Telnet path:**Setup > LLDP > Management-Addresses > Port-List****Possible values:**

>Comma-separated list of ports, max 251 alphanumeric characters, e.g., LAN-1 or WLAN-1. Use wildcards to specify a group of ports (e.g., "*_*").

Default:

Blank

Ports

This table includes all port-dependent configuration options. The table index is a string, specifically the interface/port name.

SNMP ID:

2.38.6

Telnet path:**Setup > LLDP > Ports****Name**

The name of the port or interface

SNMP ID:

2.38.6.1

Telnet path:**Setup > LLDP > Ports > Name****Possible values:**

Depending on the interfaces, e.g., LAN-1, WLAN-1

Admin status

Specifies whether PDU transfer and/or reception is active or inactive on this port. This parameter can be set individually for each port.

SNMP ID:

2.38.6.2

Telnet path:**Setup > LLDP > Ports > Admin-Status****Possible values:**

Off

TX only

RX only

Rx/Tx

Default:

Off

Notification

Use this to set whether changes in an MSAP remote station for this port are reported to possible network management systems.

SNMP ID:

2.38.6.3

Telnet path:

Setup > LLDP > Ports > Notifications

Possible values:

No

Yes

Default:

No

Admin status

Specify the quantity of the optional standard TLVs that will be transmitted to the PDUs.

SNMP ID:

2.38.6.4

Telnet path:

Setup > LLDP > Ports > TLVs

Possible values:

Port description

System name

System description

System properties

None

Default:

Port description

TLVs-802.3

Specify the quantity of the optional standard TLVs-802.3 that will be transmitted to the PDUs.

SNMP ID:

2.38.6.6

Telnet path:

Setup > LLDP > Ports > TLVs-802.3

4 LLDP

Possible values:

- PHY config status
- Power via MDI
- Link aggregation
- Max frame size
- None

Default:

- PHY config status

Maximum neighbors

This parameter specifies the maximum number of LLDP neighbors.

SNMP ID:

- 2.38.6.7

Telnet path:

- Setup > LLDP > Ports > Max-Neighbors**

Possible values:

- 0 to 65535

Default:

- 0

Update source

This parameter specifies the optional sources for LLDP updates.

SNMP ID:

- 2.38.6.8

Telnet path:

- Setup > LLDP > Ports > Update-Source**

Possible values:

- Auto
- LLDP only
- Other only
- Both

Default:

- Auto

TLVs-LCS

These settings define the quantity of the optional standard LCS TLVs that the device sends to PDUs.

SNMP ID:

- 2.38.6.9

Telnet path:

- Setup > LLDP > Ports > TLVs-LCS**

Possible values:

SSID
Radio channel
PHY type
None

Default:

SSID

Protocol

This table contains the LLDP port settings for the spanning-tree and rapid-spanning-tree protocols.

SNMP ID:

2.38.8

Telnet path:

Setup > LLDP > Protocols

Protocol

This parameter sets the protocol for which the LLDP ports are enabled.

SNMP ID:

2.38.8.1

Telnet path:

Setup > LLDP > Protocols > Protocol

Possible values:

Spanning-Tree
Rapid-Spanning-Tree

Default:

Spanning-Tree, Rapid-Spanning-Tree

Port list

This value describes the ports, which the LLDP uses with the associated protocol (spanning-tree or rapid-spanning-tree).

SNMP ID:

2.38.8.2

Telnet path:

Setup > LLDP > Protocols > Port-List

Possible values:

>Comma-separated list of ports, max 251 alphanumeric characters, e.g., LAN-1 or WLAN-1. Use wildcards to specify a group of ports (e.g., "*_*").

Default:

Blank

Notification interval

This value specifies the time interval until the device sends notifications of changes to the remote station tables. The value defines the smallest time period between notifications. Thus the default value of 5 seconds causes the device to send messages at most once every 5 seconds, even if the device has detected multiple changes in the meantime.

SNMP ID:

2.38.5

Telnet path:**Setup > LLDP > Notification-Interval****Possible values:**

0 to 9999 seconds

Default:

5

Operating

This parameter enables or disables the use of LLDP.

SNMP ID:

2.38.10

Telnet path:**Setup > LLDP > Operating****Possible values:**

Yes

No

Default:

No

Message TX hold multiplier

This value is used to calculate the time in seconds after which the device discards the information received with LLDP messages (hold time or time to live – TTL). The device calculates this value as the product of the *Message TX hold multiplier* specified here and the current *Message TX interval*:

$$\text{Hold time} = \text{Message TX hold multiplier} \times \text{Message TX interval}$$

The default settings result in a hold time for received LLDP messages of 120 seconds.

SNMP ID:

2.38.2

Telnet path:**Setup > LLDP > Message-TX-Hold-Multiplier****Possible values:**

0 to 99

Default:

4

Message TX interval

This value defines the interval in seconds for the regular transmission of LLDPDUs by the device.

-
- ❗ If the device detects changes to the LLDP information during an interval, the device can send additional LLDP messages. The *Tx delay* parameter defines the maximum frequency of LLDP messages caused by these changes.
 - ❗ The device also uses this `Message TX interval` for calculating the hold time for received LLDP messages with the help of the *Message TX hold multiplier*,

SNMP ID:

2.38.1

Telnet path:

Setup > LLDP > Message-TX-interval

Possible values:

0 to 65535 seconds

Default:

30

Reinit delay

This value defines the time the device suppresses transmission of LLDPDUs despite the LLDP being activated.

SNMP ID:

2.38.3

Telnet path:

Setup > LLDP > Reinit-Delay

Possible values:

0 to 99 seconds

Default:

2

Immediate delete

This parameter enables or disables the direct deletion of LLDPDUs.

SNMP ID:

2.38.9

Telnet path:

Setup > LLDP > Immediate-Deletion

Possible values:

Yes

No

Default:

Yes

4 LLDP

Tx delay

In principle the device sends LLDP messages in the interval set under *Message TX interval*. If the device detects changes to the LLDP information during an interval, the device can send additional LLDP messages.

The value set here defines the maximum frequency in seconds, in which the device uses LLDP messages. Thus the default value of 2 seconds causes the device to send LLDP messages once every 2 seconds, even if the device has detected multiple changes in the meantime.

SNMP ID:

2.38.4

Telnet path:**Setup > LLDP > Tx-Delay****Possible values:**

0 to 9999 seconds

Default:

2

5 IPv6

5.1 IPv6 basics

IPv4 (Internet Protocol version 4) is a protocol for unique addressing of nodes in a network and, at the time of writing, it has defined all of the IP addresses assigned globally. The limited availability of address space required the development of IPv6 (Internet Protocol version 6), which is to replace the former standard. With a different IP-address structure, IPv6 provides for a greater range of IP addresses and thus increases the possible number of participants in networks worldwide.

5.1.1 Why use IPv6-standard IP addresses?

The new IPv6 standard was developed for the following reasons:

- IPv4 address space allows for approximately four billion IP addresses for unique identities in networks. When the IPv4 standard was implemented in the '80s this address space was considered to be sufficient. Due to the enormous growth of the World Wide Web and the unexpectedly large number of computers and network devices, an address shortage has arisen that the IPv6 standard is intended to bridge.
- The increase in address space with IPv6 hampers the scanning of IP addresses by viruses and Trojans. The broader spectrum provides greater protection against attacks.
- IPv6 has been implemented with a view to the security requirements. For this reason it uses the security protocol IPSec (IP Security). This provides secure network communications on layer 3 whereas many of IPv4 security mechanisms only operate on higher layers.
- Simplified, fixed descriptors for data packets save on router processing power and thus accelerate the available throughput.
- IPv6 allows for easier and faster transmission of data in real time, making it suitable for multimedia applications such as Internet telephony and Internet TV.
- So-called mobile IPs allow you to use a fixed IP address to login to different networks. This allows you to log on with your laptop using the same IP address, whether you are in your home network, in a café or at work.

5.1.2 IP address structure according to the IPv6 standard

The new IPv6 addresses are 128 bits long and the range of possible addresses can cater for about 340 sextillion network participants. IPv6 addresses consist of eight blocks of 16 bits and are written as hexadecimal numbers. The following is an example of a possible IPv6 address:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

To improve the legibility of these IP addresses, zeros at the beginning of a block of numbers are omitted. It is also possible to omit one group of blocks that consist entirely of zeros. For the above example, one possible representation would be as follows:

2001:db8::54f3:dd6b:1/64

An IPv6 address consists of two parts; a prefix and an interface identifier. The prefix denotes the membership of the IP address to a network, while the interface identifier (e.g. in the case of auto-configuration) is generated from a link-layer address, and thus belongs to a particular network card. The device can also generate interface identifiers from random numbers. This improves security. In this way, multiple IPv6 addresses can be assigned to a single component.

The prefix describes the first part of the IP address. The length of the prefix is shown as a decimal number after a slash. For the example given here the prefix is:

2001:db8::/64

The remainder of the IP address is the interface identifier. In our example, this is:

::54f3:ddb6:1

Compared with the IP addresses for the IPv4 standard, a number of changes have resulted in the structure of the new IPv6 addresses:

- While IPv4 addresses cater for an address space of 32 bits, the new length of 128 bits results in a significantly larger address space with IPv6. IPv6 addresses are four times longer than IPv4 addresses.
- An interface can have multiple IPv6 addresses due to the potential assignment of multiple prefixes to a single interface identifier. With the IPv4 standard, an interface has only one IP address.
- IPv4 addresses must be assigned by a central server. This is usually a DHCP server. However, IPv6 can operate an auto-configuration, which makes the use of a DHCP server unnecessary. However, you the option of using a DHCP server is still open to you.

5.1.3 Stages of migration

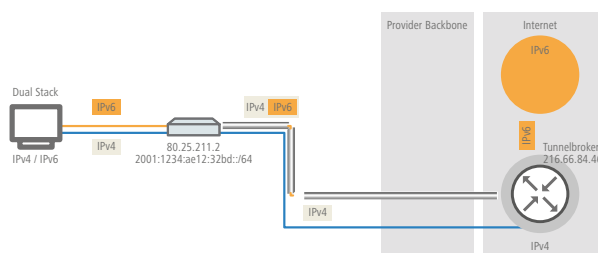
IPv6 is available to networks in a variety of ways. We make a distinction between environments with native IPv6 and those which provide IPv6 through a tunnel.

- **Native IPv6:** Native IPv6 describes a network that communicates to the outside only via IPv6. Users with IPv4 addresses can only access this network by communicating through a gateway that mediates between IPv6 and IPv4 networks.
- **IPv6 via dual stack:** Dual stack refers to the parallel operation of IPv4 and IPv6 in a network. A router mediates between devices that "speak" only IPv4 or IPv6. The clients select the protocol they need.
- **IPv6 tunneling:** If a router does not have IPv6 Internet access, it can still access IPv6 networks by means of a tunnel.

5.2 IPv6 tunneling technologies

5.2.1 6in4 tunneling

6in4 tunnels are used to connect two hosts, routers, or to interconnect a host and router. This means that 6in4 tunnels can connect two IPv6 networks via an IPv4 network. The diagram shows a static 6in4 tunnel between the local router and a 6in4 gateway belonging to a tunnel broker.



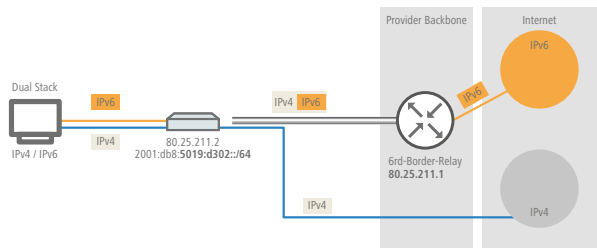
Unlike 6to4, these are dedicated services operated by a known provider. The end-points are fixed and the tunnel broker assigns a static prefix. The advantages of a 6in4 solution are that the gateways are fixed and the operator is known. The fixed prefix from the tunnel broker also determines the number of possible subnets that can be used. A 64-bit prefix (e.g. 2001:db8::/64) allows one subnet to be used. If a 48-bit prefix is used, 16 bits of the 64-bit prefix are available for use. This allows the implementation of up to 65,536 subnets.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router.

6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is also suitable for professional use.

5.2.2 6rd tunneling

6rd (rapid deployment) is a development of 6to4. The underlying function is identical. The difference is that just one particular relay is used, as operated by a provider. This solves the two basic problems of the 6to4 technology—the lack of security and stability. The prefix with 6rd is either configured manually or sent via DHCP (IPv4), which further reduces the effort involved with configuration. The diagram is a schematic representation of a 6rd scenario.

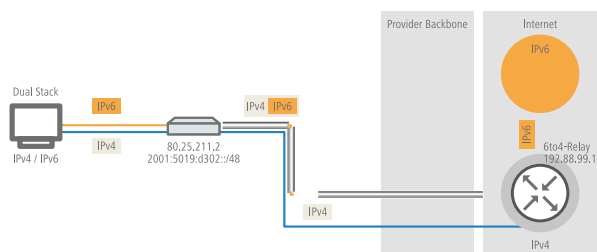


The provider assigns the router with a prefix (2001:db8::/32), which the router then supplements with its own IPv4 address. The IPv6 address generated in this way has the form: 2001:db8:5019:d302::/64. This makes 6rd interesting from two perspectives. The provider has a simple way to give its customers access to the IPv6 Internet. In addition, customers benefit from greatly simplified usage. They do not have to accept the security risks of 6to4, nor do they have to handle the complicated configuration of 6in4.

5.2.3 6to4 tunneling

6to4 tunneling offers you an easy way to set up a connection between two IPv6 networks via an IPv4 network. To this end, what is known as a 6to4 tunnel is set up:

- A router between the local IPv6 network and an IPv4 network serves to mediate between the networks.
- The router has both a public IPv4 address and an IPv6 address. The IPv6 address consists of an IPv6 prefix and the IPv4 address in hexadecimal notation. If a router such has the IPv4 address 80.25.211.2, this will first be converted into hexadecimal notation: 5019:d302. Supplementing this is an IPv6 prefix (e.g. 2002::/16), so that the IPv6 address for the router appears as follows: 2002:5019:d302::/48.
- If a device in the IPv6 network sends data packets via the router to a destination address in the IPv4 network, then the router first of all repacks the IPv6 packets and encapsulates them into a package with an IPv4 header. The router then forwards the encapsulated package to a 6to4 relay. The 6to4 relay unpacks the packet and forwards it to the desired destination. The following illustration shows the operating principle of 6to4 tunneling:



6to4 tunnels establish a dynamic connection between IPv6 and IPv4 networks: the response packets may be routed back via a different 6to4 relay. 6to4 tunnels are not a point-to-point connection. For every new connection, the router always looks for the "nearest" public 6to4 relay. This is done using the anycast address 192.88.99.1. This aspect is an advantage of 6to4 tunneling on the one hand, but it also presents a disadvantage on the other. Public 6to4 relays do not require registration and are freely accessible. What's more, the dynamic connection is easily configured. In this way it is possible for any user to create a 6to4 tunnel over a public relay, quickly and easily.

On the other hand, the dynamic connection means that the user has no influence on the choice of the 6to4 relay. The provider of the relay is able to intercept or manipulate data.

5.3 DHCPv6

Compared to IPv4, clients in an IPv6 network do not require automatic address assignment from a DHCP server because they use auto-configuration. However, because certain information such as DNS server addresses are not transmitted during auto-configuration, certain application scenarios can benefit from a DHCP service on the IPv6 network.

5.3.1 DHCPv6 server

The use of a DHCPv6 server is optional for IPv6. In principle, a DHCPv6 server supports two modes:

- **Stateless:** The DHCPv6 server does not distribute addresses but only information, such as DNS server addresses. Using this method, clients generate their own IPv6 addresses by 'stateless address auto-configuration (SLAAC)'. This method is particularly attractive for example for small networks in order to keep administration efforts to a minimum.
- **Stateful:** The DHCPv6 server distributes IPv6 addresses, similar to IPv4. This method is more complicated, since a DHCPv6 server has to assign and manage the addresses.

A DHCPv6 server distributes only the options that are explicitly requested by an IPv6 client, i. e. the server only assigns an address to a client if it explicitly requests one.

Additionally, the DHCPv6 server can pass on prefixes to routers for further distribution. This method is referred to as 'prefix delegation'. A DHCPv6 client must have explicitly requested this prefix, however.


5.3.2 DHCPv6 client


The auto-configuration available with IPv6 networks makes it very easy and convenient to configure the clients.

However, in order for a client to receive additional information, such as a DNS server address, you must configure the device so that it can activate the DHCPv6 client when necessary.

The settings for the DHCPv6 client ensure that a device receiving certain flags in the router advertisement will start the DHCPv6 client, which can then send requests to the DHCPv6 server:

- **M flag:** If an appropriately configured device receives a router advertisement with the 'M flag' set, the DHCPv6 client will request an IPv6 address from the DHCPv6 server along with other information such as DNS server, SIP server and NTP server.
- **O flag:** With an 'O flag', the DHCPv6 client requests the DHCPv6 server for information such as a DNS server, SIP server and NTP server only, but not an IPv6 address.

 If the 'M-flag' is set, the 'O-flag' does not necessarily have to be set as well.

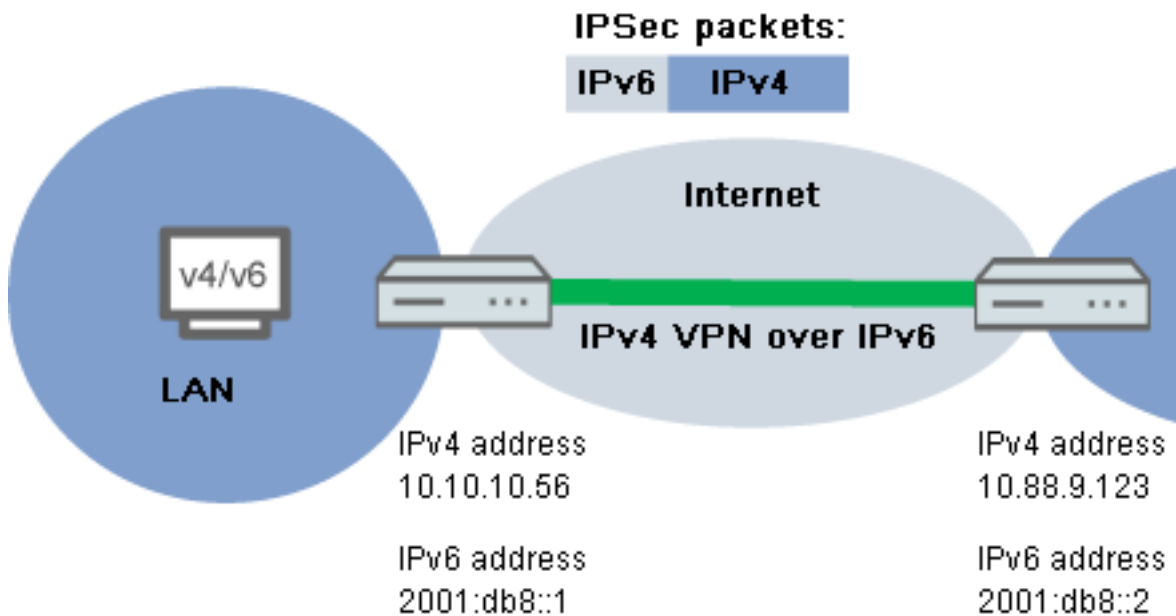
 With IPv6, the default route is distributed via router advertisements and not via DHCPv6.

5.4 IPv4 VPN tunnel via IPv6

Until now it was not possible to set up a VPN between two remote stations using private IPv4 addresses to access the Internet (e.g. 3G/4G networking).

This restriction no longer exists with IPv6, because every IPv6 device receives a public IPv6 address. Thus IPv6 can be used to set up an IPv4 VPN tunnel to interconnect two remote IPv4 networks, regardless of the IPv4 WAN addresses used at each site.

In the example shown, two local IPv4 networks are connected via an IPv4 VPN tunnel, which is established over an IPv6 Internet connection. The IPv4 VPN packets are given IPv6 headers and sent to the remote site via the IPv6 Internet connection (either native or via tunnel broker).

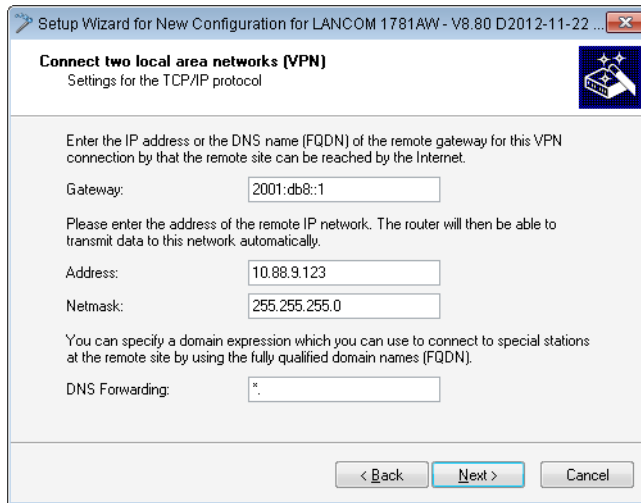


5.4 Setup Wizard – Setting up an IPv4 VPN connection via IPv6

The Setup Wizard option "Connect two local area networks" helps you to set up a VPN connection.

1. Start LANconfig, for example from the Windows start menu with **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.
2. Choose your device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools > Setup Wizard**. LANconfig first reads out the device configuration and then displays the selection window with the optional applications.
3. Launch the action **Connect two local area networks**.
4. Follow the Wizard's instructions and enter the necessary data.

5. As the gateway address, enter the IPv6 address of the gateway.



6. You can then close the Wizard with **Finish**.
The Setup Wizard writes the configuration to the device.

5.5 IPv6 firewall

5.5.1 Function

While the IPv4 firewall only controls the forwarding of IP data, the IPv6 firewall also regulates the functions of the access lists for all IPv6 server services. Therefore, the IPv6 firewall is similar to a classic firewall design, which separately supports the inbound and outbound communications, as well as forwarding. Since the LANCOM configuration specifically controls communication, LCOS does not require an outbound firewall.

5.5.2 Configuration

The configuration of the IPv6 firewall is practically the same as the IPv4 firewall; however, it is performed separately.

The inbound and forwarding firewalls each have their own rule tables, which in parts are the same as or similar to the IPv4 firewall in scope and structure.

The rules are sorted with decreasing priority, i. e. the rule with the highest priority is at the top of the list. If a rule requires further actions, these are also performed by firewall in sequence. Otherwise, firewall filtering is terminated after the current rule has been applied.

5.5.3 IPv6 firewall table

Similar to the IPv4 firewall, the IPv6 firewall provides a log table of events in the IPv6 environment.

The syntax of the log table is the same as the IPv4 log table with the exception of the IP address format (IPv6 addresses are in hexadecimal format, IPv4 in decimal format).

Analyzing the firewall table with WEBconfig

You can open IPv6 log tables in WEBconfig with **LCOS menu tree > Status > IPv6 > Firewall > Log table.**

LCOS Menu Tree

- 📁 Status
 - 📁 IPv6
 - 📁 Firewall

Log-Table


Idx.	System-time	Src-Address	Dst-Address	Prot.	Src-Port	Dst-Port	Filter-Rule	Limit	Threshold	Action
<no entries>										

Update Interval (s):

The items have the following meanings:

- **Idx.:** Consecutive index. Furthermore, the table can also be checked via SNMP.
- **System time:** System time in UTC encoding (converted to plain text for display).
- **Source addresses:** Source address of the filtered packets.
- **Destination addresses:** Destination address of the filtered packets.
- **Prot.:** Protocol (TCP, UDP, etc.) of the filtered packets.
- **Source port:** Source port of the filtered packet (only for port related protocols).
- **Destination port:** Destination port of the filtered packet (only for port related protocols).
- **Filter rule:** Name of the rule that created the entry.
- **Limit:** Bit field that contains the description of the limit that caused the firewall to apply the filter. There following values are currently defined:
 - 0x01: Absolute number
 - 0x02: Number per second
 - 0x04: Number per minute
 - 0x08: Number per hour:
 - 0X10: Global limit
 - 0x20: Byte limit (if not set, it is a packet limit)
 - 0x40: Limit only applies in the inbound direction
 - 0x80: Limit only applies in the outbound direction
- **Threshold:** Threshold limit value of the triggering limit.
- **Action:** Bit field which lists all the actions performed. There following values are currently defined:
 - 0x00000001: Accept
 - 0x00000100: Reject
 - 0x00000200: Establish filter
 - 0x00000400: Internet (default router) filter
 - 0x00000800: Drop
 - 0x00001000: Disconnect
 - 0x00004000: Lock source address
 - 0x00020000: Lock destination address and port

- 0X20000000: Send SYSLOG notification message
- 0x40000000: Send SNMP trap
- 0x80000000: Send e-mail

 All firewall actions also appear in the IP router trace . Some LANCOM models also have a firewall LED, which indicates each packet filtered.

Analyzing the firewall table with LANmonitor

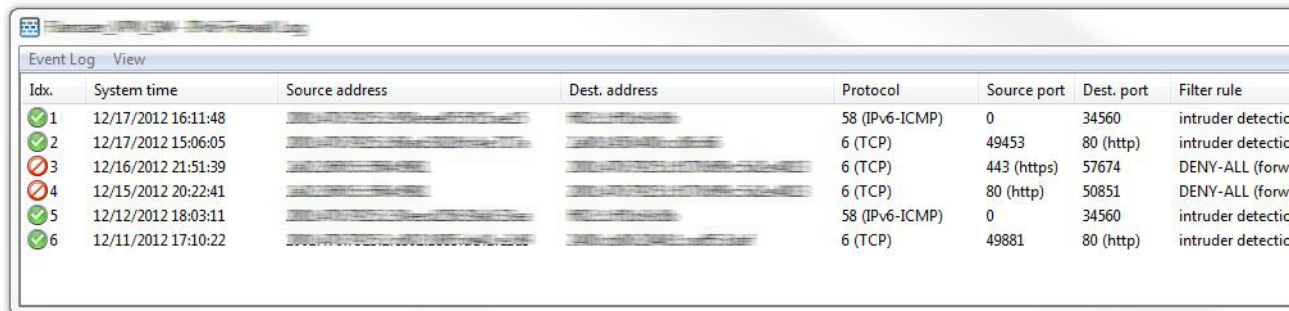
You can view the IPv6 log for a specific device in the LANmonitor.

To do this, start the LANmmonitor with **Start > Programs > LANCOM > LANmonitor**. You can also launch the LANmonitor for a specific device with the context menu in LANconfig or with the keyboard shortcut `Ctrl + M`.



Via **Device > View firewall event log** you can view the firewall events for a selected device. The firewall events show the last 100 actions of the firewall with the following details:

- Idx
- Time
- Source address
- Destination address
- Protocol
- Source port
- Destination port
- Firewall rule
- Limit
- Action



Idx.	System time	Source address	Dest. address	Protocol	Source port	Dest. port	Filter rule
1	12/17/2012 16:11:48			58 (IPv6-ICMP)	0	34560	intruder detectio
2	12/17/2012 15:06:05			6 (TCP)	49453	80 (http)	intruder detectio
3	12/16/2012 21:51:39			6 (TCP)	443 (https)	57674	DENY-ALL (forw
4	12/15/2012 20:22:41			6 (TCP)	80 (http)	50851	DENY-ALL (forw
5	12/12/2012 18:03:11			58 (IPv6-ICMP)	0	34560	intruder detectio
6	12/11/2012 17:10:22			6 (TCP)	49881	80 (http)	intruder detectio

5.6 Additions to the Setup menu

5.6.1 Tunnel

Use this setting to manage the tunneling protocols to provide access to the IPv6 Internet via an IPv4 Internet connection.

SNMP ID:

2.70.1

Telnet path:

Setup > IPv6 > Tunnel

6in4

The table contains the settings for the 6in4 tunnel.

SNMP ID:

2.70.1.1

Telnet path:

Setup > IPv6 > Tunnel > 6in4

Peer name

Contains the name of the 6in4 tunnel.

SNMP ID:

2.70.1.1.1

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Peer-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.1.2

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Gateway address

Contains the IPv4 address of the remote 6in4 gateway.



The 6in4 tunnel is only set up if the gateway can be reached by ping at this address.

SNMP ID:

2.70.1.1.3

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Gateway-Address

Possible values:

IP address in IPv4 notation, max. 64 characters

Default:

Blank

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.1.4

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > IPv4-Rtg-tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Gateway IPv6 address

Contains the IPv6 address of the remote tunnel endpoint on the intermediate network, for example, "2001:db8::1".

SNMP ID:

2.70.1.1.5

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Gateway-IPv6-Address

Possible values:

IPv6 address with max. 43 characters

Default:

Blank

Local-IPv6-Address

Contains the local IPv6 address of the device on the intermediate network, for example "2001:db8::2/64".

SNMP ID:

2.70.1.1.6

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Local-IPv6-Address

Possible values:

Max. 43 characters

Default:

Blank

Routed IPv6 prefix

Contains the prefix that is routed from the remote gateway to the local device and that is to be used in LAN, e.g. "2001:db8:1:1::/64" or "2001:db8:1::/48".

SNMP ID:

2.70.1.1.7

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Routed-IPv6-Prefix

Possible values:


Max. 43 characters

Default:

Blank

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.1.8

Telnet path:

Setup > IPv6 > Tunnel > 6in4 > Firewall

Possible values:

Yes

No

Default:

Yes

6rd border relay

A LANCOM router can operate as a 6rd client or as a 6rd border relay. A 6rd client or 6rd CE router (customer edge router) connects to an Internet service provider via a WAN connection and propagates the 6rd prefix to clients on the LAN. A 6rd border relay operates in the provider's network and connects 6rd clients to the IPv6 network. Thus a 6rd border relay used when an IPv6 connection is to be provided to 6rd routers.

SNMP ID:

2.70.1.2

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay

Peer name

Contains the name of the 6rd border relay tunnel.

SNMP ID:

2.70.1.2.1

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > Peer-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.2.2

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

IPv4 loopback address

Set the IPv4 loopback address, i.e. the address where the device operates as a 6rd border relay.

SNMP ID:

2.70.1.2.3

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > IPv4-Loopback-Address

Possible values:

Max. 16 characters

Default:

Blank

6rd prefix

Defines the prefix used by this border relay for the 6rd domain, e.g. 2001:db8:/32. This prefix must also be configured on all associated 6rd clients.

SNMP ID:

2.70.1.2.4

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > 6rd-Prefix

Possible values:

Max. 24 characters as a prefix of an IPv6 address with up to four blocks of four hexadecimal digits each

Default:

Blank

IPv4 mask length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

SNMP ID:

2.70)

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > IPv4-Mask-Length

Possible values:

Max. 2 numbers in the range 0 – 32

Default:

0: The device uses the full IPv4 address.

DHCPv4 propagate

If you enable this function, the 6rd border relay distributes the prefix via DHCPv4 if the DHCPv4 client requests it.



If you do not enable this feature, you must manually configure the required 6rd settings for the 6rd clients.

SNMP ID:

2.70.1.2.6

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > DHCPv4-Propagate

Possible values:

Yes


No

Default:

No

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.2.7

Telnet path:

Setup > IPv6 > Tunnel > 6rd-Border-Relay > Firewall

Possible values:

Yes

No

Default:

Yes

6rd

The table contains the settings for the 6rd tunnel.

SNMP ID:

2.70.1.3

Telnet path:

Setup > IPv6 > Tunnel > 6rd

Peer name

Contains the name of the 6rd tunnel.

SNMP ID:

2.70.1.3.1

Telnet path:

Setup > IPv6 > Tunnel > 6rd > Peer-Name

Possible values:

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.3.2

Telnet path:

Setup > IPv6 > Tunnel > 6rd > Rtg-Tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

Border relay address

Contains the IPv4 address of the 6rd border relay.

SNMP ID:

2.70.1.3.3

Telnet path:

Setup > IPv6 > Tunnel > 6rd4 > Border-Relay-Address

Possible values:

IPv4 address with max. 64 characters

Default:

Blank

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.3.4

Telnet path:

Setup > IPv6 > Tunnel > 6rd > IPv4-Rtg-tag

Possible values:

Max. 5 characters in the range 0 – 65534

Default:

0

6rd prefix

Contains the prefix used by the provider for 6rd services, e.g. "2001:db8::/32".



If the 6rd prefix is assigned through DHCPv4, you have to enter "::/32" here.

SNMP ID:

2.70.1.3.5

Telnet path:

Setup > IPv6 > Tunnel > 6rd > 6rd-Prefix

Possible values:

Max. 24 characters

Default:

Blank

IPv4 mask length

Defines the number of significant bits of IPv4 addresses that are identical within a 6rd domain. With mask length "0" there are no identical bits. In this case, the entire IPv4 address is used to generate the delegated 6rd prefix.

The provider sets the mask length.

Example: The IPv4 address of the device is "192.168.1.99" (in hexadecimal: "c0a8:163"). In this case, the following are examples of possible combinations:

6rd domain	Mask length	6rd prefix
2001:db8::/32	0	2001:db8:c0a8:163::/64
2001:db8:2::/48	16	2001:db8:2:163::/64
2001:db8:2:3300::/56	24	2001:db8:2:3363::/64

SNMP ID:

2.70.1.3.6

Telnet path:

Setup > IPv6 > Tunnel > 6rd > IPv4-Mask-Length

Possible values:


Max. 2 numbers in the range 0 – 32

Default:

0

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.3.7

Telnet path:

Setup > IPv6 > Tunnel > 6rd4 > Firewall

Possible values:

Yes

No

Default:

Yes

6to4

The table contains the settings for the 6to4 tunnel.



Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

SNMP ID:

2.70.1.4

Telnet path:**Setup > IPv6 > Tunnel > 6to4****Peer name**

Contains the name of the 6to4 tunnel.

SNMP ID:

2.70.1.4.1

Telnet path:**Setup > IPv6 > Tunnel > 6to4 > Peer-Name****Possible values:**

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.1.4.2

Telnet path:**Setup > IPv6 > Tunnel > 6to4 > Rtg-Tag****Possible values:**


Max. 5 characters in the range 0 – 65535

Default:

0

Gateway address

Contains the IPv4 address of the 6to4 relay or 6to4 gateway. Default value is the anycast address "192.88.99.1". In general, you can leave this address unchanged as it will always give you access to the closest 6to4 relay on the Internet.

 The 6to4 tunnel is only set up if the gateway can be reached by ping at this address.

SNMP ID:

2.70.1.4.3

Telnet path:**Setup > IPv6 > Tunnel > 6to4 > Gateway-Address****Possible values:**

IPv4 address with max. 64 characters

Default:

192.88.99.1

IPv4 routing tag

Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The IPv4 routing tag specifies which tagged IPv4 route is to be used for the data packets to reach their destination address. The following destination addresses can be entered:

- 6to4 anycast address
- 6in4 gateway address
- 6rd border relay address

SNMP ID:

2.70.1.4.4

Telnet path:**Setup > IPv6 > Tunnel > 6to4 > IPv4-Rtg-tag****Possible values:**


Max. 5 characters in the range 0 – 65534

Default:

0

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual tunnel interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General**.

 Disabling the firewall globally means that the firewall is disabled for all interfaces, even if you enable this option.

SNMP ID:

2.70.1.4.5

Telnet path:**Setup > IPv6 > Tunnel > 6to4 > Firewall****Possible values:**

Yes

No

Default:

Yes

5.6.2 Router advertisement

These settings are used to manage the router advertisements, which are used to announce the device's availability as a router to the network.

SNMP ID:

2.70.2

Telnet path:

Setup > IPv6 > Router-Advertisement

Prefix options

The table contains the settings for IPv6 prefixes for each interface.

SNMP ID:

2.70.2.1

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Options

Interface name

Defines the name of the logical interface.

SNMP ID:

2.70.2.1.1

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Prefix

Enter the prefix that is transmitted with the router advertisements, e. g. "2001:db8::/64".

The length of the prefix must always be exactly 64 bits ("/64"), or else the clients will not be able to generate their own addresses by adding their "interface identifier" (64 bits long).



If you wish to automatically use the prefix issued by the provider, then configure "::/64" here and enter the name of the corresponding WAN interface in the field **PD-Source**.

SNMP ID:

2.70.2.1.2

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Prefix

Possible values:

Max. 43 characters

Default:

Blank

Subnet ID

Here you set the subnet ID that is to be combined with the prefix issued by the provider.

If the provider assigns the prefix "2001:db8:a::/48", for example, and you assign the subnet ID "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64".

The maximum subnet length with a 48-bit long, delegated prefix is 16 bits (65,536 subnets of "0000" to "FFFF"). With a delegated prefix of "/56", the maximum subnet length is 8 bits (256 subnets of "00" to "FF").

 In general, the subnet ID "0" is used when the WAN IPv6 address is compiled automatically. For this reason you should start with "1" when assigning subnet IDs for LANs.

SNMP ID:

2.70.2.1.3

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Subnet-ID

Possible values:

Max. 19 characters

Default:

1

Adv.-OnLink

Indicates whether the prefix is "on link".

SNMP ID:

2.70.2.1.3

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-OnLink

Possible values:

Yes

No

Default:

Yes

Adv.-Autonomous

Indicates whether a host can use the prefix for a "Stateless Address Autoconfiguration". If this is the case, it can connect directly to the Internet.

SNMP ID:

2.70.2.1.5

Telnet path:

Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Autonomous

Possible values:

Yes

No

Default:

Yes

PD source

Use the name of the interface that receives a prefix issued by the provider. This prefix is combined with the string entered in the field **Prefix** to form a subnet that announces router advertisements (DHCPv6 prefix delegation).

SNMP ID:

2.70.2.1.6

Telnet path:**Setup > IPv6 > Router-Advertisements > Prefix-Options > PD-Source****Possible values:**

Max. 16 characters

Default:

Blank

Advertise preferred lifetime

Defines the time in milliseconds for which an IPv6 address is to be "Preferred". The client also uses this lifetime for its generated IPv6 address. If the lifetime of the prefix has expired, the client no longer uses the corresponding IPv6 address. If the "preferred lifetime" of an address expires, it will be marked as "deprecated". This address is then used only by already active connections until those connections end. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.1.7

Telnet path:**Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Pref.-Lifetime****Possible values:**

Max. 10 numbers in the range 0 – 2147483647

Default:

604800

Adv.-Valid-Lifetime

Defines the time in seconds, after which the validity of an IPv6 address expires. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.1.8

Telnet path:**Setup > IPv6 > Router-Advertisements > Prefix-Options > Adv.-Valid-Lifetime****Possible values:**

Max. 10 numbers in the range 0 – 2147483647

Default:

2592000

Decrement lifetimes

If this option is enabled, the preferred and valid lifetime of the prefix in the router advertisements are automatically counted down over time or extended. The preferred and valid lifetimes of the prefix in the router advertisements are synchronized with the times from the delegated prefix as retrieved from the WAN. If the prefix from the provider is not updated, then the preferred and valid lifetimes are counted down to 0, and thus expire. As soon as the device updates the lifetimes of the delegated prefix from the WAN, then the prefix in the router advertisements is extended again. If this option is disabled, the preferred and valid lifetime from the delegated prefix are applied statically, but they are not reduced or extended. This parameter has no effect on tunneled WAN connections (6to4, 6in4 and 6rd), because in this case the prefixes are not retrieved by DHCPv6 prefix delegation, and thus they have no lifetimes. Here, the statically-configured preferred and valid lifetimes from the prefix are applied. This parameter also has no effect if the value for PD source is left empty, because in this case there is no synchronization with the delegated WAN prefix.

SNMP ID:

2.70.2.1.10

Telnet path:**Setup > IPv6 > Router-Advertisement > Prefix-Options****Possible values:**

Yes

No

Default:

Yes

Interface options

The table contains the settings for the IPv6 interfaces.

SNMP ID:

2.70.2.2

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options****Interface name**

Defines the name of the logical interface to be used for sending router advertisements.

SNMP ID:

2.70.2.2.1

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Interface-Name****Possible values:**

Max. 16 characters

Default:

Blank

Send adverts

Enables the periodic transmission of router advertisements and the response to router solicitations.

SNMP ID:

2.70.2.2.2

Telnet path:**Setup > IPv6 > Router-Advertisement > Interface-Options > Send-Adverts****Possible values:**

Yes

No

Default:

Yes

Min. RTR interval

Defines in seconds the minimum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

SNMP ID:

2.70.2.2.3

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Min-RTR-Interval****Possible values:**

Min. 3 seconds

Max. $0.75 * \text{Max-RTR-Interval}$

Max. 10 numbers

Default: $0.33 * \text{Max-RTR-Interval}$ (if **Max-RTR-Interval** ≥ 9 seconds)**Max-RTR-Interval** (if **Max-RTR-Interval** < 9 seconds)**Max. RTR interval**

Defines in seconds the maximum time allowed between the transmission of consecutive unsolicited multicast router advertisements. **Min-RTR-Interval** and **Max-RTR-Interval** form a time space within which the device sends a router advertisement at random.

SNMP ID:

2.70.2.2.4

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Max-RTR-Interval****Possible values:**

Min. 4 seconds

Max. 1800 seconds

Max. 10 numbers

Default:

600 seconds

Managed flag

Sets the "Managed address configuration" flag in the router advertisement.

Setting this flag causes the clients to configure all addresses via "Stateful Autoconfiguration" (DHCPv6). In this case the clients also automatically retrieve other information, such as DNS server addresses.

SNMP ID:

2.70.2.2.5

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Managed-Flag

Possible values:

Yes

No

Default:

No

Other config flag

Sets the "Other configuration" flag in the router advertisement.

If this flag is set, the device instructs the clients to retrieve additional information (but not the addresses for the client) such as DNS server addresses via DHCPv6.

SNMP ID:

2.70.2.2.6

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Other-Config-Flag

Possible values:

Yes

No

Default:

Yes

Link MTU

Here you set the valid MTU for the corresponding link.

SNMP ID:

2.70.2.2.7

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Link-MTU

Possible values:

Max. 5 numbers in the range 0 – 99999

Default:

1500

Reachable time

Specifies the time in seconds for which the router is considered to be reachable.

The default value of "0" means that the router advertisements have no specifications for reachable time.

SNMP ID:

2.70.2.2.8

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Reachable-Time

Possible values:

Max. 10 numbers in the range 0 – 2147483647

Default:

0

Hop limit

Defines the maximum number of routers to be used to forward a data packet. One router corresponds to one "hop".

SNMP ID:

2.70.2.2.10

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Hop-Limit

Possible values:

Max. 5 numbers in the range 0 – 255

Default:

0: No hop limit defined

Default lifetime

Specifies the time in seconds for which the router is considered to be reachable in the network.



If this value is set to **0**, the operating system will not use this router as the default router.

SNMP ID:

2.70.2.2.11

Telnet path:

Setup > IPv6 > Router-Advertisements > Interface-Options > Def.-Lifetime

Possible values:

Max. 10 numbers in the range 0 – 2147483647

Default:

1800

Default router mode

Defines how the device advertises itself as the default gateway or router.

The settings have the following functions:

- **Auto:** As long as a WAN connection exists, the router sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway. If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway. This behavior is compliant with RFC 6204.
- **Always:** The router lifetime is always positive—i. e. greater than "0"—irrespective of the WAN connection status.
- **Never:** The router lifetime is always "0".

SNMP ID:

2.70.2.2.12

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Default-Router-Mode****Possible values:**

Auto

Always

Never

Default:

Auto

Router preference

Defines the preference of this router. Clients enter this preference into their local routing tables.

SNMP ID:

2.70.2.2.13

Telnet path:**Setup > IPv6 > Router-Advertisements > Interface-Options > Router-Preference****Possible values:**

Low

Medium

High

Default:

Medium

Route options

The table contains the settings for the route options.

SNMP ID:

2.70.2.3

Telnet path:**Setup > IPv6 > Router-Advertisement > Route-Options****Interface name**

Defines the name of the interface that this route option applies to.

SNMP ID:

2.70.2.3.1

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Interface-Name

Possible values:

Max. 16 characters

Default:

Blank

Prefix

Set the prefix for this route. This should not exceed 64 bits in length if it is to be used for auto-configuration.

SNMP ID:

2.70.2.3.2

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Prefix

Possible values:

IPv6 prefix with max. 43 characters, e.g. 2001:db8::/64

Default:

Blank

Route lifetime

Set how long in seconds the route should remain valid.

SNMP ID:

2.70.2.3.3

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Route-Lifetime

Possible values:

Max. 5 numbers in the range 0 – 65335

Default:

0: No route lifetime specified

Route preference

This parameter specifies the priority of an advertised route. A router receiving a router advertisement with two routes of different preference will choose the route with the higher priority.

SNMP ID:

2.70.2.3.4

Telnet path:

Setup > IPv6 > Router-Advertisement > Route-Options > Route-Preference

Possible values:

Low

Medium


High

Default:

Medium

RDNSS options

This table contains the settings of RDNSS extension (recursive DNS server).

 This function is not currently supported by Windows. Propagation of a DNS server, where required, is performed via DHCPv6.

SNMP ID:

2.70.2.5

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options****Interface name**

Name of the interface used by the device to announce information about the IPv6 DNS server in router advertisements.

SNMP ID:

2.70.2.5.1

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options****Possible values:**

Max. 16 characters

Default:

Blank

Primary DNS

IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC6106) for this interface.

SNMP ID:

2.70.2.5.2

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options****Possible values:**

Valid IPv6 address

Default:

Blank

Secondary DNS

IPv6 address of the secondary IPv6 DNS server for this interface.

SNMP ID:

2.70.2.5.3

Telnet path:**Setup > IPv6 > Router-Advertisements > RDNSS-Options**

Possible values:

Valid IPv6 address

Default:

Blank

DNS search list

This parameter defines which DNS search list the device propagates on this logical network.

SNMP ID:

2.70.2.5.4

Telnet path:

Setup > IPv6 > Router-Advertisements > RDNSS-Options

Possible values:

Internal: If you select this option, the device propagates either the DNS search list from the internal DNS server or the domain of this logical network. The domain is configured under **Setup > DNS > Domain**.

WAN: If you select this option, the device propagates the DNS search list from the provider (e.g. provider-xy.com) for this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under **Receive prefix from**.

Default:

Internal enabled, WAN disabled.

Lifetime

Defines the time in seconds for which a client may use this DNS server for name resolution.

SNMP ID:

2.70.2.5.5

Telnet path:

Setup > IPv6 > Router-Advertisements > RDNSS-Options

Possible values:

- Max. 5 numbers in the range 0 – 65535
- 0: Discontinuation

Default:

900

5.6.3 DHCPv6

This menu contains the DHCPv6 settings.

SNMP ID:

2.70.3

Telnet path:

Setup > IPv6 > DHCPv6

Server

This menu contains the DHCP server settings for IPv6.

SNMP ID:

2.70.3.1

Telnet path:**Setup > IPv6 > DHCPv6 > Server****Address pools**

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool.

SNMP ID:

2.70.3.1.2

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pool****Address pool name**

Specify the name of the address pool here.

SNMP ID:

2.70.3.1.2.1

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pools > Address-Pool-Name****Possible values:**

Maximum 31 characters

Default:

Blank

Start address pool

Here you specify the first address in the pool, e. g. "2001:db8::1"

SNMP ID:

2.70.3.1.2.2

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pools > Start-Address-Pool****Possible values:**

Maximum 39 characters

Default:

Blank

End address pool

Here you specify the last address in the pool, e. g. "2001:db8::9"

SNMP ID:

2.70.3.1.2.3

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Address-Pools > End-Address-Pool**

Possible values:

Maximum 39 characters

Default:

Blank

Preferred lifetime

Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".

SNMP ID:

2.70.3.1.2.5

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools > Pref.-Lifetime

Possible values:

Maximum 10 characters.

Default:

3600

Valid lifetime

Here you specify the time in seconds that the client should treat this address as "valid".

SNMP ID:

2.70.3.1.2.6

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools > Valid-Lifetime

Possible values:

Maximum 10 characters.

Default:

86400

PD source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

SNMP ID:

2.70.3.1.2.7

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Address-Pools

Possible values:

Maximum 16 characters

Default:

Blank

PD pools

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers.

SNMP ID:

2.70.3.1.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools

PD pool name

Specify the name of the PD pool here.

SNMP ID:

2.70.3.1.3.1

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > PD-Pool-Name

Possible values:

Maximum 31 characters

Default:

Blank

Start PD pool

Here you specify the first prefix for delegation in the PD pool, e. g. "2001:db8:1100::"

SNMP ID:

2.70.3.1.3.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > Start-PD-Pool

Possible values:

Maximum 39 characters

Default:

Blank

End PD pool

Here you specify the last prefix for delegation in the PD pool, e. g. "2001:db8:FF00::"

SNMP ID:

2.70.3.1.3.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > PD-Pools > End-PD-Pool

Possible values:

Maximum 39 characters

Default:

Blank

Prefix length

Here you set the length of the prefixes in the PD pool, e. g. "56" or "60"

SNMP ID:

2.70.3.1.3.4

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > Prefix-Length****Possible values:**

Maximum 3 characters.

Default:

56

Preferred lifetime

Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".

SNMP ID:

2.70.3.1.3.5

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > Pref.-Lifetime****Possible values:**

Maximum 10 characters.

Default:

3600

Valid lifetime

Here you specify the time in seconds that the client should treat this prefix as "valid".

SNMP ID:

2.70.3.1.3.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools > Valid-Lifetime****Possible values:**

Maximum 10 characters.

Default:

86400

PD source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

SNMP ID:

2.70.3.1.3.7

Telnet path:**Setup > IPv6 > DHCPv6 > Server > PD-Pools****Possible values:**

Maximum 16 characters

Default:

Blank

Interface list

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.

SNMP ID:

2.70.3.1.4

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Interface name or relay

Name of the interface on which the DHCPv6 server is working, for example "INTRANET"

SNMP ID:

2.70.3.1.4.1

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Interface-Name

Possible values:

Selection from the list of LAN interfaces defined in the device; max. 39 characters

Default:

Blank

Operating

Activates or deactivates the DHCPv6 server.

SNMP ID:

2.70.3.1.4.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Operating

Possible values:

No

Yes

Default:

Yes

Primary DNS

IPv6 address of the primary DNS server.

SNMP ID:

2.70.3.1.4.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List > Primary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

Secondary DNS

IPv6 address of the secondary DNS server.

SNMP ID:

2.70.3.1.4.4

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-List > Secondary-DNS****Possible values:**

IPv6 address with max. 39 characters

Default:

Blank

Address pool name

Here you specify the address pool that the devices uses for this interface.



If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the table **Setup > IPv6 > DHCPv6 > Server > Address-Pools**.

SNMP ID:

2.70.3.1.4.5

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-List > Address-Pool-Name****Possible values:**

Maximum 31 characters

Default:

Blank

PD pool name

Determine the prefix-delegation pool that the devices is to use for this interface.



If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Setup > IPv6 > DHCPv6 > Server > PD-Pools**.

SNMP ID:

2.70.3.1.4.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Interface-List > PD-Pool-Name****Possible values:**


Maximum 31 characters

Default:

Blank

Rapid commit

With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

 The client must explicitly include the rapid commit option in its solicit message.

SNMP ID:

2.70.3.1.4.7

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-Liste > Rapid-Commit

Possible values:

No

Yes

Default:

No

Preference

Where multiple DHCPv6 servers are operated on the network, the preference parameter gives you the control over which server the clients will use. The primary server requires a higher preference value than the backup server.

SNMP ID:

2.70.3.1.4.8

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-Liste > Preference

Possible values:

0 to 255

Default:

0

Renew time

This specifies the time in seconds when the client should contact the server again (using a renew message) to extend the address/prefix received from the server. The parameter is also called T1.

SNMP ID:

2.70.3.1.4.9

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Possible values:

0 to 255

Default:

0 (automatic)

Rebind time

This specifies the time when the client should contact any server (using a rebind message) to extend its delegated address/prefix. The rebind event occurs only if the client receives no answer its renew request. The parameter is also called T2.

SNMP ID:

2.70.3.1.4.10

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Possible values:

0 to 255

Default:

0 (automatic)

Unicast address

Unicast address of the DHCP server. The DHCP server uses this address in the server unicast option to allow the client to communicate with to the server via unicast messages. By default, multicast is used.

SNMP ID:

2.70.3.1.4.11

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Possible values:

Valid unicast address

Default:

Blank

DNS search list

This parameter defines which DNS search list is sent to the clients by the DNS server.

SNMP ID:

2.70.3.1.4.12

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Possible values:

None: The DNS server distributes no search lists to the clients.

Internal: Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under IPv4 > DNS > General settings.

WAN: Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under Receive prefix from.

Default:

Internal

Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can define a reservation for each client in this table.

SNMP ID:

2.70.3.1.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server****Interface name or relay**

Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.

SNMP ID:

2.70.3.1.6.1

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations****Possible values:**

Selection from the list of LAN interfaces defined in the device; max. 39 characters

Default:

Blank

Address or PD prefix

IPv6 address or PD prefix that you want to assign statically.

SNMP ID:

2.70.3.1.6.2

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations****Possible values:**

Maximum 43 characters

Default:

Blank

Client ID

DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer be identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `ipconfig /all` or in WEBconfig under **Status > IPv6 > DHCPv6 > Client > Client ID**.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under **Status > IPv6 > DHCPv6 > Server > Address bindings**, and retrieved IPv6 prefixes are under **Status > IPv6 > DHCPv6 > Server > PD bindings**.

LANmonitor displays that client IDs under **DHCPv6 server**.

SNMP ID:

2.70.3.1.6.3

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations****Possible values:**

Maximum 96 characters

Default:

Blank

Preferred lifetime

Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".

SNMP ID:

2.70.3.1.6.5

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations****Possible values:**


Maximum 10 characters.

Default:

3600

Valid lifetime

Here you specify the time in seconds that the client should treat this prefix as "valid".

 If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for preferred lifetime and valid lifetime. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

SNMP ID:

2.70.3.1.6.6

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations****Possible values:**

Maximum 10 characters.

Default:

86400

PD source

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

SNMP ID:

2.70.3.1.6.7

Telnet path:**Setup > IPv6 > DHCPv6 > Server > Reservations**

Possible values:

Maximum 16 characters

Default:

Blank

Client

This menu contains the DHCP client settings for IPv6.

SNMP ID:


2.70.3.2

Telnet path:

Setup > IPv6 > DHCPv6 > Client

Interface list

This table determines the behavior of the DHCPv6 client.

 Normally client behavior is controlled by the auto-configuration.

SNMP ID:

2.70.3.2.1

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List

Interface name

Specify the name of the interface that the DHCPv6 client operates on. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

SNMP ID:

2.70.3.2.1.1

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Interface-Name

Possible values:

Selection from the list of LAN interfaces defined in the device; max. 16 characters

Default:

Blank

Operating

Here you specify if and how the device enables the client. Possible values are:

- **Autoconf:** The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
- **Yes:** The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements.
- **No:** The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

SNMP ID:

2.70.3.2.1.2

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Operating

Possible values:

Autoconf

No

Yes

Default:

Autoconf

Request DNS

Here you specify whether the client should query the DHCPv6 server for DNS servers.



You must enable this option in order for the device to obtain information about a DNS server.

SNMP ID:

2.70.3.2.1.3

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-DNS

Possible values:

No

Yes

Default:

Yes

Request address

Here you specify whether the client should query the DHCPv6 server for an IPv6 address.



Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i. e. not distributed by 'SLAAC'.

SNMP ID:

2.70.3.2.1.4

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-Address

Possible values:

No

Yes

Default:

Yes

Request PD

Here you specify whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This

option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

SNMP ID:

2.70.3.2.1.5

Telnet path:**Setup > IPv6 > DHCPv6 > Client > Interface-List > Request-PD****Possible values:**

No

Yes

Default:

No

Rapid commit

When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

SNMP ID:

2.70.3.2.1.6

Telnet path:**Setup > IPv6 > DHCPv6 > Client > Interface-List > Rapid-Commit****Possible values:**

No

Yes

Default:

Yes

User class identifier

This assigns the device a unique user class ID.

A user class identifier is used to identify the type or category of client to the server. For example, the user class identifier can be used to identify all clients of people in the accounting department, or all printers at a specific location.

SNMP ID:

2.70.3.2.2

Telnet path:**Setup > IPv6 > DHCPv6 > Client > User-Class-Identifier****Possible values:**

Maximum 253 characters

Default:

Blank

Vendor class identifier

This assigns the device a unique vendor class ID.

The vendor-class-identifier is used to identify the manufacturer of the hardware running the DHCP client.

SNMP ID:

2.70.3.2.3

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Vendor-Class-Identifier

Possible values:

Maximum 253 characters

Default:

Manufacturer name

Vendor class number

Determines the enterprise number that the device manufacturer used to register with the Internet Assigned Numbers Authority (IANA).

SNMP ID:

2.70.3.2.4

Telnet path:

Setup > IPv6 > DHCPv6 > Client

Possible values:

Maximum 10 characters

Default:

2356

5.6.4 Relay agent

This menu contains the DHCP relay agent settings for IPv6.

SNMP ID:

2.70.3.3

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent

Interface list

This table determines the behavior of the DHCPv6 relay agent.

SNMP ID:

2.70.3.3.1

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List

Interface name

Define the name of the interface on which the relay agent receives requests from DHCPv6 clients, e. g. "INTRANET".

SNMP ID:

2.70.3.3.1.1

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Interface-Name

Possible values:

Selection from the list of LAN interfaces defined in the device; max. 16 characters

Default:

Blank

Relay agent operating

With this option you define if and how the device enables the relay agent.

SNMP ID:

2.70.3.3.1.2

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Relay-Agent-Operating

Possible values:

Yes: Relay agent is enabled. This option is the default setting.

No: Relay agent is not enabled.

Default:

Yes

Interface address

Specify the relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.

SNMP ID:

2.70.3.3.1.3

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Interface-Address

Possible values:

Maximum 39 characters

Default:

Blank

Destination address

Define the IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

SNMP ID:

2.70.3.3.1.4

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Dest-Address

Possible values:

Maximum 39 characters

Default:

ff02::1:2

Destination interface

Here you specify the destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

SNMP ID:

2.70.3.3.1.5

Telnet path:

Setup > IPv6 > DHCPv6 > Relay-Agent > Interface-List > Dest-Interface

Possible values:

Maximum 39 characters

Default:

Blank

5.6.5 Network

Here you can adjust further IPv6 network settings for each logical interface supported by your device.

SNMP ID:

2.70.4

Telnet path:

Setup > IPv6 > Network

Addresses

This table is used to manage the IPv6 addresses.

SNMP ID:

2.70.4.1

Telnet path:

Setup > IPv6 > Network > Addresses

Interface name

Give a name to the interface that you want to assign the IPv6 network.

SNMP ID:

2.70.4.1.1

Telnet path:

Setup > IPv6 > Network > Addresses > Interface-Name

Possible values:


Max. 16 characters

Default:

Blank

IPv6 address prefix length

Specify an IPv6 address including the prefix length for this interface.

 The default prefix length is 64 bits ("/64"). If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device are designed for a maximum length of 64 bits.

A possible address is, for example, "2001:db8::1/64". An interface can have multiple IPv6 addresses:

- A "global unicast address", e. g. "2001:db8::1/64",
- A "unique local address", e. g. "fd00::1/64".

"Link local addresses" are fixed and not configurable.

SNMP ID:

2.70.4.1.2

Telnet path:

Setup > IPv6 > Network > Addresses > IPv6-Address-Prefixlength

Possible values:

Max. 43 characters

Default:


Blank

Address type

Determine the type of IPv6 address.

Using the address type **EUI-64** causes IPv6 addresses to be formed according to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64".

 "EUI-64" ignores any value set as "interface identifier" in the corresponding IPv6 address and replaces it with an "interface identifier" as per "EUI-64".

 The prefix length for "EUI-64" must be "/64".

SNMP ID:

2.70.4.1.3

Telnet path:

Setup > IPv6 > Network > Addresses > Address-Type

Possible values:


- Unicast
- Anycast
- EUI-64

Default:

Unicast

Name

Enter a descriptive name for this combination of IPv6 address and prefix.

 Entering a name is optional.

SNMP ID:

2.70.4.1.4

Telnet path:

Setup > IPv6 > Network > Addresses > Name

Possible values:


Max. 16 characters

Default:

Blank

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

SNMP ID:

2.70.4.1.5

Telnet path:

Setup > IPv6 > Network > Addresses > Comment

Possible values:

Max. 64 characters

Default:

Blank

Parameter

This table is used to manage the IPv6 parameters.

SNMP ID:

2.70.4.2

Telnet path:

Setup > IPv6 > Network > Parameter

Interface name

Give a name to the interface for which the IPv6 parameters are to be configured.

SNMP ID:

2.70.4.2.1

Telnet path:

Setup > IPv6 > Network > Parameter > Interface-Name

Possible values:


Max. 16 characters

Default:

Blank

IPv6 gateway

Specify the IPv6 gateway to be used by this interface.

 This parameter overrides gateway information that the device may receive via router advertisements, for example.

SNMP ID:

2.70.4.2.2

Telnet path:

Setup > IPv6 > Network > Parameter > IPv6-Gateway

Possible values:

- Global unicast address, e.g. 2001:db8::1
- Link-local address to which you add to the corresponding interface (%<INTERFACE>), e.g. fe80::1%INTERNET

Default:

::

Primary DNS

Specify the primary IPv6 DNS server to be used by this interface.

SNMP ID:

2.70.4.2.3

Telnet path:

Setup > IPv6 > Network > Parameter > Primary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

Secondary DNS

Specify the secondary IPv6 DNS server to be used by this interface.

SNMP ID:

2.70.4.2.4

Telnet path:

Setup > IPv6 > Network > Parameter > Secondary-DNS

Possible values:

IPv6 address with max. 39 characters

Default:

::

5.6.6 Firewall

This menu contains the settings for the firewall.

SNMP ID:

2.70.5

Telnet path:

Setup > IPv6 > Firewall

Operating

Enables or disables the firewall.



This item enables the firewall globally. The firewall is only active if you enable it here. If you disable the firewall here and at the same time enable it for individual interfaces, it remains disabled for all interfaces.

SNMP ID:

2.70.5.1

Telnet path:

Setup > IPv6 > Firewall > Operating

Possible values:

Yes

No

Default:

Yes

Forwarding rules

This table contains the rules that the firewall will apply for forwarding data.

SNMP ID:

2.70.5.2

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Name

Defines the name for the forwarding rule.

SNMP ID:

2.70.5.2.1

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Flags

These options determine how the firewall handles the rule. The options have the following meanings:

- **Deactivated:** The rule is disabled. The firewall skips this rule.
- **Linked:** After processing the rule, the firewall looks for additional rules which come in question.
- **Stateless:** This rule does not take the statuses of the TCP sessions into account.

You can select several options at the same time.

SNMP ID:

2.70.5.2.2

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:

Deactivated

Linked

Stateless

Default:

No selection

Priority

This information determines the priority with which the firewall applies the rule. A higher value determines a higher priority.

SNMP ID:

2.70.5.2.3

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:

Max. 4 characters from 1234567890

Default:

0

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

SNMP ID:

2.70.5.2.4

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:

Max. 5 characters from 1234567890

Default:

0

Action

Specifies the action that the firewall performs if the rule condition is true. There are certain standard actions already specified in the table **Setup IPv > IPv6 > Firewall > Actions**. In addition, you can also define your own actions.

You can enter multiple actions, separated by commas.

SNMP ID:

2.70.5.2.5

Telnet path:**Setup > IPv6 > Firewall > Forwarding-Rules****Possible values:**

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

Services

This information determines for which services the firewall applies this rule. There are certain services already specified in the table **Setup > IPv6 > Firewall > Actions**. In addition, you can also define your own services.

You can enter multiple services separated by commas.

SNMP ID:

2.70.5.2.7

Telnet path:**Setup > IPv6 > Firewall > Forwarding-Rules****Possible values:**

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

Source stations

This information determines for which source stations the firewall applies this rule. There are certain stations already specified in the table **Setup > IPv6 > Firewall > Stations**. In addition, you can also define your own stations.

You can enter multiple stations separated by commas.

SNMP ID:

2.70.5.2.8

Telnet path:**Setup > IPv6 > Firewall > Forwarding-Rules****Possible values:**

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

Destination stations

This information determines, for which destination stations the firewall applies this rule. There are certain stations already specified in the table **Setup > IPv6 > Firewall > Stations**. In addition, you can also define your own stations.

You can enter multiple stations separated by commas.

SNMP ID:

2.70.5.2.9

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{ }~!\$%&'()+-./:;<=>?[\]^_ .0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.70.5.2.10

Telnet path:

Setup > IPv6 > Firewall > Forwarding-Rules

Possible values:


Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{ }~!\$%&'()+-./:;<=>?[\]^_ .0123456789abcdefghijklmnopqrstuvwxyz`

Default:

Blank

Actions list

In this table, you can group actions. Define the actions you previously under **Setup > IPv6 > Firewall > Actions**.

 You can not delete an action in this list if the firewall is used in a forwarding or inbound rule.

SNMP ID:

2.70.5.3

Telnet path:

Setup > IPv6 > Firewall > Action-List

Name

Specifies the name of a group of actions.

SNMP ID:

2.70.5.3.1

Telnet path:**Setup > IPv6 > Firewall > Action-List****Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Description

Contains the list of actions that are grouped together under this group name.

Separate the individual entries with a comma.

SNMP ID:

2.70.5.3.2

Telnet path:**Setup > IPv6 > Firewall > Action-List****Possible values:**

Maximum 252 characters from:

#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

Blank

Station listYou can group stations in this table. Define the actions previously under **Setup > IPv6 > Firewall > Stations**.

You can not delete a station in this list if the firewall is used in a forwarding or inbound rule.

SNMP ID:

2.70.5.5

Telnet path:**Setup > IPv6 > Firewall > Stations-List****Name**

Specifies the name of a group of stations.

SNMP ID:

2.70.5.5.1

Telnet path:**Setup > IPv6 > Firewall > Stations-List****Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Description

Contains the list of stations that are grouped together under this group name.

Separate the individual entries with a comma.

SNMP ID:

2.70.5.5.2

Telnet path:

Setup > IPv6 > Firewall > Stations-List

Possible values:

Maximum 252 characters from:

#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

Blank

Service list

You can group services in this table. Define the services previously under **Setup > IPv6 > Firewall > Services**.



You can not delete a service in this list if the firewall is used in a forwarding or inbound rule.

SNMP ID:

2.70.5.6

Telnet path:

Setup > IPv6 > Firewall > Service-List

Name

Specifies the name of a group of services.

SNMP ID:

2.70.5.6.1

Telnet path:

Setup > IPv6 > Firewall > Service-List

Possible values:

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Description

Contains the list of services that are grouped together under this group name.

Separate the individual entries with a comma.

SNMP ID:

2.70.5.6.2

Telnet path:

Setup > IPv6 > Firewall > Service-List

Possible values:

Maximum 252 characters from:

#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+,-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

Blank

Actions

The firewall can perform the forwarding and inbound rule actions for the actions contained in this table.

You can combine multiple actions under **Setup > IPv6 > Firewall > Actions-list**.

SNMP ID:

2.70.5.7

Telnet path:

Setup > IPv6 > Firewall > Actions

Name

Specifies the name of the action.

SNMP ID:

2.70.5.7.1

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+,-./:;<=>?[\]^_0123456789

Default:

Blank

Limit

When this limit is exceeded, the firewall applies the filter rule.

SNMP ID:

2.70.5.7.2

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Max. 10 characters from 0123456789

Special values:

0: The rule will come into force immediately.

Default:

0

Unit

Determines the unit for the limits.

SNMP ID:

2.70.5.7.3

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

- kBit
- kByte
- Packets
- Sessions
- Bandwidth (%)

Default:

Packets

Time

Determines the measurement period that the firewall applies to the limit.

SNMP ID:

2.70.5.7.4

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

- Second
- Minute
- Hour
- Absolute

Default:

Absolute

Context

Determines the context that the firewall applies to the limit. Possible values are:

- **Session:** The limit only applies to the data traffic for the current session.
- **Station:** The limit only applies to the data traffic for the current station.
- **Global:** All sessions to which this rule applies use the same limit counter.

SNMP ID:

2.70.5.7.5

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

- Session
- Station
- Global

Default:

Session

Flags

Determines the properties of the limits of the action. Possible values are:

- **Reset:** If the limit is exceeded, the action resets the counter.
- **Shared:** All rules to which this limit applies use the same limit counter.

SNMP ID:

2.70.5.7.6

Telnet path:**Setup > IPv6 > Firewall > Actions****Possible values:**

Reset

Shared

Default:

Blank

Action

Determines the action the firewall performs when the limit is reached.

The following options are possible:

- **Reject:** The firewall rejects the data packet and sends an appropriate notification to the sender.
- **Drop:** The firewall discards the data packet without notification.
- **Accept:** The firewall accepts the data packet.

SNMP ID:

2.70.5.7.7

Telnet path:**Setup > IPv6 > Firewall > Actions****Possible values:**

Reject

Drop


Accept

Default:

.

DiffServ

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

SNMP ID:

2.70.5.7.11

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

- BE
- EF
- CS0 to CS7
- AF11 to AF43
- No
- Value

Special values:

Value: You can enter the DSCP decimal value directly in the **DSCP value** field.


Default:

No

DSCP value

Determines the value for the Differentiated Services Code Point (DSCP).

If you selected the "Value" option in the **DiffServ** field, enter a value here.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

SNMP ID:

2.70.5.7.12

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Max. 2 characters from 1234567890

Default:

0

Conditions

Determines which conditions must be met in order for the action to be performed. Define the conditions under **Setup > IPv6 > Firewall > Conditions**.

SNMP ID:

2.70.5.7.13

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+,./:;<=>?[\^_ .0123456789

Default:

Blank

Trigger actions

Determines which trigger actions the firewall should start in addition to filtering the data packets. Define the trigger actions under **Setup > IPv6 > Firewall > Trigger-actions**.

SNMP ID:

2.70.5.7.14

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./,:;<=>?[\]^_0123456789

Default:

Blank

Stations

The firewall can perform the forwarding and inbound rule actions for inbound connections from the source stations listed in this table.

You can combine multiple stations under **Setup > IPv6 > Firewall > Station-list**.

SNMP ID:

2.70.5.9

Telnet path:

Setup > IPv6 > Firewall > Stations

Name

Specifies the name of the station.

SNMP ID:

2.70.5.9.1

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./,:;<=>?[\]^_0123456789

Default:

Blank

Type

Determines the station type.

SNMP ID:

2.70.5.9.2

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

Local network

5 IPv6

Remote peer

Prefix

Identifier

IP address

Named host

Default:

Local network

Local network

If you selected the appropriate option in the **Type** field, you enter the name of the local network here.

SNMP ID:

2.70.5.9.3

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

Max. 16 characters from: #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Remote peer/local host

If you selected the appropriate option in the **Type** field, you enter the name of the remote peer or local host here.

SNMP ID:

2.70.5.9.6

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

Maximum 64 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789

Default:

Blank

Address/Prefix

If you selected the appropriate option in the **Type** field, enter the IP address or prefix of the station here.

SNMP ID:

2.70.5.9.7

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

Max. 43 characters from ABCDEFabcdef0123456789:

Default:

Blank

Services

The firewall can perform the forwarding and inbound rule actions for the connection protocols of the services listed in this table.

You can combine multiple services under **Setup > IPv6 > Firewall > Service-list**.

SNMP ID:

2.70.5.10

Telnet path:

Setup > IPv6 > Firewall > Services

Name

Specifies the name of the service.

SNMP ID:

2.70.5.10.1

Telnet path:

Setup > IPv6 > Firewall > Services

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()*+,-./:;<=>?[\]^_0123456789

Default:

Blank

Protocol

Specifies the protocol of the service.

SNMP ID:

2.70.5.10.2

Telnet path:

Setup > IPv6 > Firewall > Services

Possible values:

TCP+UDP

TCP

UDP

Default:

TCP+UDP

Ports

Specifies the port for the service. Separate multiple ports with a comma.



Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

SNMP ID:

2.70.5.10.3

Telnet path:

Setup > IPv6 > Firewall > Services

Possible values:

Max. 64 characters from 0123456789,

Default:

Blank

Source ports

Determines whether the specified ports are source ports.

 In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

SNMP ID:

2.70.5.10.4

Telnet path:

Setup > IPv6 > Firewall > Stations

Possible values:

No
Yes

Default:

No

Protocol

The firewall can perform the forwarding and inbound rule actions for the protocols listed in this table.

SNMP ID:

2.70.5.11

Telnet path:

Setup > IPv6 > Firewall > Protocols

Name

Specifies the name of the protocol.

SNMP ID:

2.70.5.11.1

Telnet path:

Setup > IPv6 > Firewall > Protocols

Possible values:


Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+,./:;<=>?[\\]^_0123456789

Default:

Blank

Protocol

Specifies the protocol number.

 Lists with the official protocol and port numbers are available in the Internet at [.http://www.iana.org](http://www.iana.org).

SNMP ID:

2.70.5.11.2

Telnet path:**Setup > IPv6 > Firewall > Protocols****Possible values:**

Max. 3 characters from 0123456789

Default:

Blank

Conditions

The firewall can perform the forwarding and inbound rule actions for the conditions listed in this table.

SNMP ID:

2.70.5.12

Telnet path:**Setup > IPv6 > Firewall > Conditions****Name**

Specifies the name of the condition.

SNMP ID:

2.70.5.12.1

Telnet path:**Setup > IPv6 > Firewall > Conditions****Possible values:**

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+,./:;<=>?[\]^_0123456789

Default:

Blank

Conditions

Specifies the conditions which must be met.

SNMP ID:

2.70.5.12.2

Telnet path:**Setup > IPv6 > Firewall > Conditions****Possible values:**

Not connected

Default route

Backup connection

VPN route

Transmitted

Received

Default:

Blank

Transport direction

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

SNMP ID:

2.70.5.12.3

Telnet path:

Setup > IPv6 > Firewall > Conditions

Possible values:

Physical

Logical

Default:

Physical

DiffServ

Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

SNMP ID:

2.70.5.7.11

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

BE

EF

CS0 to CS7, CSx

AF11 to AF43, AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx

No

Value

Special values:

CSx: Extends the range to all class selectors.

AF1x, AF2x, AF3x, AF4x, AFx1, AFx2, AFx3, AFxx: Extends the range to the corresponding assured-forwarding classes (e.g., AF1x takes the classes AF11, AF12, AF13 into account)

Value: You can enter the DSCP decimal value directly in the **DSCP value** field.


Default:

Ignore

DSCP value

Determines the value for the Differentiated Services Code Point (DSCP).

If you selected the "Value" option in the **DiffServ** field, enter a value here.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

SNMP ID:

2.70.5.12.5

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

Max. 2 characters from 1234567890

Default:

0

Trigger actions

This table contains a list of the trigger actions, which the firewall actions can start.

SNMP ID:

2.70.5.13

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Name

Specifies the name of the trigger action.

SNMP ID:

2.70.5.13.1

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:


Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()*+,-./:;<=>?[\]^_ .0123456789

Default:

Blank

Notifications

Determines whether and how a notification should be sent.

 If you want to receive e-mail notifications, you must enter an e-mail address in **Setup > IP-Router > Firewall > Admin-Email**.

SNMP ID:

2.70.5.13.2

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

SNMP
Syslog
E-mail

Default:

Blank

Disconnect

Determines whether the firewall disconnects the connection to the remote station if the filter condition is true.

SNMP ID:

2.70.5.13.3

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

No
Yes

Default:

No

Block source

Determines whether the firewall disconnects the source if the filter condition is true. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the **Host-lock-list** under **Status > IPv6 > Firewall**.

SNMP ID:

2.70.5.13.4

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

No
Yes

Default:

No

Lockout period

Specifies how many minutes the firewall blocks the source.

SNMP ID:

2.70.5.13.5

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

Max. 8 characters from 0123456789

Special values:

0: Disables the lock because, in practice, the lockout period expires after 0 minutes.

Default:

0

Close destination

Specifies whether the firewall disconnects the source if the filter condition is true. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the **Port-block-list** under **Status > IPv6 > Firewall**.

SNMP ID:

2.70.5.13.6

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

No

Yes

Default:

No

Closing time

Determines, for how many seconds the firewall closes the destination.

SNMP ID:

2.70.5.13.7

Telnet path:

Setup > IPv6 > Firewall > Trigger-Actions

Possible values:

Max. 8 characters from 0123456789

Special values:


0: Disables the lock because, in practice, the lockout period expires after 0 minutes.

Default:

0

ICMP service

This table contains a list of ICMP-service.

 Since ICMPv6 has central importance for numerous IPv6 features, basic ICMPv6 rules are already configured by default. You can not delete these rules.

SNMP ID:

2.70.5.14

Telnet path:

Setup > IPv6 > Firewall > ICMP-Services

Name

Specifies the name of the ICMP service.

SNMP ID:

2.70.5.14.1

Telnet path:

Setup > IPv6 > Firewall > ICMP-Services

Possible values:

Maximum 32 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()*+,-./:;<=>?[\]^_0123456789

Default:

Blank

Type

Specifies the type of the ICMP service.

 Lists with the official ICMP types and port codes are available in the Internet under www.iana.org.

SNMP ID:

2.70.5.14.2

Telnet path:

Setup > IPv6 > Firewall > ICMP-Services

Possible values:

Max. 3 characters from 0123456789

Default:

0

Code

Specifies the codes of the ICMP service.

 Lists with the official ICMP types and port codes are available in the Internet under www.iana.org.

SNMP ID:

2.70.5.14.2

Telnet path:

Setup > IPv6 > Firewall > ICMP-Services

Possible values:

Max. 3 characters from 0123456789

Default:

0

Inbound rules

This table contains the rules that the firewall will apply to inbound connections.

By default, there are already some rules for the most important cases.

SNMP ID:

2.70.5.15

Telnet path:**Setup > IPv6 > Firewall > Inbound-Rules****Name**

Specifies the name of the inbound rule.

SNMP ID:

2.70.5.15.1

Telnet path:**Setup > IPv6 > Firewall > Inbound-Rules****Possible values:**

Maximum 36 characters from: ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()*+,-./:;<=>?[\\]^_0123456789

Default:

Blank

Operating

This option enables the inbound rule.

SNMP ID:

2.70.5.15.2

Telnet path:**Setup > IPv6 > Firewall > Inbound-Rules****Possible values:**

Yes

No

Default:

Yes

Priority

This information determines the priority with which the firewall applies the rule. A higher value determines a higher priority.

SNMP ID:

2.70.5.15.3

Telnet path:**Setup > IPv6 > Firewall > Inbound-Rules****Possible values:**

Max. 4 characters from 1234567890

Default:

0

Action

Specifies the action that the firewall performs if the rule condition is true. There are certain standard actions already specified in the table **Setup IPv > IPv6 > Firewall > Actions**. In addition, you can also define your own actions.

SNMP ID:

2.70.5.15.5

Telnet path:

Setup > IPv6 > Firewall > Inbound-Rules

Possible values:

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

REJECT

Services

This information determines for which services the firewall applies this rule. There are certain services already specified in the table **Setup > IPv6 > Firewall > Actions**. In addition, you can also define your own services.

SNMP ID:

2.70.5.15.7

Telnet path:

Setup > IPv6 > Firewall > Inbound-Rules

Possible values:

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANY

Source stations

This information determines for which source stations the firewall applies this rule. There are certain stations already specified in the table **Setup > IPv6 > Firewall > Stations**. In addition, you can also define your own stations.

SNMP ID:

2.70.5.15.8

Telnet path:

Setup > IPv6 > Firewall > Inbound-Rules

Possible values:

Maximum 64 characters from:
 #ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

ANYHOST

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.70.5.15.10

Telnet path:**Setup > IPv6 > Firewall > Inbound-Rules****Possible values:**

Maximum 64 characters from:

#ABCDEFGHIJKLMNOPQRSTUVWXYZ@{ }~!\$%&'()+-./:;<=>?[\]^_0123456789abcdefghijklmnopqrstuvwxyz`

Default:

Blank

5.6.7 LAN interfaces

This table contains the settings for the LAN interfaces.

SNMP ID:

2.70.6

Telnet path:**Setup > IPv6 > LAN-Interfaces****Interface name**

Enter a name for the logical IPv6 interface that is defined by the physical interface (interface assignment) and the VLAN ID.

SNMP ID:

2.70.6.1

Telnet path:**Setup > IPv6 > LAN-Interfaces > Interface-Name****Possible values:**

Max. 16 characters

Default:

Blank

Interface ID

Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface.

SNMP ID:

2.70.6.2

Telnet path:**Setup > IPv6 > LAN-Interfaces > Interface-ID****Possible values:**


All physically available interfaces on the device

Default:

LAN-1

VLAN ID

Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.

 If you enter an invalid VLAN ID here, no communication will take place.

SNMP ID:

2.70.6.3

Telnet path:

Setup > IPv6 > LAN-Interfaces > VLAN-ID

Possible values:

0 to 4096

Max. 4 numbers

Default:

0

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.6.4

Telnet path:

Setup > IPv6 > LAN-Interfaces > Rtg-Tag

Possible values:


Max. 5 characters in the range 0 – 65535

Default:

0

Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.

 If the device sends router advertisements from this interface, it does not generate any IPv6 addresses even with auto-configuration enabled.

SNMP ID:

2.70.6.5

Telnet path:

Setup > IPv6 > LAN-Interfaces > Autoconf

Possible values:

Yes

No

Default:

Yes

Accept RA

Enables or disables the processing of received router advertisement messages.



With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

SNMP ID:

2.70.6.6

Telnet path:**Setup > IPv6 > LAN-Interfaces > Accept-RA****Possible values:**

Yes

No

Default:

Yes

Interface status

Enables or disables this interface.

SNMP ID:

2.70.6.7

Telnet path:**Setup > IPv6 > LAN-Interfaces > Interface-Status****Possible values:**

Up

Down

Default:

Up

Forwarding

Enables or disables the forwarding of data packets to other interfaces.



With forwarding disabled, no router advertisements are transmitted from this interface.

SNMP ID:

270.6.8

Telnet path:**Setup > IPv6 > LAN-Interfaces > Forwarding****Possible values:**

Yes

No

Default:

Yes

MTU

Specify the applicable MTU for this interface.

SNMP ID:

2.70.6.9

Telnet path:**Setup > IPv6 > LAN-Interfaces > MTU****Possible values:**

Max. 4 numbers in the range 0 – 9999

Default:

1500

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here. To enable the firewall globally for all interfaces, select **IPv6 firewall/QoS enabled** in the menu **Firewall/QoS > General** .



If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

SNMP ID:

2.70.6.10

Telnet path:**Setup > IPv6 > LAN-Interfaces > Firewall****Possible values:**

Yes

No

Default:

No

Comment

Enter a descriptive comment for this entry.



Entering a comment is optional.

SNMP ID:

2.70.6.11

Telnet path:**Setup > IPv6 > LAN-Interfaces > Comment****Possible values:**

Max. 64 characters

Default:

Blank

5.6.8 WAN interfaces

This table contains the settings for the LAN interfaces.

SNMP ID:

2.70.7

Telnet path:**Setup > IPv6 > WAN-Interfaces**

Interface name

Specify the name of the WAN remote peer here. Use the name as specified at the remote site.

SNMP ID:

2.70.7.1

Telnet path:**Setup > IPv6 > WAN-Interfaces > Interface-Name****Possible values:**

Max. 16 characters

Default:

Blank

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.7.2

Telnet path:**Setup > IPv6 > WAN-Interfaces > Rtg-Tag****Possible values:**

Max. 5 characters in the range 0 – 65534

Default:

0

Autoconf

Enable or disable "stateless address autoconfiguration" for this interface.



If the device sends router advertisements from this interface, it does not generate any addresses even with auto-configuration enabled.

SNMP ID:

2.70.7.3

Telnet path:

Setup > IPv6 > WAN-Interfaces > Autoconf

Possible values:

Yes

No

Default:

Yes

Accept RA

Enables or disables the processing of received router advertisement messages.



With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.

SNMP ID:

2.70.6.6

Telnet path:

Setup > IPv6 > WAN-Interfaces > Accept-RA

Possible values:

Yes

No

Default:

Yes

Interface status

Enables or disables this interface.

SNMP ID:

2.70.7.5

Telnet path:

Setup > IPv6 > WAN-Interfaces > Interface-Status

Possible values:

Up

Down

Default:

Up

Forwarding

Enables or disables the forwarding of data packets to other interfaces.

SNMP ID:

2.70.7.6

Telnet path:

Setup > IPv6 > WAN-Interfaces > Forwarding

Possible values:

Yes

No

Default:

Yes

Firewall

Enables the firewall for this interface.



If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

SNMP ID:

2.70.7.7

Telnet path:

Setup > IPv6 > WAN-Interfaces > Firewall

Possible values:

Yes

No

Default:

Yes

Comment

Enter a descriptive comment for this entry.



Entering a comment is optional.

SNMP ID:

2.70.7.8

Telnet path:

Setup > IPv6 > WAN-Interfaces > Comment

Possible values:

Max. 64 characters

Default:

Blank

DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way the device avoids address conflicts on the network.

This option specifies the number of times that the device attempts to find duplicate IPv6 addresses on the network.

Telnet path:**Setup > IPv6 > WAN-Interfaces > DaD-Attempts****Possible values:**

Max. 1 number

Default:

1

5.6.9 Operating

Switches the IPv6 stack on or off, globally. With the IPv6 stack deactivated, the device does not perform any IPv6-related functions.

SNMP ID:

2.70.10

Telnet path:**Setup > IPv6 > Operating****Possible values:**

Yes

No

Default:

No

5.6.10 Forwarding

If forwarding is turned off, the device transmits no data packets between IPv6 interfaces.



Forwarding is essential if you wish to operate the device as a router.

SNMP ID:

2.70.11

Telnet path:**Setup > IPv6 > Forwarding****Possible values:**

Yes

No

Default:

Yes

5.6.11 Router

These are the router settings.

SNMP ID:

2.70.12

Telnet path:

Setup > IPv6 > Router

Routing table

The table contains the entries to be used for routing packets with IPv6 addresses.

SNMP ID:

2.70.12.1

Telnet path:

Setup > IPv6 > Router > Routing-Table

Prefix

This prefix denotes the network range from which the current remote site, e.g. 2001:db8::/32, is to receive data

SNMP ID:

2.70.12.1.1

Telnet path:

Setup > IPv6 > Router > Routing-Table > Prefix

Possible values:

Max. 43 characters

Default:

Blank

Routing tag

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.



Routing tags are only necessary if used in combination with routing tags as set by firewall rules or as set at an interface.

SNMP ID:

2.70.12.1.2

Telnet path:

Setup > IPv6 > Router > Routing-Table > Routing-Tag

Possible values:

Max. 5 characters

Default:

Blank

Peer or IPv6

This is where you specify the remote site for this route. Enter one of the following options:

- An interface name
- An IPv6 address (e.g. 2001:db8::1)
- An interface supplemented with a link-local address (e.g. fe80::1%INTERNET)

 The device stores the remote sites for IPv6 routing as (*WAN interfaces*).

SNMP ID:

2.70.12.1.3

Telnet path:**Setup > IPv6 > Router > Routing-Table > Peer-or-IPv6****Possible values:**


Max. 56 characters

Default:

Blank

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

SNMP ID:

2.70.12.1.4

Telnet path:**Setup > IPv6 > Router > Routing-Table > Comment****Possible values:**

Max. 64 characters

Default:

Blank

Destination cache timeout

The 'destination cache timeout' specifies how long the device remembers the path to a destination address when no packets are sent to it.

This value also influences the length of time the device takes to change the settings of the firewall: It accepts state changes after at least half of the 'destination cache timeout' time, on average after one quarter of the timeout. Thus with the default setting of 30 seconds, changes to the firewall come into effect on average after 7.5 seconds, but no later than after 15 seconds.

SNMP ID:

2.70.12.2

Telnet path:**Setup > IPv6 > Router > Dest.-Cache-Timeout****Possible values:**

Max. 3 characters

Default:

30 seconds

5.6.12 IPv6 address

Enter the IPv6 address of the station.

If a client needs to resolve the name of a station, it sends a request with that name to the DNS server. The server responds by communicating the IPv6 address entered here.

SNMP ID: 2.17.5.3

Telnet path: /Setup/DNS/DNS-List

Possible values:

- Valid IPv6 address.

Default: Blank

5.7 Additions to the Status menu

5.7.1 Log table

This table contains a list of all IPv6 firewall events.

SNMP ID:

1.77.9.1

Telnet path:

Status > IPv6 > Firewall

Idx.

Sequential index. Furthermore, the table can also be checked via SNMP.

System time

System time in UTC encoding (converted to plain text for display).

Source address

Source address of the filtered packet.

Destination address

Destination address of the filtered packet.

Prot.

Protocol (TCP, UDP, etc.) of the filtered packets.

Source port

Source port of the filtered packet (only for port related protocols).

Destination port

Destination port of the filtered packet (only for port related protocols).

Filter rule

Name of the rule that created the entry.

Limit

Bit field that contains the description of the limit that caused the firewall to apply the filter. There following values are currently defined:

- 0x01: Absolute number
- 0x02: Number per second
- 0x04: Number per minute
- 0x08: Number per hour:
- 0x10: Global limit
- 0x20: Byte limit (if not set, it is a packet limit)
- 0x40: Limit only applies in the inbound direction
- 0x80: Limit only applies in the outbound direction

Threshold

Threshold limit value of the triggering limit.

Action

Bit field which lists all the actions performed. There following values are currently defined:

- 0x00000001: Accept
- 0x00000100: Reject
- 0x00000200: Establish filter
- 0x00000400: Internet (default router) filter
- 0x00000800: Drop
- 0x00001000: Disconnect
- 0x00004000: Lock source address
- 0x00020000: Lock destination address and port
- 0x20000000: Send SYSLOG notification message
- 0x40000000: Send SNMP trap
- 0x80000000: Send e-mail

5.8 Additional command-line commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- *IPv6 addresses*: `show ipv6-addresses`
- *IPv6 prefixes*: `show ipv6-prefixes`
- *IPv6 interfaces*: `show ipv6-interfaces`
- *IPv6 neighbor cache*: `show ipv6-neighbor-cache`
- *IPv6 DHCP*: `show dhcp6-server`
- *IPv6 DHCP*: `show dhcpv6-client`
- *IPv6 route*: `show ipv6-route`

5.8.1 IPv6 addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80 :`.

The output is formatted as follows:

<Interface> :
 <IPv6 address>, <status>, <attribute>, (<type>)

Table 2: Components of the command-line output `show ipv6-addresses`:

Output	Comment
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	The status field can contain the following values: <ul style="list-style-type: none"> ■ TENTATIVE Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. ■ PREFERRED The address is valid ■ DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. ■ INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	Shows an attribute of the IPv6 address. Possible attributes are: <ul style="list-style-type: none"> ■ None No special attributes ■ (ANYCAST) This is an anycast address ■ (AUTO CONFIG) The address was retrieved by auto-configuration ■ (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

5.8.2 IPv6 prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

- **Delegated prefixes:** All prefixes that the router has obtained by delegation.
- **Advertised prefixes:** All prefixes that the router announces in its router advertisements.
- **Deprecated prefixes:** All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

5.8.3 IPv6 interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

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

Table 3: Components of the command-line output `show ipv6-interfaces`:

Output	Comment
Interface	The name of the interface
Status	The status of the interface. Possible entries are: <ul style="list-style-type: none"> ■ oper status is up ■ oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: <ul style="list-style-type: none"> ■ forwarding is enabled ■ forwarding is disabled
Firewall	The status of the firewall. Possible entries are: <ul style="list-style-type: none"> ■ forwarding is enabled ■ firewall is disabled

5.8.4 IPv6 neighbor cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>

Table 4: Components of the command-line output `show ipv6-neighbor-cache`:

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)
Status	The status of the connection to neighboring devices. Possible entries are: <ul style="list-style-type: none"> ■ INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. ■ REACHABLE The neighbor was reached in the last ten seconds. ■ STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. ■ DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols.

Output	Comment
	<ul style="list-style-type: none"> ■ PROBE <p>The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.</p>
Source	The IPv6 address at which the neighbor was detected.

5.8.5 IPv6 DHCP server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

5.8.6 IPv6 DHCP client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and the prefixes and DNS server that it is using.

5.8.7 IPv6 route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

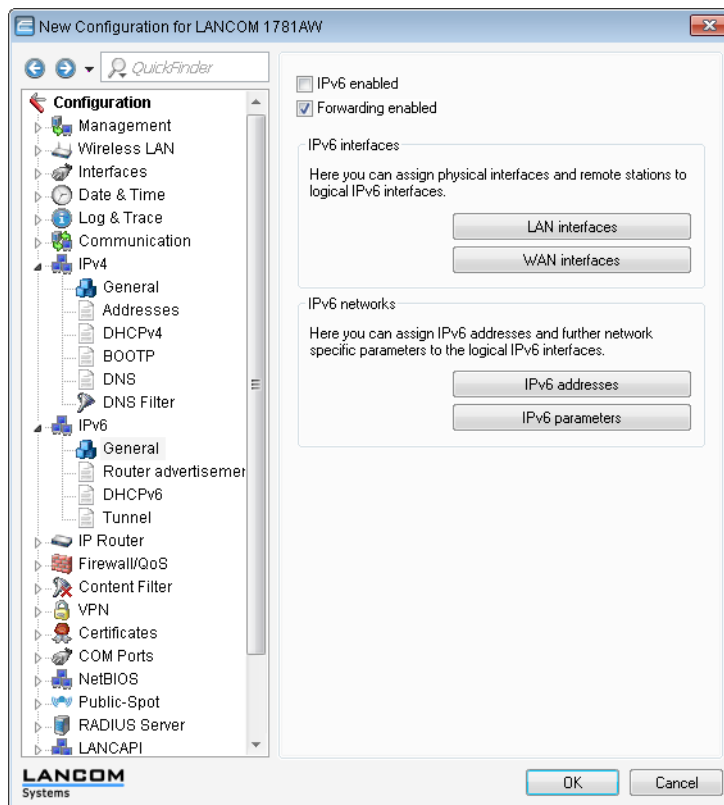
5.8.8 Release IPv6 address

Command	Description
Release [-x] <Interface 1> ... <Interface n>	<p>The DHCPv6 client returns its IPv6 address and/or its prefix to the DHCPv6 server. It then submits a new request for an address or prefix to the DHCPv6 server. Depending on the provider, the server assigns a new address to the client, or reassigns the previous one. Whether the client receives a different address or prefix is determined solely by the server.</p> <p>The option switch <code>-x</code> suppresses the confirmation message.</p> <p>The <code>*</code> wildcard applies the command on all of the interfaces and prefix delegations.</p>

5.9 Enhancements to LANconfig

5.9.1 IPv6 configuration menu

Where previous versions provided configuration menus for TCP/IP for IPv4, you now find the options **IPv4** and **IPv6**.



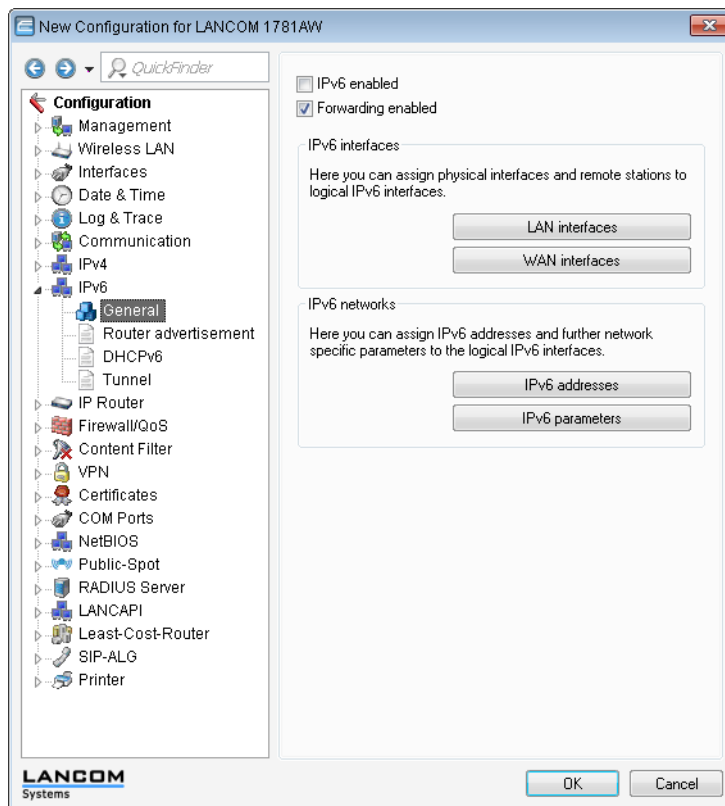
Click on **IPv6** to adjust the settings for this protocol. The configuration dialog **IPv6** is divided into the options **General**, **Router advertisement** and **Tunnel**. By default a click on **IPv6** takes you straight to the *General* options.

General

This is where you make the basic settings.

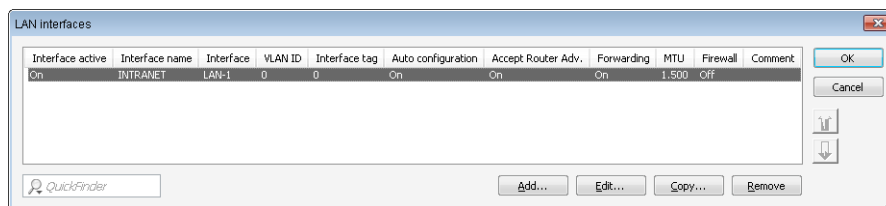
- **IPv6 enabled:** This is where you can enable or disable IPv6 for the device.

- **Forwarding enabled:** Forwarding is used for packet forwarding between IPv6 interfaces. This option is activated by default.



- The buttons **LAN interfaces** and **WAN interfaces** access the tables where you can add new interfaces, configure existing interfaces, or delete them.

For each existing IPv4 network, you must create an equivalent IPv6 network under **LAN interfaces**. Here, the settings for interface binding, routing tag, and VLAN ID must match the settings of the corresponding IPv4 network settings. Because a device can have multiple IPv6 addresses, you must add statically configured IPv6 addresses under **IPv6 addresses**.

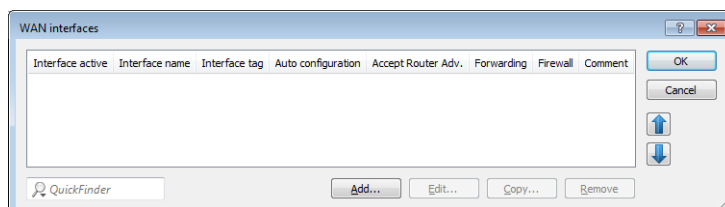


Entries in the **LAN interfaces** table have the following meaning:

- **Interface active:** Activates or deactivates this LAN interface.
- **Interface name** or **Network name:** Enter a name for the logical IPv6 interface which is to apply to the physical interface (interface assignment) and the VLAN ID.
- **Interface:** Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface. With IPv6, the mapping "any" used with IPv4 is no longer possible.
- **VLAN-ID:** Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.
- **Interface tag:** The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

- **Auto-configuration:** Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.
-
- ❗ If the device itself sends router advertisements from this interface, it does not produce IPv6 addresses from received router advertisements from other routers, even when auto-configuration is enabled.
- **Accept router advertisements:** Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
 - **Forwarding:** Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
 - **MTU:** Here you set the valid MTU for the corresponding link.
 - **Firewall:** If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
 - **Comment:** Enter a descriptive comment for this entry.

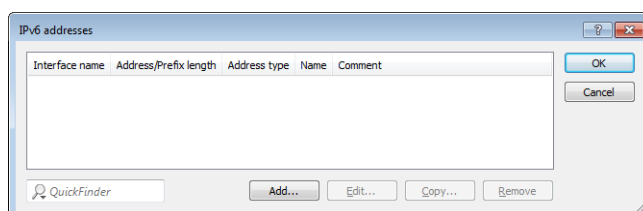
For each remote station with which you want to communicate using IPv6, you must additionally create an equivalent logical IPv6 WAN interface under **WAN interfaces**. The name of the IPv6 WAN interface must match the name of the IPv4 remote station.



Entries in the **WAN interfaces** table have the following meaning:

- **Interface active:** Activates or deactivates this WAN interface.
- **Interface name:** The name of the logical IPv6 interface must match that of the corresponding IPv4 connection.
- **Interface tag:** The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- **Auto-configuration:** Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.
- **Accept router advertisements:** Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
- **Forwarding:** Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
- **Firewall:** If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
- **Comment:** Enter a descriptive comment for this entry.
- The buttons **IPv6 addresses** and **IPv6 parameters** are used to assign IPv6 addresses to interfaces and to configure the interface parameters (gateway address, primary and secondary DNS).

The **IPv6 addresses** table is used to create IPv6 addresses for LAN and WAN interfaces.



Entries in the **IPv6 addresses** table have the following meaning:

- **Interface name:** Give a name to the interface that you want to assign the IPv6 network.
- **Address/prefix length:** Specify an IPv6 address including the prefix length for this interface.

The default prefix length is 64 bits ("/64"). If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device (e. g. autoconfiguration) are designed for a maximum length of 64 bits.

Example:

- Global unicast address: "2001:db8::1/64"
- Unique local address: "fd00::1/64"

! Link-local addresses are fixed and not configurable.

- **Address type:** Determine the type of IPv6 address.

Options:

- Unicast
- Anycast
- EUI-64

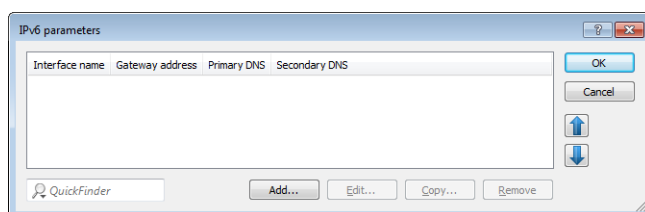
With the address type EUI-64, IPv6 addresses conform to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64". "EUI-64" ignores any value set as interface identifier in the corresponding IPv6 address and replaces it with an interface identifier as per "EUI-64". The prefix length for "EUI-64" must be "/64".

With the Unicast address type, you use the **Address/prefix length** field to specify a full IPv6 address along with its interface identifier, e. g. "2001:db8::1234/64".

With the Anycast address type, you can also use the **Address/prefix length** field to specify a full IPv6 address along with its interface identifier, e. g. "2001:db8::1234/64". Internally, the device handles this address as an anycast address.

- **Name:** Enter a descriptive name for this combination of IPv6 address and prefix.
- **Comment:** Enter a descriptive comment for this entry.

The table **IPv6 parameters** is used to manually configure static parameters for LAN or WAN interfaces, IPv6 DNS servers, and IPv6 gateways if you choose not to use autoconfiguration or DHCPv6.



Entries in the **IPv6 parameters** table have the following meaning:

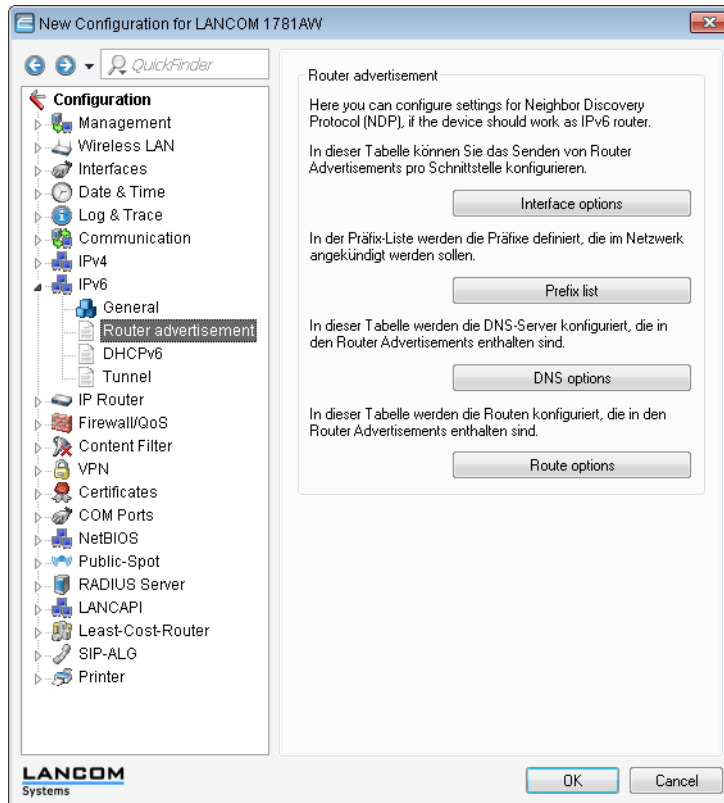
- **Interface name:** Give a name to the interface for which the IPv6 parameters are to be configured.
- **Gateway address:** Specify the IPv6 gateway to be used by this interface.

! This parameter overrides gateway information that the device may receive via router advertisements, for example.

- **Primary DNS:** Specify the primary IPv6 DNS server to be used by this interface.
- **Secondary DNS:** Specify the secondary IPv6 DNS server to be used by this interface.

Router advertisement

The **Router advertisement** configuration provides you with four buttons for setting up the Neighbor Discovery Protocol (NDP) if the device is to operate as an IPv6 router:



Each button opens a table with the settings for the corresponding function:

- **Interface options:** Enable or disable the following interface features:
 - **Send router advertisements:** Regulates the periodic transmission of router advertisements and the response to router solicitations.
 - **Managed address configuration flag:** With this function enabled, clients receiving this router advertisement will configure their addresses with Stateful Autoconfiguration (DHCPv6). Clients then automatically retrieve other information, such as the DNS server.
 - **Other flag:** If this function is active, a client will attempt to obtain additional information via DHCPv6, such as DNS server addresses.

For each prefix, you can specify whether or not a client should form addresses by auto-configuration: Navigate to the **Prefix list** under **Allow auto-configuration (SLAAC)**.

- **Default router:** Defines how the device advertises itself as the default gateway or router.

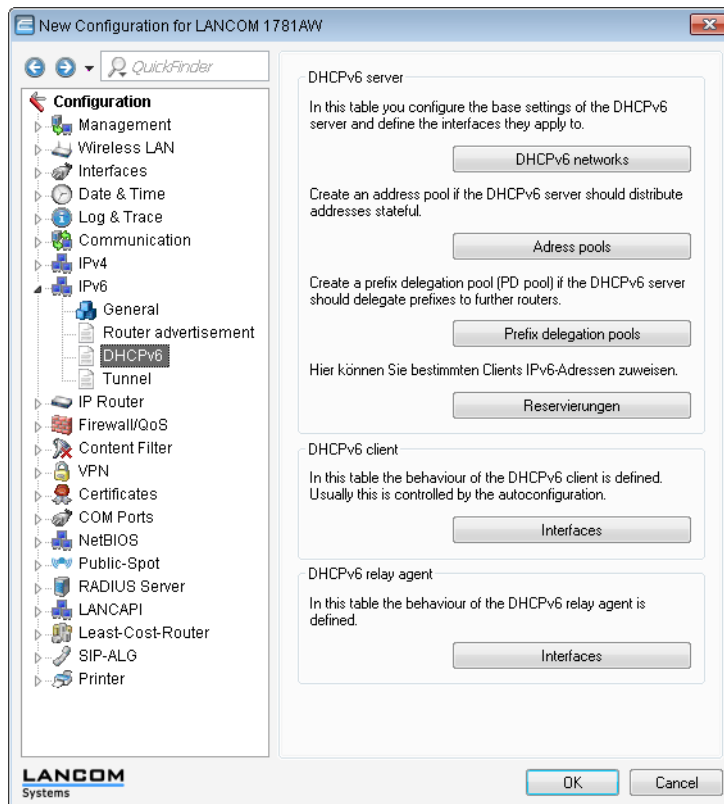
The parameters have the following functions:

- ▶ "Automatic": As long as a WAN connection exists, the device sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway.
If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway.
- ▶ "Always": The router lifetime is always positive—i. e. greater than "0"—irrespective of the WAN connection status.
- ▶ "Never": The router lifetime is always "0".

- **Router priority:** Defines the preference of this router. Clients enter this preference into their local routing tables.
- **Prefix list:** Set the prefix options for the interfaces that are being used. The following settings are possible:
 - **Prefix:** Enter a prefix that is announced in the router advertisements, e. g. "2001:db8::/64". The prefix length must always be exactly "/64", otherwise it will be impossible for clients to generate their addresses by adding their interface identifiers (with a length of 64 bits). If a prefix delegated by the provider is to be propagated automatically, set "::/64" here and enter the name of the corresponding WAN interface as the parameter **Receive prefix from**.
 - **Subnet ID:** Here you enter the subnet ID that is to be combined with the prefix delegated by the provider. If the provider assigns the prefix "2001:db8:a::/48", for example, and the subnet ID is "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64". The maximum subnet length with a 48-bit long delegated prefix is 16 bits (i.e. 65,536 subnets), with available subnet IDs ranging from "0000" to "FFFF". With a delegated prefix of "/56", the maximum subnet length is 8 bits (i.e. 256 subnets) with subnet IDs ranging from "00" to "FF". In general, the subnet ID "0" is used when the WAN IPv6 address is formed automatically. This is why subnet IDs for LANs start at "1". The default setting is '1'.
 - **Allow auto configuration (SLAAC):** Specifies whether the prefix is to be used for a stateless address autoconfiguration (SLAAC). The default setting is "enabled".
 - **Receive prefix from:** Defines the name of the interface used to receive a prefix via DHCPv6 prefix delegation or via a tunnel. This prefix can be used to derive and propagate a subnet for each interface.
- **DNS options:** Defines the DNS information in router advertisements according to RFC 6106. The following settings are possible:
 - **Interface name:** Name of the interface on which the IPv6 DNS server announces information in router advertisements.
 - **Primary DNS:** IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC 6106) for this interface.
 - **Secondary DNS:** IPv6 address of the secondary IPv6 DNS server for this interface.
 - **Import DNS search list from the internal DNS server:** Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under **IPv4 > DNS > General settings**. The default setting is "enabled".
 - **Import DNS search list from WAN:** Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under **Receive prefix from**.
- **Route options:** Defines the route option in router advertisements according to RFC 4191 (Route Information Option). The following settings are possible:
 - **Interface name:** Defines the name of the logical interface to be used for sending router advertisements with this route option.
 - **Prefix:** Prefix of the route option, e.g. "2001:db8::/32".
 - **Route preference:** Preferred route. Possible values are "high", "medium" (default) and "low".

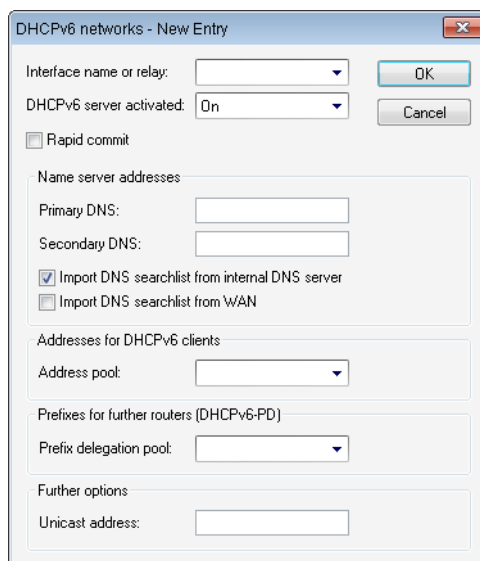
DHCPv6

This is where you configure the DHCPv6 server, the DHCPv6 client and the DHCPv6 relay agent.



DHCPv6 server

Use the following buttons to access the tables and adjust the respective functions:



- **DHCPv6 networks:** This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.

- **Interface name or relay:** Name of the interface on which the DHCPv6 server is working, e.g. "INTRANET". Alternatively, you can also enter the IPv6 address of the remote DHCPv6 relay agent.
- **DHCPv6 server activated:** Activates or deactivates the entry.
- **Rapid commit:** With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

! The client must explicitly include the rapid commit option in its solicit message.

- **Primary DNS:** IPv6 address of the primary DNS server.
- **Secondary DNS:** IPv6 address of the secondary DNS server.
- **Import DNS search list from the internal DNS server:** Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under **IPv4 > DNS > General settings**. The default setting is "enabled".
- **Import DNS search list from WAN:** Specifies whether the DNS search list from the provider (e.g., provider-xy.com) is announced on this logical network. The default setting is "disabled".
- **Address pool:** Name of the address pool used for this interface.

! If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the **Address pools** table.

- **Prefix delegation pool:** Name of prefix pools to be used by the DHCPv6 server.

! If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Prefix delegation pools**.

- **Unicast address:** By default the DHCPv6 server exclusively responds to multicast requests. If the DHCPv6 server should respond to a unicast request, this IPv6 address can be configured here. Generally speaking, multicast is sufficient for communication.

- **Address pools:** If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:

- **Address pool name:** Name of the address pool
- **First address:** First address in the pool, e.g., "2001:db8::1"
- **Last address:** Last address in the pool, e.g., "2001:db8::9"
- **Preferred lifetime:** Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".
- **Valid lifetime:** Here you specify the time in seconds that the client should treat this address as "valid".

! If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

- **Receive prefix from:** With this parameter you can assign addresses to the network clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then enter the value "::1" in the parameter **First address** and "::9" in **Last address**. In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9".

If the provider prefix is greater than "/64", e.g., "/48" or "56", you must take subnetting for the logical network in to account in the address.

Example:

- ▶ Assigned provider prefix: "2001:db8:abcd:aa::/56"
- ▶ "/64" as the prefix of the logical network (subnet ID 1): "2001:db8:abcd:aa01::/64"
- ▶ First address: "0:0:0:0001::1"
- ▶ Last address: "0:0:0:0001::9"

! You should only use this mechanism if the provider assigns a fixed prefix. Otherwise, it is possible that the provider delegates a new prefix to the router, but the client still has an address from the pool with the old prefix. In this case, the client must update its address at the server.

- **Prefix delegation pools:** In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:

- **PD pool name:** Name of the PD pool
- **First prefix:** First prefix to be delegated in the PD pool, e.g., "2001:db8:1100::"
- **Last prefix:** Last prefix to be delegated in the PD pool, e.g., "2001:db8:FF00::"
- **Prefix length:** Length of the prefixes in the PD pool, e.g., "56" or "60"
- **Preferred lifetime:** Here you specify the time in seconds that the client should treat this prefix as "preferred". After this time elapses, a client classifies this address as "deprecated".
- **Valid lifetime:** Here you specify the time in seconds that the client should treat this prefix as "valid".

! If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for preferred lifetime and valid lifetime. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

- **Receive prefix from:** Name of the WAN interface from which the client should use the prefix to form the address or prefix.

- **Reservations:** If you want to assign fixed IPv6 addresses to clients, you can make a reservation for each client in this table:

- **Interface name or relay:** Name of the interfaces on which the DHCPv6 server is working, e.g., "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.
- **Address/PD-Prefix:** IPv6 address, or PD prefix that you want to assign statically.
- **Client ID:** DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `ipconfig /all` or in WEBconfig under **Status > IPv6 > DHCPv6 > Client > Client ID**.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under **Status > IPv6 > DHCPv6 > Server > Address bindings**, and retrieved IPv6 prefixes are under **Status > IPv6 > DHCPv6 > Server > PD bindings**.

LANmonitor displays that client IDs under **DHCPv6 server**.

- **Preferred lifetime:** Here you specify the time in seconds that the client should treat this address as "preferred". After this time elapses, a client classifies this address as "deprecated".
- **Valid lifetime:** Here you specify the time in seconds that the client should treat this address as "valid".



If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

- **Receive prefix from:** Name of the WAN interface from which the client should use the prefix to form the address or prefix.

DHCPv6 client

Use the following buttons to access the tables and adjust the respective functions:

- **Interfaces:** This table determines the behavior of the DHCPv6 client.



Normally client behavior is controlled by the auto-configuration. Only make entries in this table if you want to use the client in "stand-alone" mode or if there are other specific options that deviate from the default settings.

- **Interface name:** Name of the interface on which the DHCPv6 client is working. These can be LAN interfaces or WAN interfaces (remote stations), e.g. "INTRANET" or "INTERNET".
- **Operating:** Determines if and how the device enables the client. Possible values are:
 - ▶ "Autoconfiguration": The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
 - ▶ "Yes": The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements. The device ignores the specifications from router advertisements.
 - ▶ "No": The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.
- **Rapid commit:** When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.
- **Reconfigure accept:** If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The

mechanism is protected by the so-called 'Reconfigure Key', so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation.

The client supports the "Reconfigure Key Authentication Protocol" according to RFC 3315 for the options "Renew" and "Information Request", and also "Rebind" as per RFC 6644.

This option is enabled by default for WAN interfaces.

- **Send own name (FQDN):** The client sends its own host name (Fully Qualified Domain Name). By default, this option is active on LAN interfaces.
- **Request DNS server:** Specifies whether the client queries the DHCPv6 server for DNS servers.

! You must enable this option in order for the device to obtain information about a DNS server.

- **DNS search list:** The client queries the DNS search list.
- **Request address:** Determines whether the client should request an IPv6 address from the DHCPv6 server.

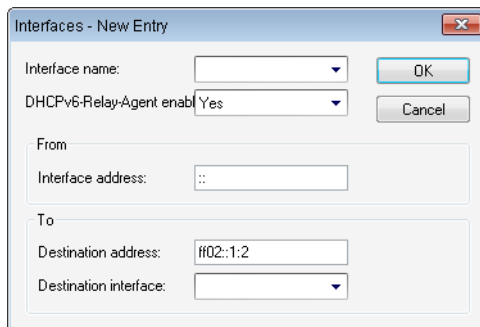
! Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i. e. not distributed by 'SLAAC'.

- **Request prefix:** Determines whether the client should request an IPv6 prefix from the DHCPv6 server. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

DHCPv6 relay agent

Use the following buttons to access the tables and adjust the respective functions:

- **Interfaces:** A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks. This table determines the behavior of the DHCPv6 relay agent.



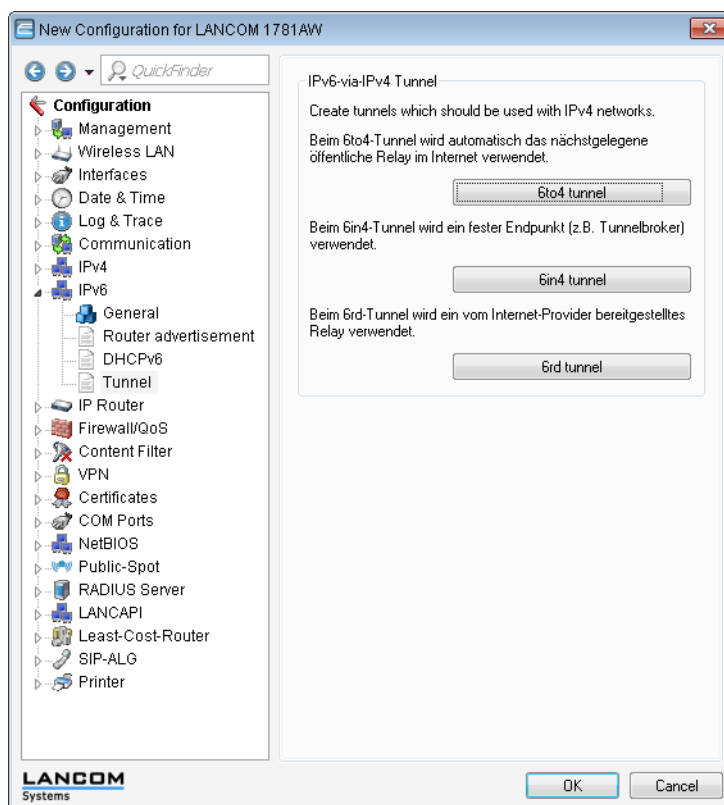
- **Interface name:** Name of the interface on which the relay agent receives requests from DHCPv6 clients, e.g. "INTRANET".
- **DHCPv6-Relay-Agent-enabled:** Determines if and how the device enables the relay agent. Possible values are:
 - ▶ "Yes": Relay agent is enabled. This option is the default setting.
 - ▶ "No": Relay agent is not enabled.
- **Interface address:** The relay agent's own IPv6 address on the interface that is configured under Interface name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.
- **Destination address:** The IPv6 address of the (destination) DHCPv6 server which the relay agent should forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local

multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.

- **Destination interface:** The destination interface where the parent DHCPv6 server or the next relay agent can be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

Tunnel

The **Tunnel** configuration offers you 3 buttons to create IPv6 tunnels that can be used over IPv4 networks. Use these options to gain access to the IPv6 Internet using an IPv4 connection.



- **6to4 tunnel:** This button opens the 6to4 tunnel settings.

⚠ Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

- **6in4 tunnel:** This button opens the 6in4 tunnel settings.

⚠ 6in4 tunnels require more administrative effort, but they represent a secure and stable technology for IPv6 Internet access. This option is also suitable for professional use.

- **6rd tunnel:** This button opens the 6rd tunnel settings.

⚠ 6rd tunneling is suitable for end users and for professional applications because configuration is less complex than with 6in4 tunneling and the technology avoids the security risks of 6to4 tunneling.

5.9.2 Settings in the PPP list

In the PPP list, you are able to specify your own definition of PPP negotiation for every remote site contacting your network. You can also specify whether communications should use an IPv4 or an IPv6 connection.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MSCHAP or MSCHAPv2. The protocols here have a "hierarchy" amongst themselves, i.e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the LANCOM, the connection may fail because no common authentication protocol can be negotiated.

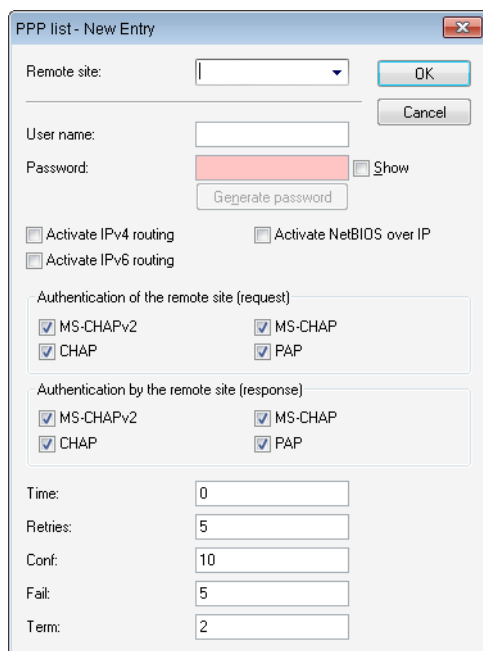
! In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the device must explicitly refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the device ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the device (inbound connections) and on login of the device into other remote sites (outbound connections).

- When establishing inbound connections, the device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the device).
- When establishing outbound connections, the device offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.

LANconfig: **Communication > Protocols > PPP list**

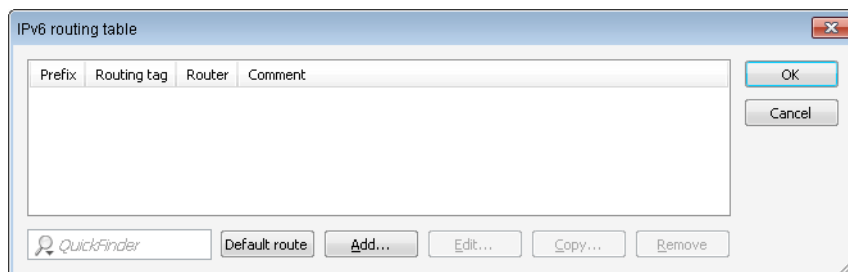
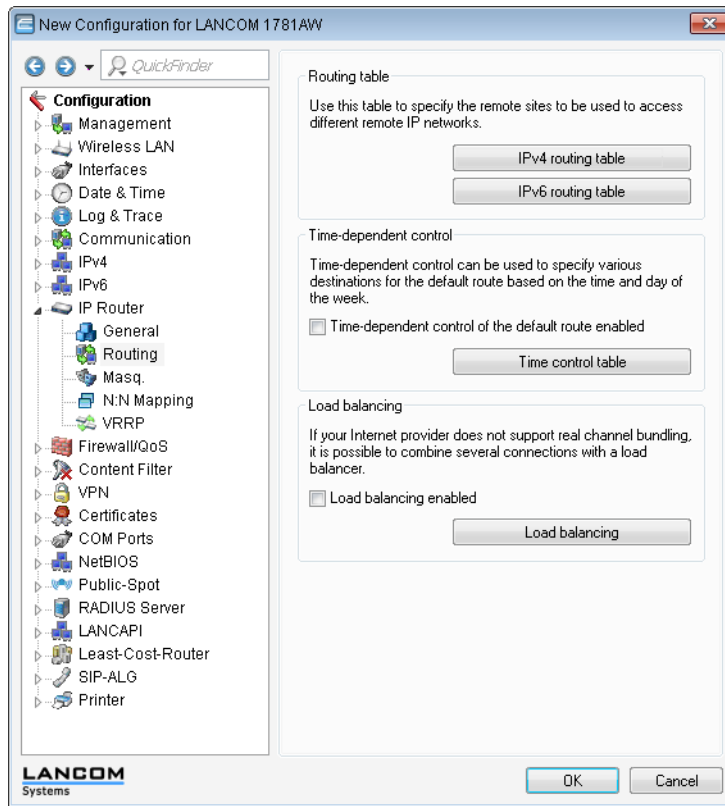


5.9.3 IP routing tables

Unlike previous versions where the configuration menu contained just a single IP routing table, this item now offers the configuration of separate routing tables for IPv4 and IPv6 connections.

You will find the new table under **IP router > Routing > IPv6 routing table**

The IPv4 settings that were previously in the table **IP routing table** are now located in the **IPv4 routing table**.



The table contains the entries to be used for routing packets with IPv6 addresses.

Prefix

Specify the prefix of the network area for which the data is to be routed to the given remote station.

Routing tag


Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.

Router

This is where you specify the remote site for this route.

Comment

Enter a descriptive comment for this entry.

 Entering a comment is optional.

5.9.4 Separate views for the IPv4 and IPv6 firewalls

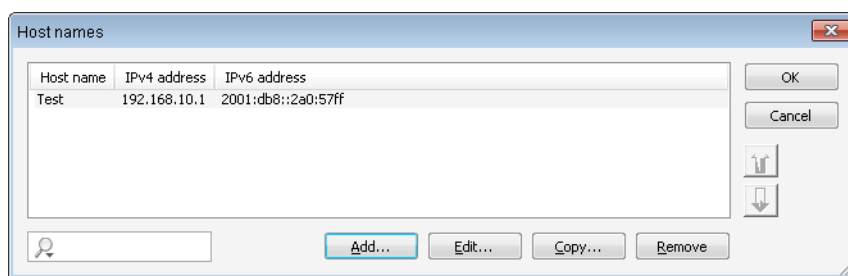
As of LCOS version 8.80, you can configure the rules for the IPv4 and IPv6 firewalls in separate views.

The corresponding configurations are located under **Firewall/QoS > IPv4 rules** and **Firewall/QoS > IPv6 rules** respectively.

5.9.5 IPv6 DNS hosts in the DNS list

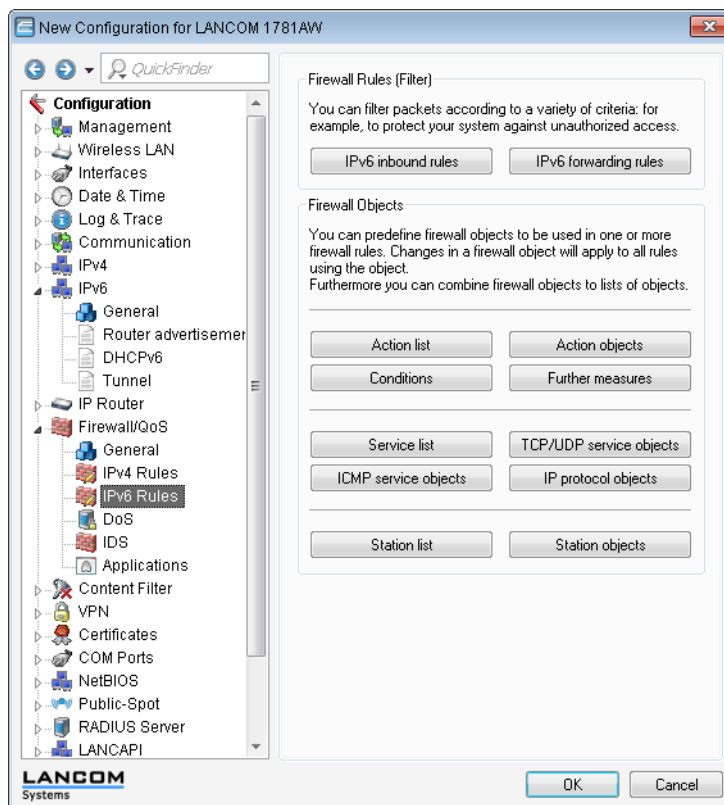
When the DNS server in your device receives a query about a station name, it responds with the IP address contained in the Host names list. For each station/host name you define either the IPv4 or the IPv6 address, or alternatively you can enter both IP addresses.

In LANconfig, the table with the station names and the associated IP addresses is under **IPv4 > DNS > Host names**.




5.9.6 Configuring the IPv6 firewall rules

With LANconfig you can set the firewall rules under **Firewall/QoS > IPv6 Rules**.



The factory settings provide various objects and lists for the most important applications.

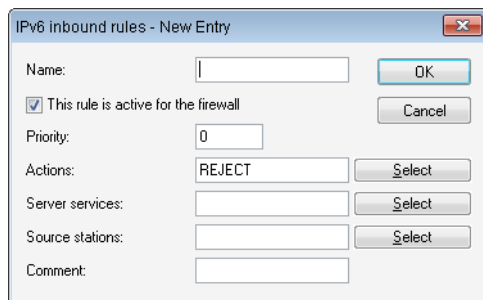
 You cannot delete objects or lists if the firewall uses them in a forwarding or inbound rule.

IPv6 inbound rules

Using the **IPv6 inbound rules** you set the rules that the IPv6 firewall should use to handle incoming traffic.

The factory settings provide various rules for the most important applications.

Click on **Add...** to create a new rule.



You can set the following properties for the rule:

Name

Specifies the name of the rule.

This rule is active for the firewall

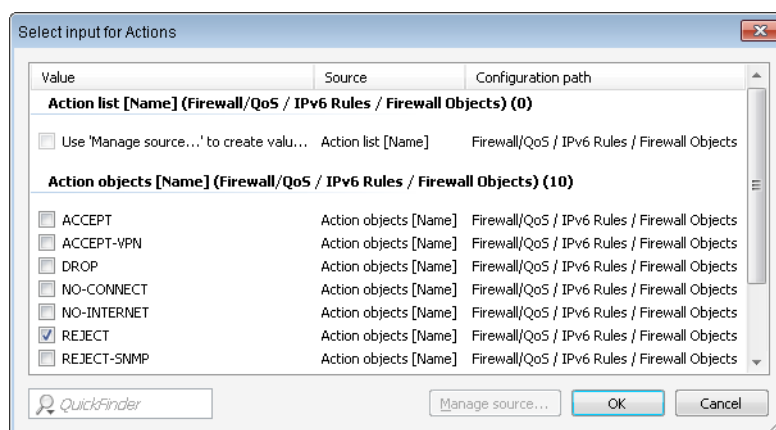
Enables the rule.

Priority

Specifies the priority of the rule: The higher the value, the higher the priority.

Actions

Specifies the action that the firewall performs if the rule condition is true. Using **Select** you can choose one action or a list of actions.



If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source**. Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Server services

Determines the services which the firewall applies this rule to. Using **Select** you can choose one service or a list of services.

Source stations

Determines the source stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

Comment

Here you assign a meaningful description for the filter rule.

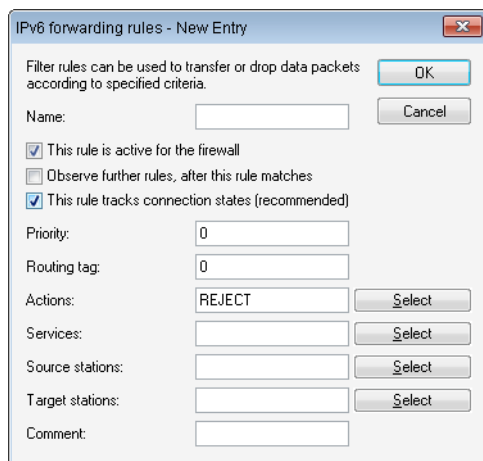
IPv6 forwarding rules

The **IPv6 forwarding rules** button accesses dialog where you set the rules that the IPv6 firewall should use to handle forwarded traffic.

The factory settings provide various rules for the most important applications.

In order to change the order of the rules, highlight the specific rule in the table and move it up or down in the table by clicking on the arrow buttons. The firewall applies the rules one after the other from top to bottom.

Click on **Add...** to create a new rule.



You can set the following properties for the rule:

Name

Specifies the name of the rule.

This rule is active for the firewall

Enables the rule.

Observe further rules after this one matches

If you enable this option, the firewall also applies the subsequent rules in the list. This is useful if the firewall should, for example, initially apply a group rule and then apply each rule to the individual objects in the group.

This rule tracks connection states (recommended)

Select this option if the rule should track the TCP connection states.

Priority

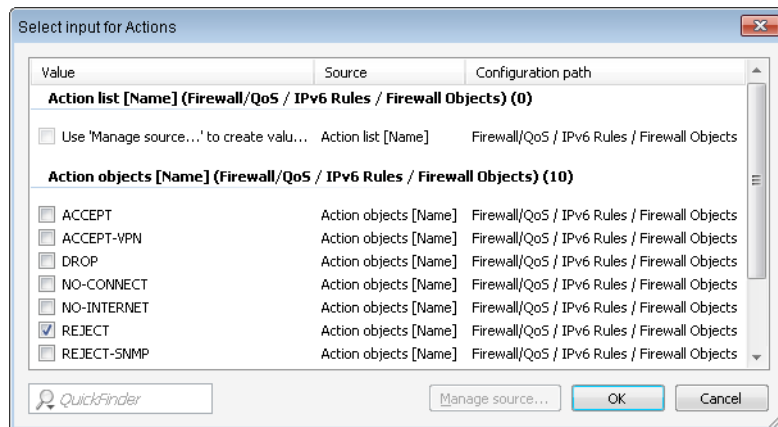
Specifies the priority of the rule: The higher the value, the higher the priority.

Routing tag

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

Actions

Specifies the action that the firewall performs if the rule condition is true. Using **Select** you can choose one action or a list of actions.



If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source**. Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Server services

Determines the services which the firewall applies this rule to. Using **Select** you can choose one service or a list of services.

Source stations

Determines the source stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

Target stations

Determines the target stations which the firewall applies this rule to. Using **Select** you can choose one station or a list of stations.

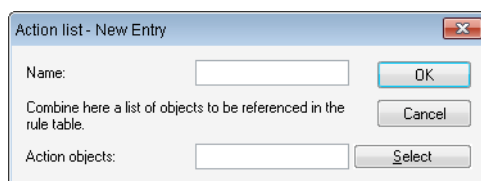
Comment

Here you assign a meaningful description for the filter rule.

Action list

Using the **Action list** button, you can collect actions into groups. The actions available here must first be defined using **Action objects**.

Click on **Add...** to create a new rule.



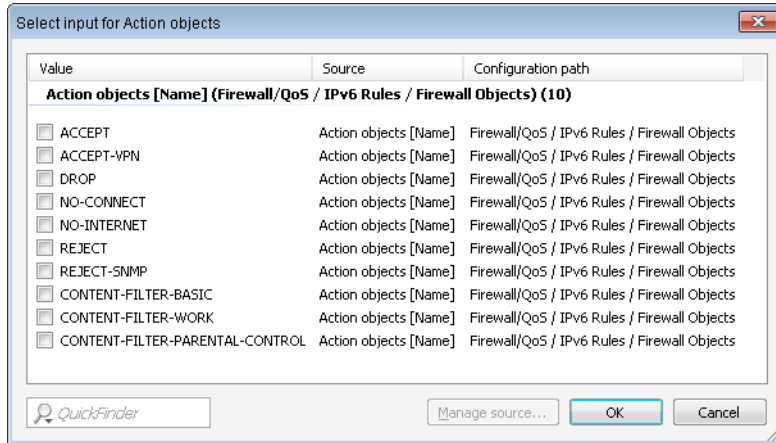
You can set the following properties for a list:

Name

Determines the name of the list.

Action objects

Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

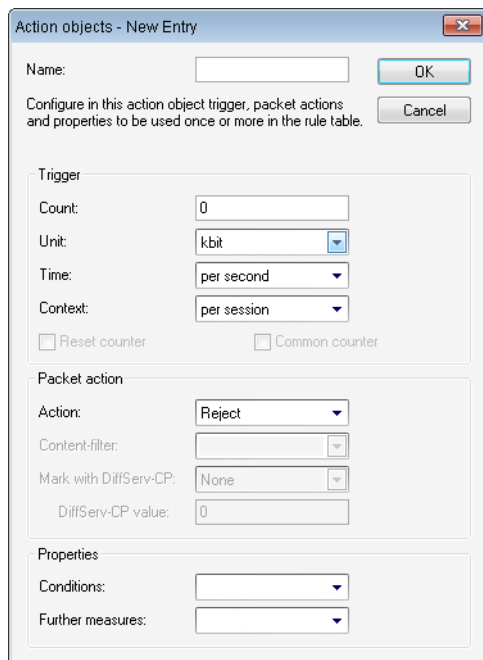


If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source**. Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Action objects

Using the **Action objects** button, you define actions that the IPv6 firewall runs when a filter is true.

Click on **Add...** to create a new action.



You can set the following properties for the object:

Name

Specifies the name of the object.

Count

When this limit is exceeded, the firewall performs the action.

Unit

Determines the unit for the limits. Select the corresponding value in the drop-down menu.

Time

Determines the measurement period that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

Context

Determines the context that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

Reset counter

If you enable this option, the firewall resets the counter after running the action.



You can only activate this option if you selected "absolute" in the **time** value.

Common counter

If you enable this option, the firewall adds all action triggers together in one counter.



You can only activate this option if you selected "per station" or "global" in the **Context** value.

Action

Determines the action the firewall performs when the limit is reached.

The following options are possible:

- **Reject:** The firewall rejects the data packet and sends an appropriate notification to the sender.
- **Drop:** The firewall discards the data packet without notification.
- **Transmit:** The Firewall accepts the data packet.

Mark with DiffServ-CP

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.



You can only activate this option if you selected "transmit" in the **Action** value.



Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

DiffServ-CP value

Determines the value for the Differentiated Services Code Point (DSCP).



You can only activate this option if you selected "Value" in **Mark with DiffServ-CP**.

Conditions

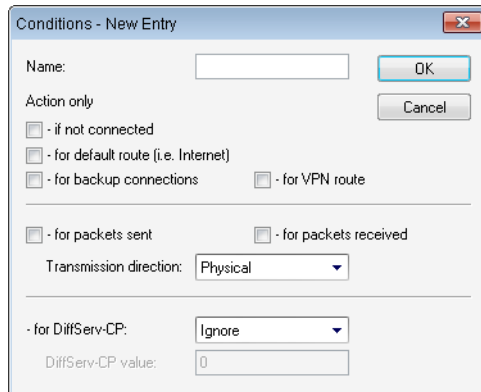
Determines which conditions must be met in order for the action to be performed. The item **Conditions** is used to specify any conditions.

Further measures

Determines which trigger actions the firewall should start in addition to filtering the data packets. You can specify trigger actions under the **Further measures**.

Conditions

Use the **Conditions** button to specify the conditions that have to be met for the forwarding and inbound rules to apply. Click on **Add...** to create a new condition.



You can set the following properties for the condition:

Name

Specifies the name of the object.

Action only – if not connected

Select this option if the firewall should only perform the action if there is no connection.

Action only – for default route (e.g. Internet)

Select this option if the firewall should only perform the action if there is a connection over the default route.

Action only – for backup connections

Select this option if the firewall should only perform the action if the connection is a backup connection.

Action only – for VPN route

Select this option if the firewall should only perform the action if the connection is a VPN connection.

Action only – for packets sent

Select this option if the firewall should only perform the action for packets sent.

Action only – for packets received


Select this option if the firewall should only perform the action for packets received.

Transmission direction

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

Action only – for DiffServ-CP


Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

DiffServ-CP value

Determines the value for the Differentiated Services Code Point (DSCP).

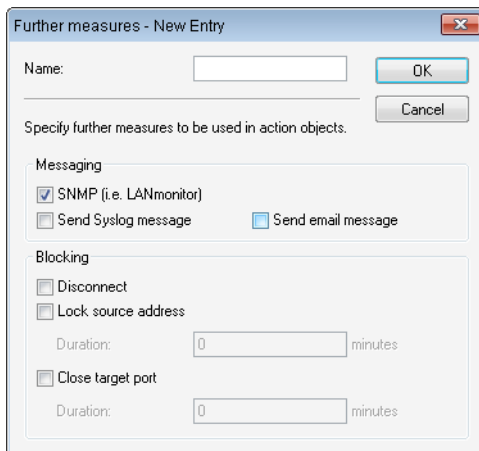
Enter a value here if you selected the "Value" option in the – **for DiffServ-CP** field.

 Further information about DiffServ CodePoints is available in the Reference Manual under the section "QoS".

Further measures

Use the **Further measures** button to define further measures that the firewall performs after you apply the forwarding and inbound rules.

Click on **Add...** to create a new measure.



You can set the following properties for the trigger actions:

Name


Specifies the name of the object.

SNMP (e.g. LANmonitor)

Select this option if the firewall should send a notification via SNMP. You can receive this notification, e.g., with LANmonitor.


Send Syslog message

Select this option if the firewall should send a SYSLOG notification via SNMP.

 For more information about SYSLOG, refer to the chapter "Diagnostics" in the section "SYSLOG" in the Reference Guide.

Send e-mail message

Select this option, if the firewall should send a notification by e-mail.

 If you want to receive e-mail notifications, you must enter an e-mail address in **Firewall/QoS > General > Administrator e-mail**.

Disconnect

Select this option if the firewall should disconnect.

Lock source address

Select this option if the firewall should block the source address. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the **Host-lock-list** under **Status > IPv6 > Firewall**.

Duration

If the firewall should block the sender, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

Close destination port

Select this option, if the firewall should block the target port. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the **Port-block-list** under **Status > IPv6 > Firewall**.

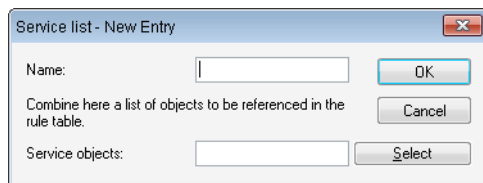
Duration

If the firewall should block the target port, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

Service list

Using the **Service list** button, you can collect services into groups. You first define the services under **TCP/UDP service objects**, **ICMP service objects** and **IP protocol objects**.

Click on **Add...** to specify a new service.



You can set the following properties for a list:

Name

Determines the name of the list.

Service objects

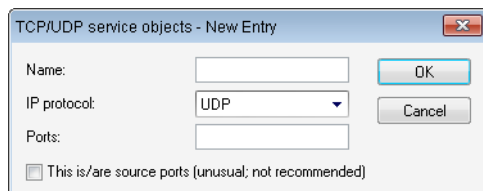
Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source**. Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

TCP/UDP service objects

Using the **TCP/UDP service objects** button, you define TCP/UDP services that the IPv6 firewall can use in filter rules.

Click on **Add...** to create a new service.



You can set the following properties for the rule:

Name

Specifies the name of the object.

IP protocol

Specifies the protocol of the service

Ports

Specifies the ports for the service. Separate multiple ports with a comma.

! Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

This is/are source ports

Determines whether the specified ports are source ports.

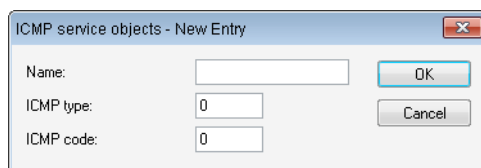
! In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

ICMP service objects

Using the **ICMP service objects** button, you define ICMP services that the IPv6 firewall can use in filter rules.

! Lists with the official ICMP types and port codes are available in the Internet under www.iana.org.

Click on **Add...** to create a new service.



You can set the following properties for the rule:

Name

Specifies the name of the object.

ICMP type

Specifies the type of the ICMP service.

ICMP code

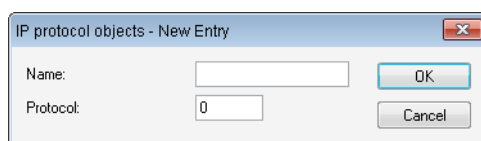
Specifies the code of the ICMP service.

IP protocol objects

Using the **IP protocol objects** button, you define IP protocol objects that the IPv6 firewall can use in filter rules.

! Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

Click on **Add...** to create a new object.



You can set the following properties for the rule:

Name

Specifies the name of the object.

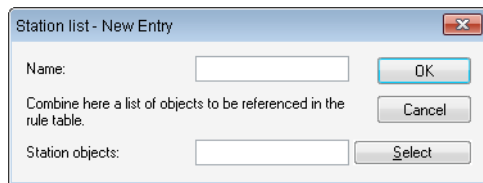
Protocol

Defines the protocol number.

Station list

Using the **Station list** button, you can collect stations into groups. Stations must previously be defined using **Station objects**.

Click on **Add...** to create a new list.



You can set the following properties for a list:

Name

Determines the name of the list.

Station objects

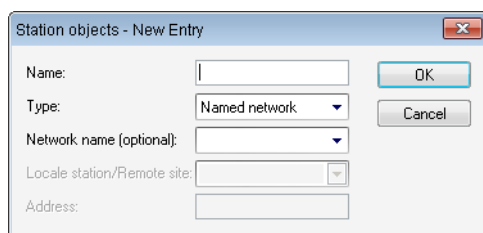
Determines the objects that you want to combine in this list. Using **Select** you can choose one or more objects from a list.

If you make a new entry here, it initially appears under **Unknown source**. Next, highlight the entry for a source that you want to assign to the new entry, and click on **Manage source**. Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Station objects

Using the **Station objects** button, you define stations that the IPv6 firewall can use in filter rules.

Click on **Add...** to create a new object.



You can set the following properties for the object:

Name

Specifies the name of the object.

Type

Determines the station type.

Network name

Here you enter the name of the network if you selected the appropriate option in the **Type** field.



Entering the network name is optional.

Remote site

Here you enter the name of the remote site if you selected the appropriate option in the **Type** field.

Address

Here you enter the address of the remote site if you selected the appropriate option in the **Type** field.

5.10 Tutorials

5.10.1 Setting up IPv6 Internet access

You can set up access to an IPv6 network if

- You have an IPv6-capable device,
- You use a tunneling technology and
- Your provider supports a native IPv6 network or you have access to a so-called tunnel broker who can mediate your IPv6 packets.

IPv6 access using the Setup Wizard in LANconfig

The Setup Wizard assists you with the configuration of IPv6 access with your equipment.

The Wizard presents following options:

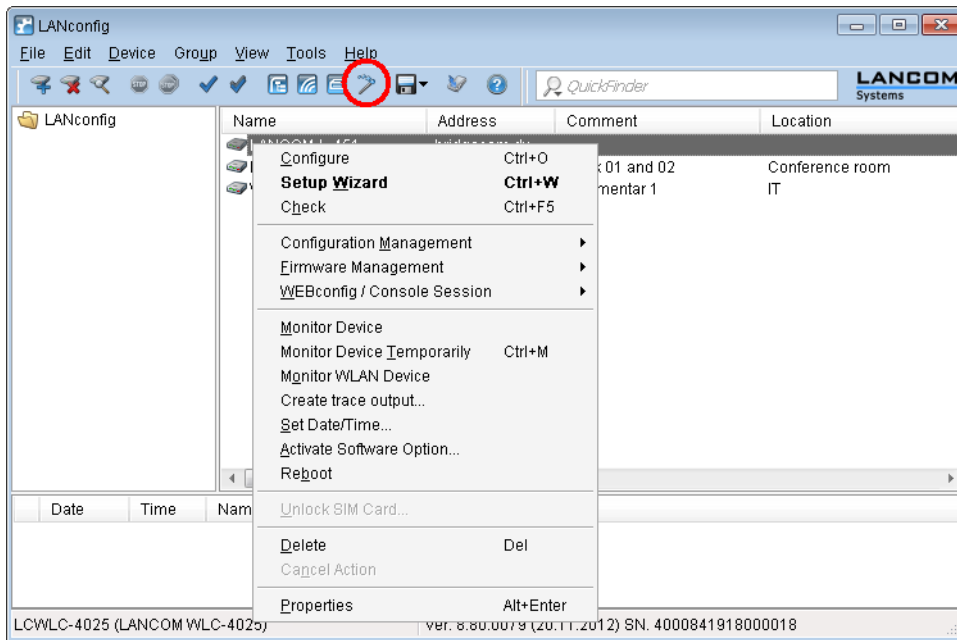
- [Set up IPv6 access for a new, unconfigured device.](#)
- [Set up IPv6 access in addition to a functioning IPv4 access for an existing device.](#)

Setup Wizard – setting up IPv6 in a new device

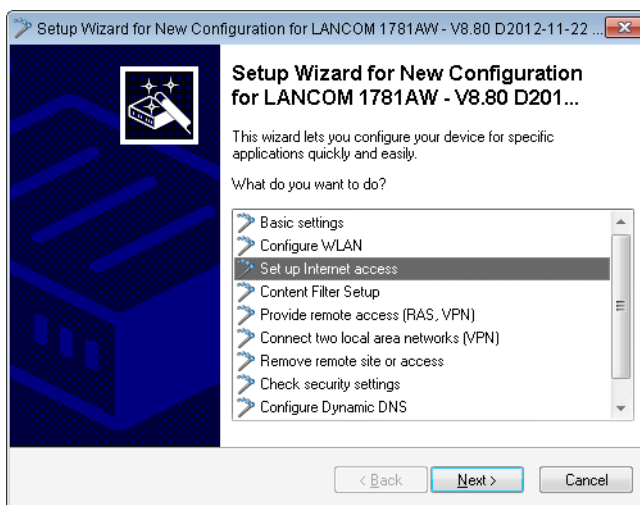
If you have connected up a new device but not have yet configured it, you have the option of using a Setup Wizard to set up IPv4 and IPv6 connections.

To save your entries and proceed to the next screen, click **Next**.

1. Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar

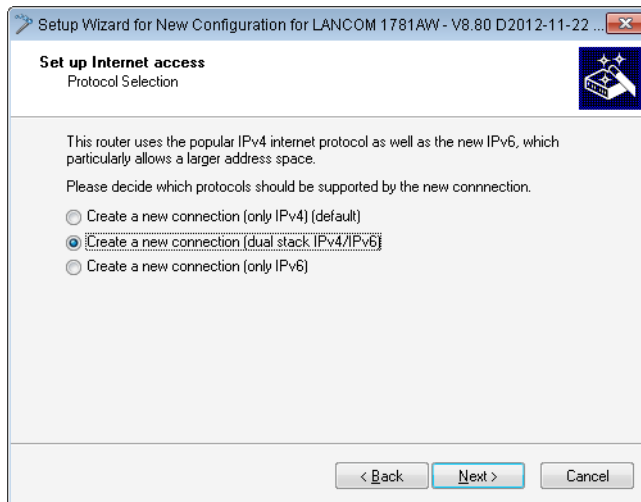


2. In the Setup Wizard, select the option **Set up Internet access**.

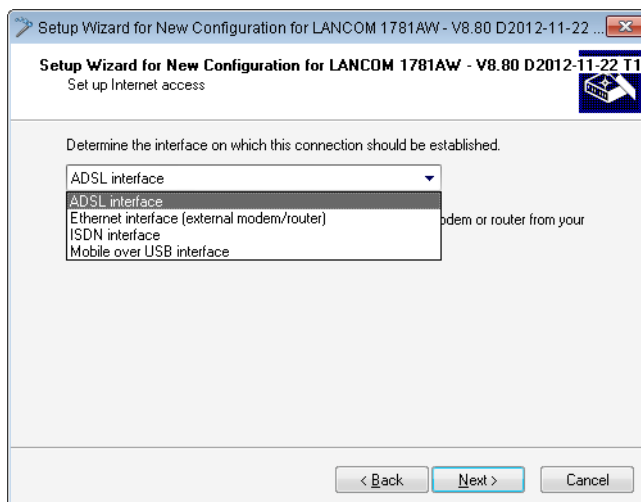


3. You can choose from the following options:
 - Set up a dual-stack connection. This is IPv4-and IPv6-capable and currently the recommended option for a new device.
 - Set up an IPv4-only connection.
 - Set up an IPv6-only connection.

In the following we take you through the setup of a dual-stack connection. Activate the appropriate selection.



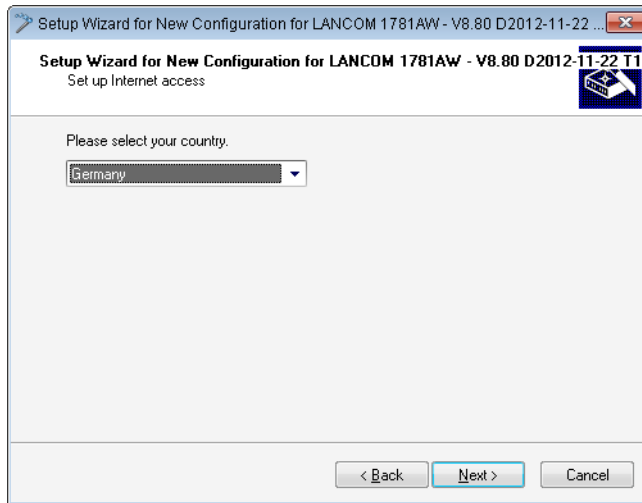
4. Set the interface to be used for the connection.



You can select from the following entries:

- ADSL interface
- Ethernet interface (external modem/router)
- ISDN interface
- Mobile over USB interface

5. Select your country from the list.

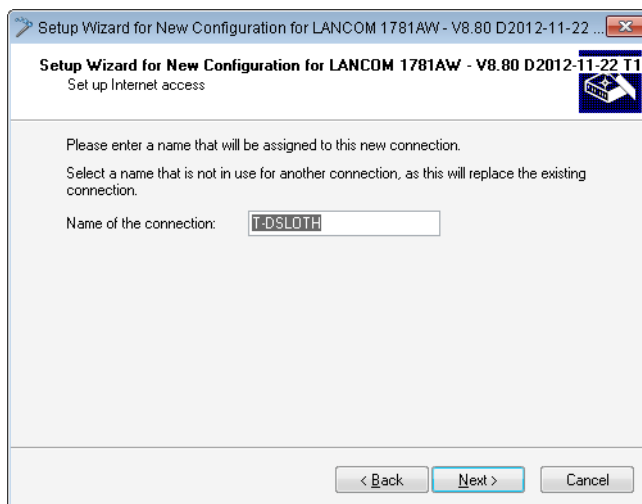


6. Select your Internet provider.

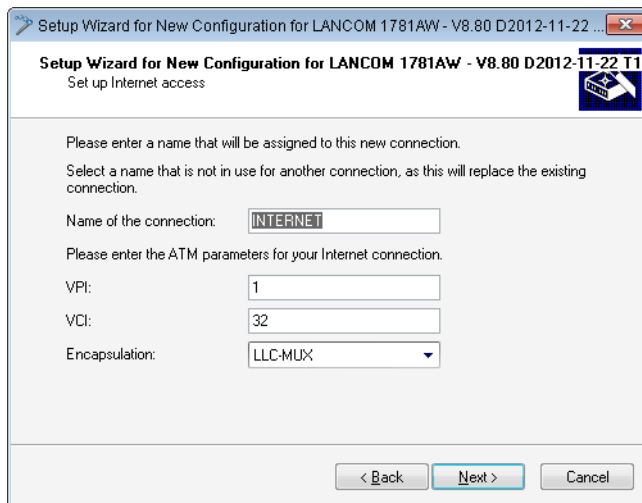
You can select from the following entries:

- A selection of the major Internet providers
- Alternative Internet providers over T-DSL
- Internet access via PPP over ATM (PPPoA)
- Internet access via PPP over Ethernet (PPPoE, PPPoEoA)
- Internet access via plain IP (IPoA)
- Internet access over Plain Ethernet (IPoE, IPoEoA)

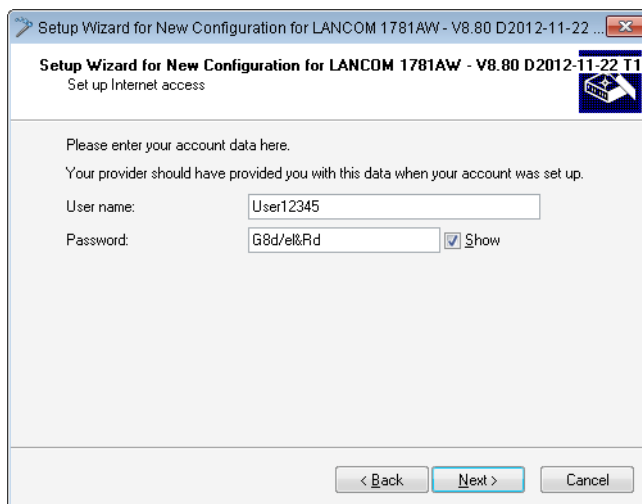
7. Enter a name for this connection.



If you access the Internet with an alternative connection, e. g. over a PPPoE connection, you should additionally enter the appropriate ATM parameters.

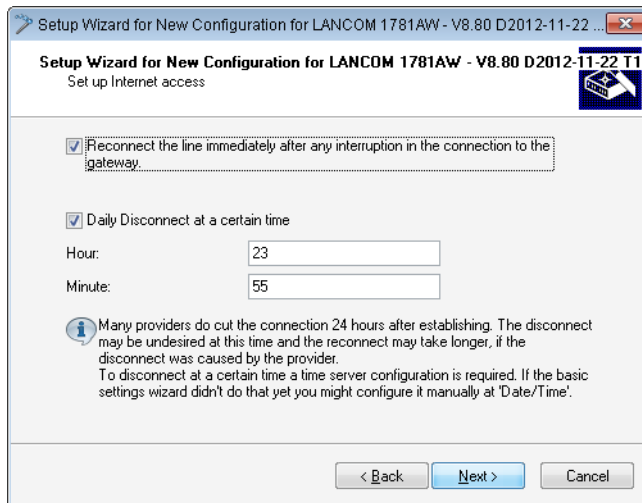


8. Enter the login details given to you by your provider for setting up your Internet access.

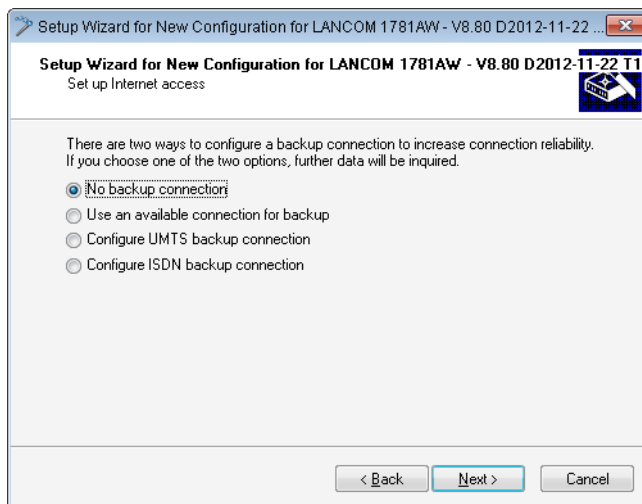


! Depending on the provider, the type and number of fields may vary.

9. Specify how you want the device to behave in case of disconnection. You can also specify if and when the device is to carry out a forced re-connection.



10. Define the type of backup connection to be used in case of connection failure.



You can select from the following options:

- No backup connection: Skips the configuration of a backup.
- Use the connection already configured in case of backup: In the following dialog, select an already configured connection from a list.
- Setup a backup connection over UMTS: In the next dialog, set up a new UMTS connection. You will need the access data for your UMTS provider.
- Setup a backup connection over ISDN: In the next dialog, set up a new ISDN connection. You will need the access data for your ISDN provider.

11. If your device does not yet have an IP address, enter a new IP address and corresponding netmask.

Setup Wizard for New Configuration for LANCOM 1781AW - V8.80 D2012-11-22 ...

Setup Wizard for New Configuration for LANCOM 1781AW - V8.80 D2012-11-22 T14
Set up Internet access

You have not yet assigned an IP address to your device.
Please enter an available IP address from your local network, along with the corresponding netmask.

IP address:

Netmask:

< Back Next > Cancel

12. Select the type of IPv6 Internet access.

Setup Wizard for New Configuration for LANCOM 1781AW - V8.80 D2012-11-22 ...

Set up Internet access
IPv6 Tunnel Selection

You can use your internet connection with the new internet protocol IPv6 (bigger address space) besides IPv4.

Please select the IPv6 internet access mode:

Additional native IPv6 - direct connection without tunnel

6to4 tunnel - Endpoint is detected automatically (no more settings needed).

6in4 tunnel - Endpoint is supplied by tunnel broker, e.g.

6rd tunnel - Endpoint is supplied by provider.

Please mind that native IPv6 has to be supported by provider.
A 6to4 tunnel is possible without provider support.

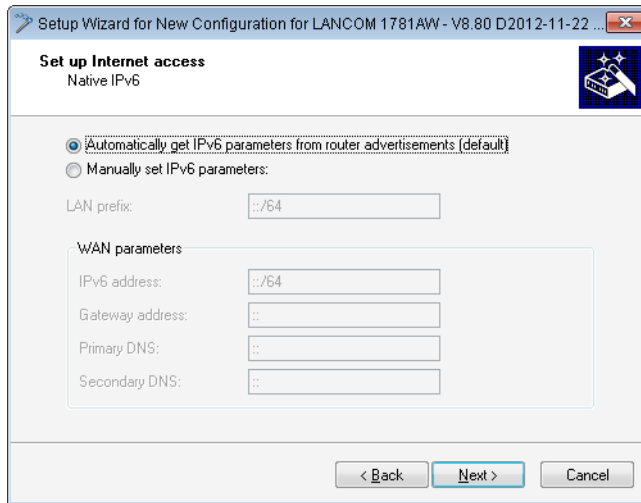
< Back Next > Cancel

You can select from the following options:

- **Additional native IPv6:** Configure a direct connection without a tunnel.
- **6to4 tunnel:** Start the wizard to configure a 6to4 tunnel.
- **6in4 tunnel:** Use the input mask to set the parameters for the 6in4 tunnel.
- **6rd tunnel:** Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

13. Accept the default setting of **Automatically take IPv6 parameters from router advertisements.**



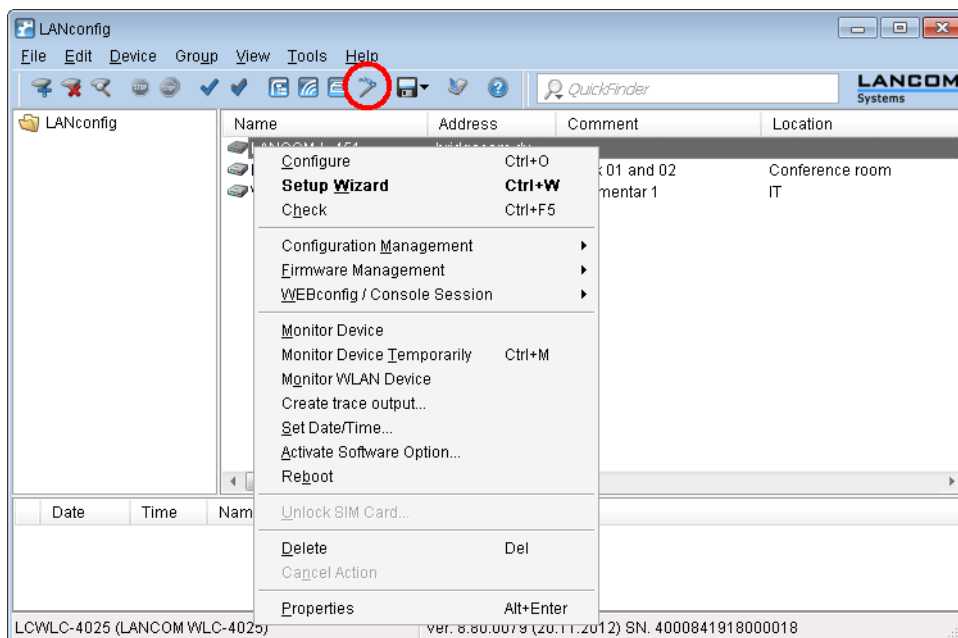
14. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.

Setup Wizard – Setting up IPv6 on an existing device

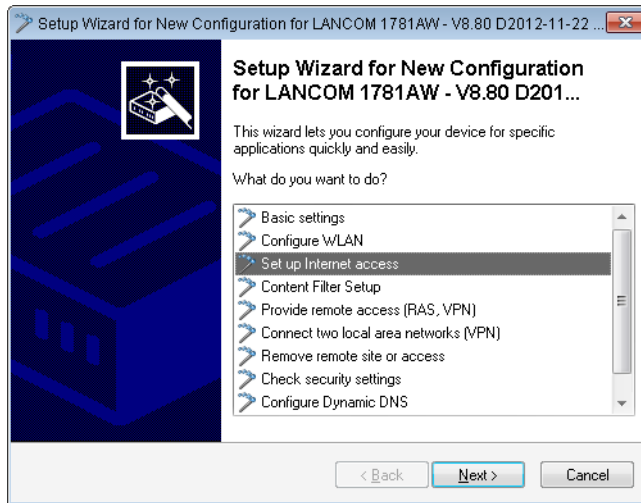
If you have a device configured for IPv4 and you wish to set up an additional IPv6 connection, you have the option of setting up the IPv6 connections with the Setup Wizard.

To save your entries and proceed to the next screen, click **Next**.

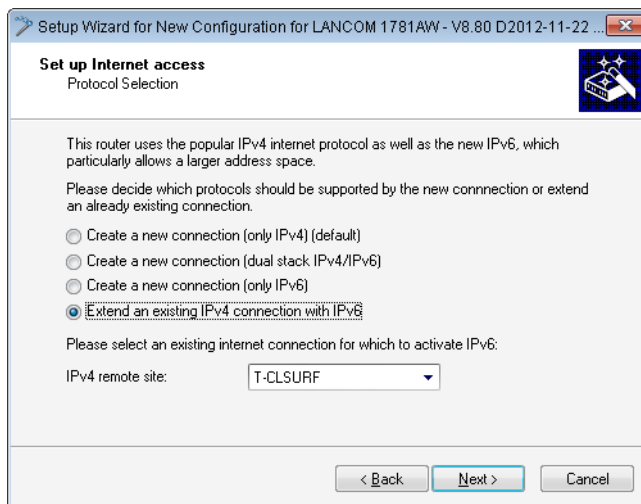
1. Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



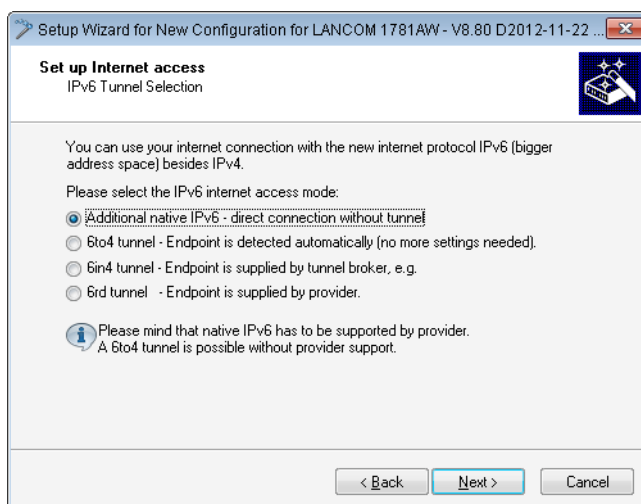
- In the Setup Wizard, select the option **Set up Internet access**. To continue, click on **Next**.



- Because your device is already IPv4-capable, the Setup Wizard gives you the opportunity to extend your existing settings with IPv6. Select this option and click on **Next**.



- Select the type of IPv6 Internet access.

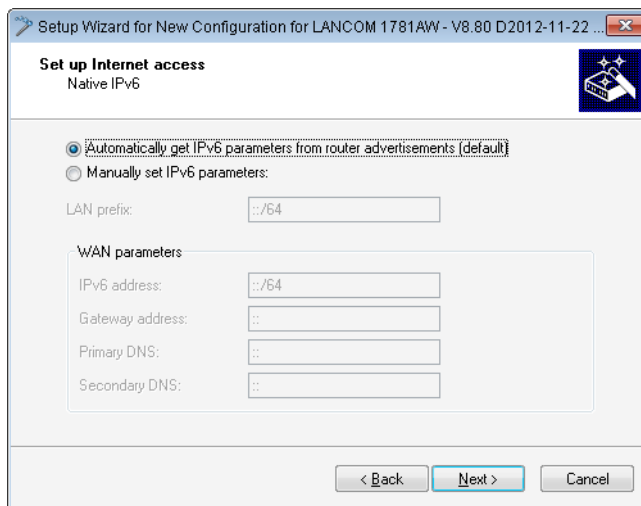


You can select from the following options:

- **Additional native IPv6:** Configure a direct connection without a tunnel.
- **6to4 tunnel:** Start the wizard to configure a 6to4 tunnel.
- **6in4 tunnel:** Use the input mask to set the parameters for the 6in4 tunnel.
- **6rd tunnel:** Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

5. Accept the default setting of **Automatically take IPv6 parameters from router advertisements.**



6. You have completed the setup of the native IPv6 Internet access. Click on **Finish** when you are done and the wizard will save your entries to the device.


5.10.2 Setting up a 6to4 tunnel

The use of a 6to4 tunnel is feasible when

- Your device is IPv6 capable and you want to access IPv6 services,
- Your provider does not support a native IPv6 network and
- You do not have access to a so-called tunnel broker who can mediate your IPv6 packets.

When using a 6to4 tunnel, the lack of support of IPv6 by the provider means the device does not receive an IPv6 address or an IPv6 prefix.

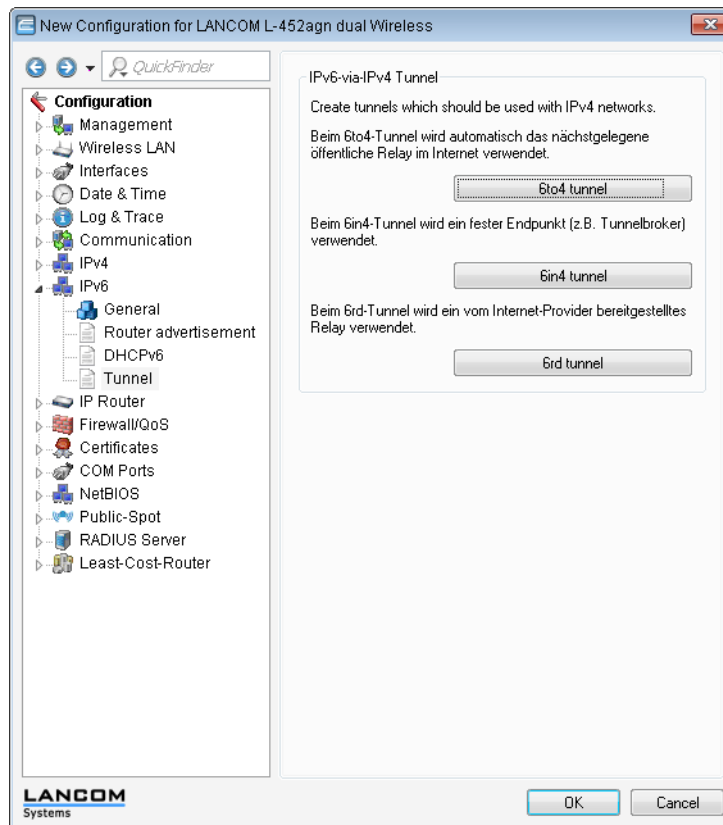
The device calculates its own unique prefix from "2002::/16" and the hexadecimal representation of its own public IPv4 address from the provider. This application only works if the device has a public IPv4 address. The device does not receive a public IPv4 address but an IPv4 address from a private address range only, for example when it accesses the Internet via UMTS and the provider supplies an IP address from its private address range, or if the device does not access the Internet directly, but is "behind" another router.

 Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the relay used can change without the administrator knowing about it. For this reason, connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

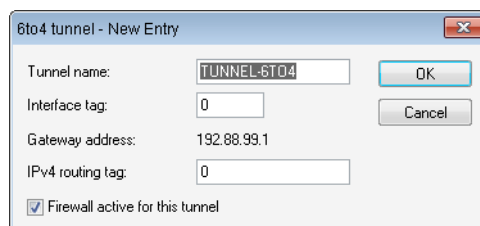
Working with LANconfig

To set up a 6to4 tunnel with LANconfig, proceed as follows:

1. LANconfig can be started from the Windows Start bar: Click on **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices.
2. Select the device on which you want to set up a 6to4 tunnel. Select it with a left-click and start the configuration from the menu bar with **Device > Configure**.
3. Navigate to **IPv6 > Tunnel** and click on **6to4 tunnel**.

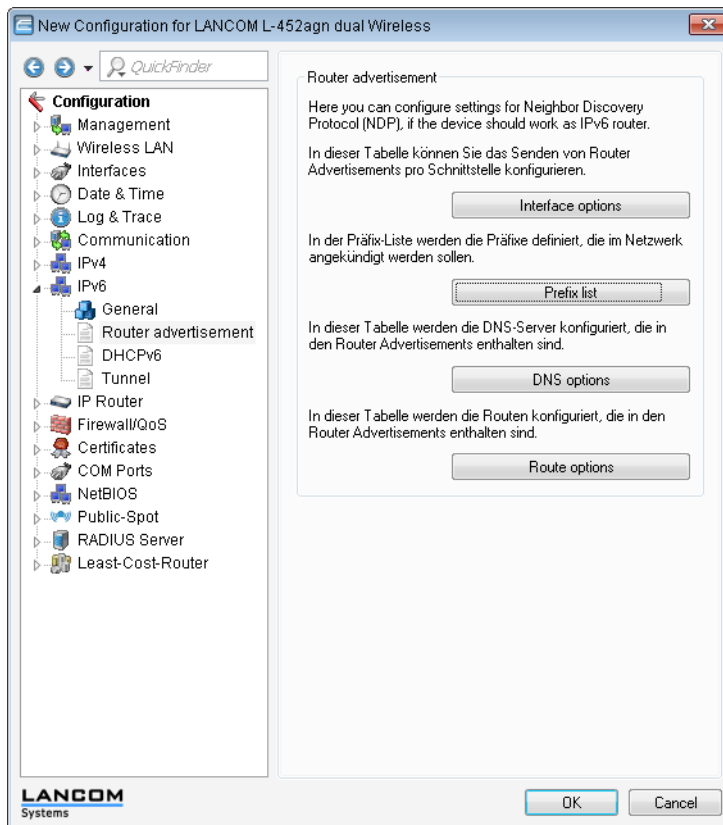


4. Click on **Add** to create a new 6to4 tunnel.

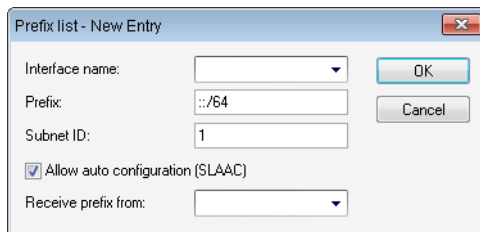


5. Set the name of the 6to4 tunnel.
6. Set the **Interface tag** to a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
7. The **Gateway address** is set by default to the anycast address "192.88.99.1". This address can only be changed with WEBconfig or Telnet.
8. Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The **IPv4 routing tag** specifies which tagged IPv4 route is to be used for the data packets to reach their destination address.
9. The default value is this tunnel's firewall.
If you disable the global firewall, you should also disable the firewall for the tunnel.
10. Accept your entries with **OK**.

11. Change to the directory **IPv6 > Router advertisements**.

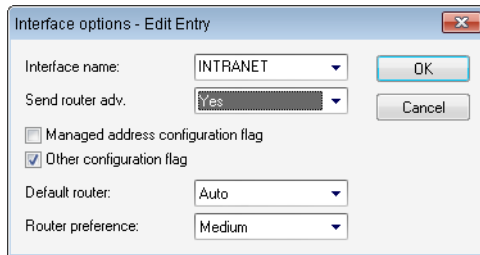


12. Open the **Prefix list** and click on **Add**.



13. Enter a name for the interface that is used by the 6to4 tunnel, e. g. "INTRANET".
14. Set the value for the **Prefix** to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
15. Accept the default value of "1" for the **Subnet ID**.
16. Accept the activated option **Stateless address configuration**.
17. In the field **Prefix delegation from**, enter the name of the tunnel that you have defined earlier, e.g. in the example above "TUNNEL-6TO4".
18. Accept your entries with **OK**.
19. In the directory **IPv6 > Router advertisements**, open the **Interface options**, select the entry INTRANET and click on **Edit**.

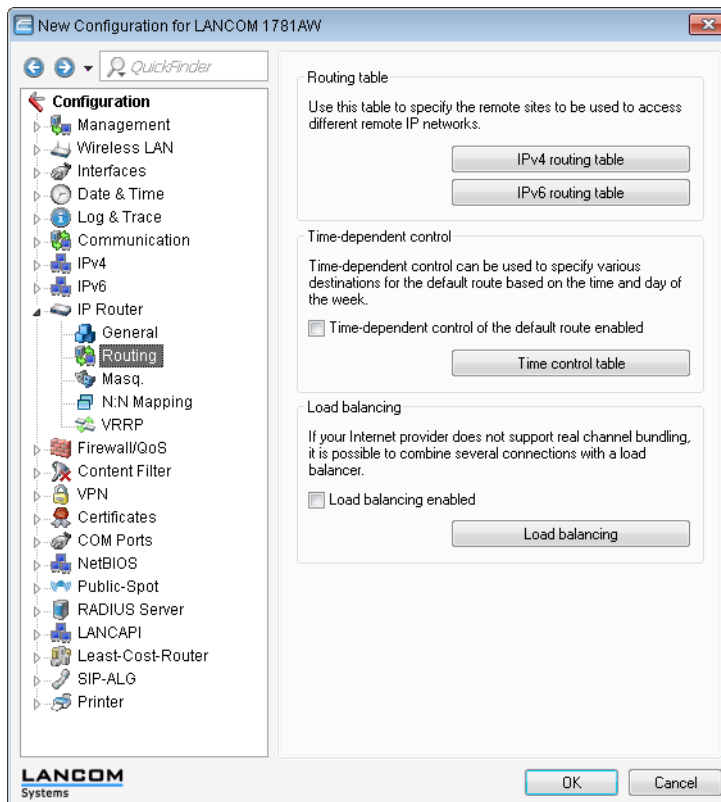
20. In the drop-down menu **Send router advertisements** select the option 'Yes'.



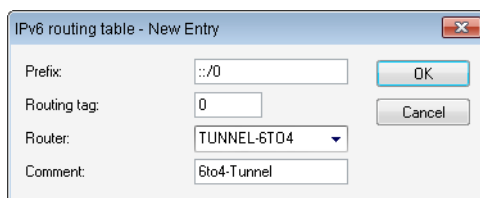
21. Accept all other default values without change.

22. Save your entries with **OK**.

23. Change to the directory **IP router > Routing**.



24. Open the **IPv6 routing table** and click on **Add**.



25. Set the **Prefix** to the value ":::0".

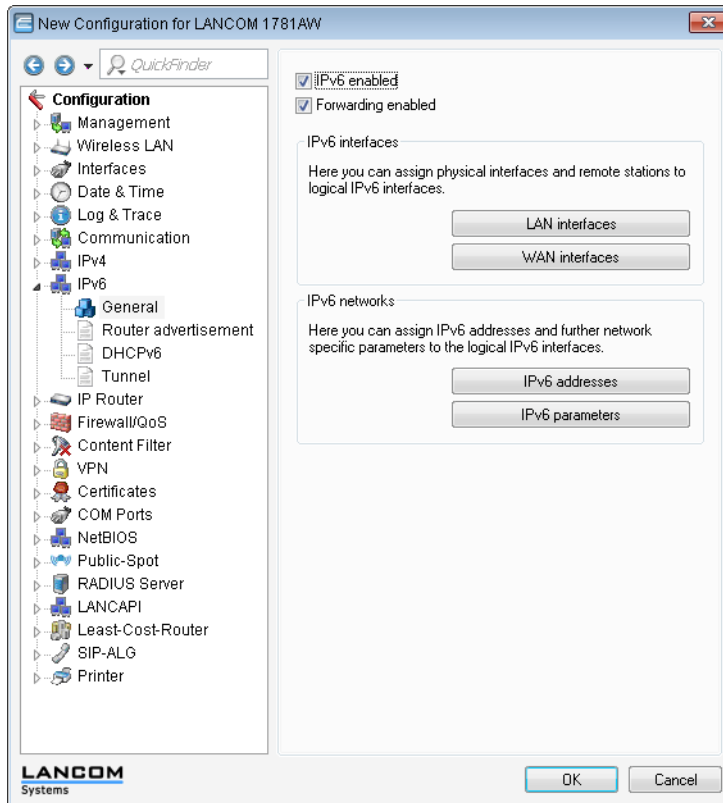
26. In the field **Routing tag** accept the default value "0".

27. In the field **Router**, select from the list the name of the tunnel that you defined earlier, e.g. in the example above "TUNNEL-6TO4".

28. Enter a descriptive **Comment** for this entry.

29. Save your entries with **OK**.

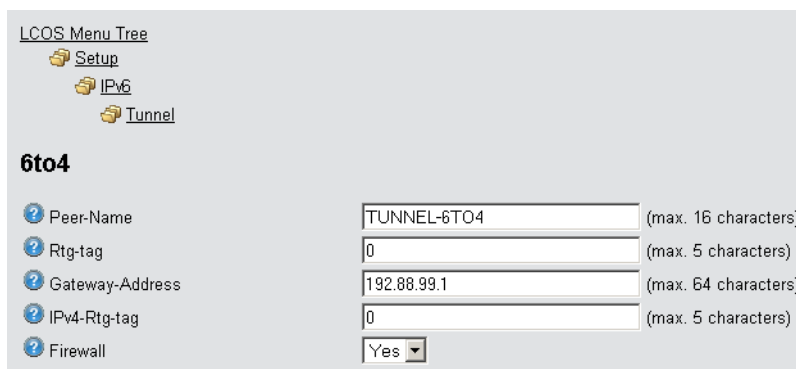
30. Change to the directory **IPv6 > General** and enable the IPv6 stack.



Working with WEBconfig

To set up a 6to4 tunnel with WEBconfig, proceed as follows:

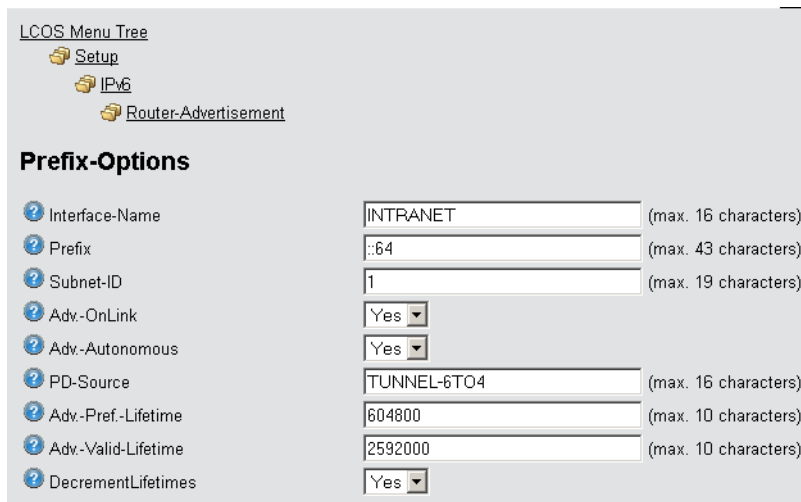
1. Type into your browser's address bar the address of the device to be set up with a 6to4 tunnel.
2. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Tunnel > 6to4** and click on **Add**.



3. Enter a name for the remote peer, e. g. "TUNNEL-6TO4".
4. Leave the **Routing tag** unchanged as the default value "0".
5. As the **Gateway address** you can accept the default value "192.88.99.1". This is the default anycast address for 6to4 relays that your device connects to.

This address is the reason why 6to4 tunnels are unstable and insecure. There is no assurance that a 6to4 relay will be available, and publicly available 6to4 relays may not be trustworthy. There is no guarantee that the relay does not record your traffic.

6. In the field **IPv4-Rtg-tag** accept the default value "0"
7. Enable the **firewall** for this tunnel.
If you disable the global firewall, you should also disable the firewall for the tunnel.
8. Save your entries with **Send**.
9. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Router-Advertisement**, open the **Prefix options** table and click on **Add**.



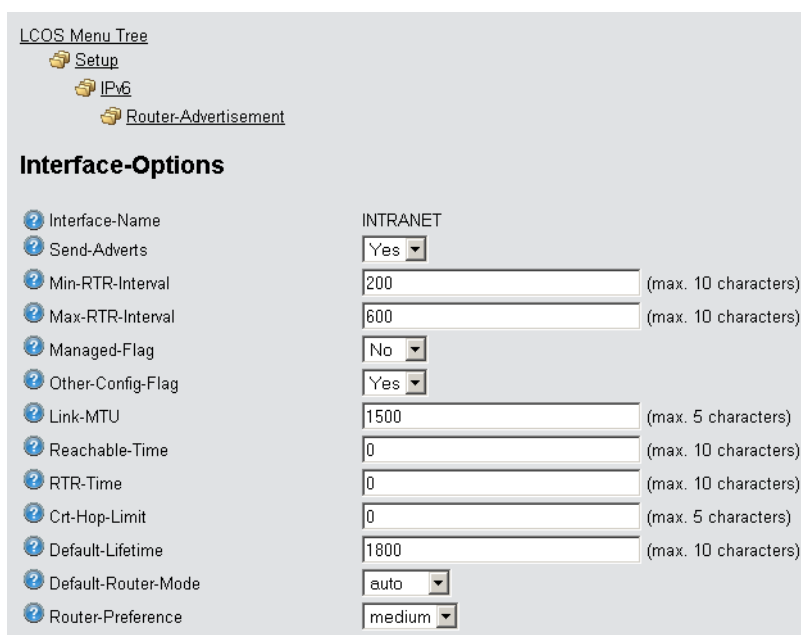
LCOS Menu Tree

- Setup
- IPv6
- Router-Advertisement

Prefix-Options

Interface-Name	INTRANET	(max. 16 characters)
Prefix	::64	(max. 43 characters)
Subnet-ID	1	(max. 19 characters)
Adv.-OnLink	Yes	
Adv.-Autonomous	Yes	
PD-Source	TUNNEL-6TO4	(max. 16 characters)
Adv.-Pref.-Lifetime	604800	(max. 10 characters)
Adv.-Valid-Lifetime	2592000	(max. 10 characters)
DecrementLifetimes	Yes	

10. Enter a name for the interface that uses the 6to4 tunnel, e. g. "INTRANET".
11. Set the value for the **Prefix** to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
12. Accept the default value of "1" for the **Subnet ID**.
13. Set **PD source** to the name of the remote peer that you previously defined in the example above, e.g. "TUNNEL-6TO4".
14. Save your entries with **Send**.
15. Change to the directory **LCOS Menu Tree > Setup > IPv6 > Router-Advertisement**, open the **Interface options** table and click on **Add**.



LCOS Menu Tree

- Setup
- IPv6
- Router-Advertisement

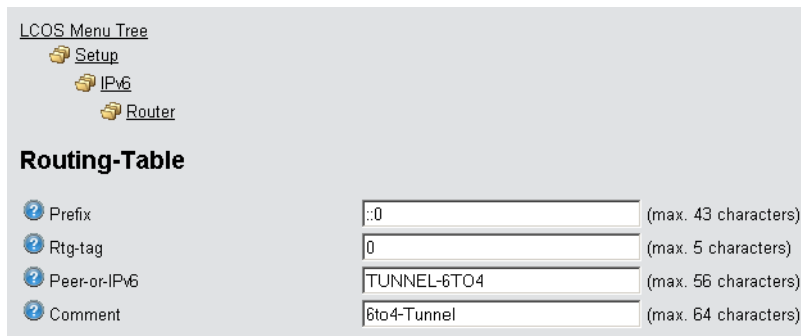
Interface-Options

Interface-Name	INTRANET	
Send-Adverts	Yes	
Min-RTR-Interval	200	(max. 10 characters)
Max-RTR-Interval	600	(max. 10 characters)
Managed-Flag	No	
Other-Config-Flag	Yes	
Link-MTU	1500	(max. 5 characters)
Reachable-Time	0	(max. 10 characters)
RTR-Time	0	(max. 10 characters)
Crit-Hop-Limit	0	(max. 5 characters)
Default-Lifetime	1800	(max. 10 characters)
Default-Router-Mode	auto	
Router-Preference	medium	

16. Accept all other default values without change.

17. Save your entries with **Send**.

18. Change to the directory **LCOS Menu Tree > Setup > IPv6**, open the **Routing table** and click on **Add**.



LCOS Menu Tree

- Setup
 - IPv6
 - Router

Routing-Table

Prefix	:::0	(max. 43 characters)
Rtg-tag	0	(max. 5 characters)
Peer-or-IPv6	TUNNEL-6TO4	(max. 56 characters)
Comment	6to4-Tunnel	(max. 64 characters)

19. Set the **Prefix** to the value ":::0".

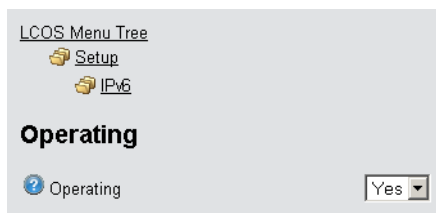
20. In the field **Rtg-tag** accept the default value "0".

21. In the field **Peer or IPv6**, enter the name of the interface that will use the 6to4 tunnel, e.g. "TUNNEL-6TO4" in the example above.

22. Enter a descriptive **Comment** for this entry.

23. Save your entries with **Send**.

24. Enable the IPv6 stack under **LCOS Menu Tree > Setup > IPv6** by setting the option **Operating** to "yes" and save with **Send**.



LCOS Menu Tree

- Setup
 - IPv6


Operating

Operating	Yes
-----------	-----

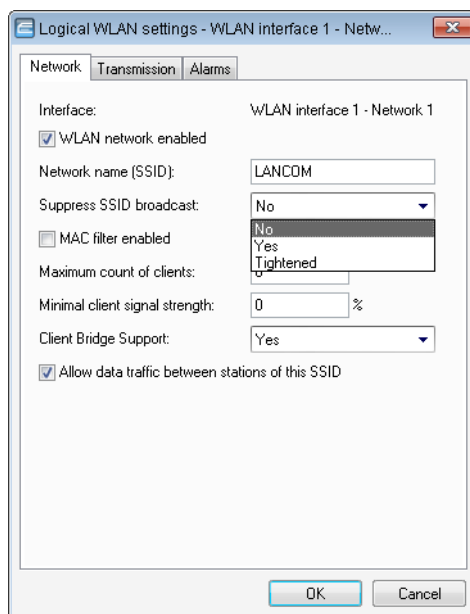
6 WLAN

6.1 Closed-network function: Suppress SSID broadcast

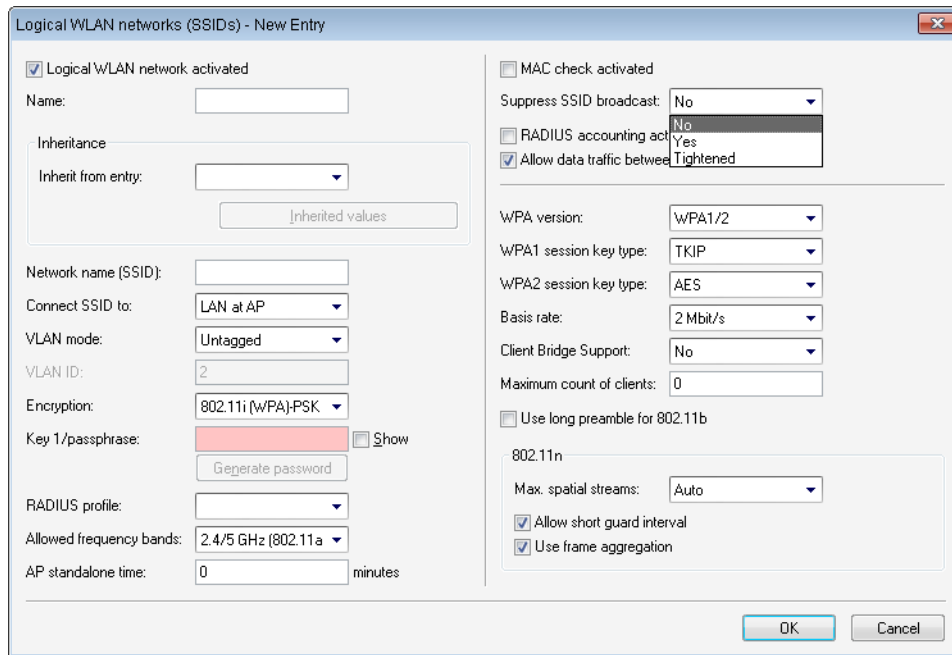
A WLAN client can only connect to a wireless network if it is informed of the corresponding SSID. The factory settings for many wireless networks allow the use of a blank SSID or the SSID "any", and continuing to use this means that potential intruders do not need to know the wireless LAN's SSID. The closed network function prevents unauthorized WLAN clients from logging into the WLAN. The access point rejects any attempt to log on with a blank SSID or the SSID "any". Any user wanting to logon to the WLAN must know the correct SSID.

 Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

LANconfig:Wireless LAN > General > Interfaces > Logical WLAN settings > Network.



LANconfig:WLAN Controller > Profiles > Logical WLAN networks (SSIDs)



The option **Suppress SSID broadcast** provides the following settings:

- **No:** The access point broadcasts the radio cell's SSID. When a client sends a probe request with a blank or incorrect SSID, the device responds with the SSID of the radio cell (publicly visible WLAN).
- **Yes:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID. The client cannot log on to the radio cell.
- **Tightened:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with a blank or incorrect SSID, the device does not respond. The client cannot log on to the radio cell. This setting also reduces the network load if there is a large number of WLAN clients in the radio cell.

6.1.1 Additions to the menu system


Closed network (for standalone access points only)

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

- **No:** The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
- **Tightened:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

 Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

SNMP ID:

2.23.20.1.4

Telnet path:**Telnet path: Setup > Interfaces > WLAN > Network****Possible values:**

No

Yes

Tightened

Default:

No


SSID broadcast (for WLAN controllers only)


You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated on the access point, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **SSID broadcast** provides the following settings:

- **Yes:** The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (publicly visible WLAN).
- **No:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
- **Tightened:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

 Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

 The "closed network" function for the access point is to be found under **Setup > Interfaces > WLAN > Network**. Please note: If the WLAN controller has the option **SSID broadcast** set to "No" (device does not broadcast the SSID), the access point sets its **closed network** option to "Yes", and vice versa. Only with the setting "Tightened" do both devices retain identical settings.

SNMP ID:

2.37.1.1.19

Telnet path:**Telnet path: Setup > WLAN-Management > AP-Configuration > Networkprofiles****Possible values:**

No

Yes

Tightened

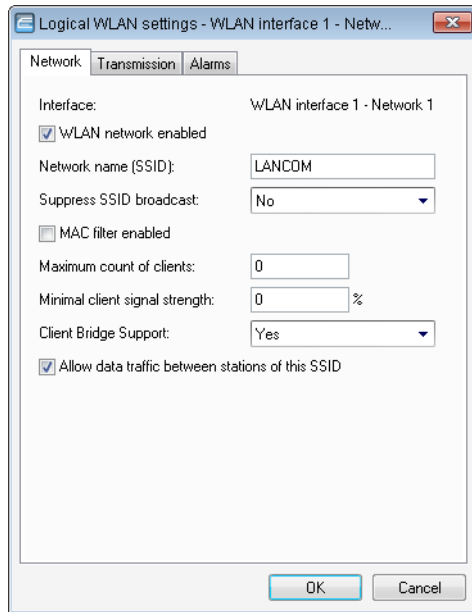
Default:

Yes

6.1.2 Enhancements to LANconfig

Network settings

LANconfig:Wireless LAN > General > Logical WLAN settings > Network



- **WLAN network enabled**

This switch enables or disables the corresponding logical WLAN.

- **Network name (SSID)**

Specify a unique SSID (the network name) for each of the required logical wireless LANs. Only network cards that have the same SSID can register with this wireless network.


- **Suppress SSID broadcast**

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.


The option **Suppress SSID broadcast** provides the following settings:

- **No:** The access point broadcasts the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty SSID, the access point similarly responds with an empty SSID.
- **Tightened:** The access point does not broadcast the radio cell's SSID. When a client sends a probe request with an empty or incorrect SSID, the access point does not respond.

 Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

- **MAC filter enabled**

The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (**Wireless LAN > Stations > Stations**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

 Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The access point always consults the MAC filter list for registrations with an individual passphrase, even if this option is deactivated here.

- **Maximum number of clients**

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

- **Minimum client signal strength**

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

- **Client-bridge support**

Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode.

 The client-bridge mode operates between two LANCOM devices only.

- **Allow traffic between stations of this SSID**

Check this option if all stations logged on to this SSID are to be able to communicate with one another.

6.2 New parameter for WLAN-client signal strength

LCOS version 8.62 now optionally evaluates the signal strengths of wireless LAN clients when they logon.

6.2.1 Additions to the menu system

Minimum client strength

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

SNMP ID:

2.23.20.1.16

Telnet path:**Telnet path: Setup > Interfaces > WLAN > Network****Possible values:**

0-100

Default:

0

6.3 Spectral scan

In addition to connecting computers to the Internet, professional users are increasingly using wireless local area networks (WLAN) for business-critical applications. Examples include accessing of patient files, online monitoring of production facilities, and the transmission of video and audio data (ideally without any time lags). The reliability and performance of WLAN systems are thus increasingly important.

The rising significance and usage of WLAN for data transmission is resulting in more and more scenarios where the equipment and systems of various users are crowding the WLAN frequency ranges. These may include, for example, microwave ovens, cordless telephones, Bluetooth devices and video transmitters, with their signals occurring on a continual or intermittent basis. The simultaneous usage of a frequency band or frequency range gives rise to interference that can disrupt or negatively impact the reliability and performance of a WLAN. This type of interference can result in data packets or connections being lost. If the interference is too strong, the complete failure of the WLAN may result.

It is therefore becoming increasingly important to use targeted analysis to check the frequency ranges. These checks should identify the interference or other interference factors, and introduce countermeasures as required. It can also be used to ensure that the WLAN is working properly and operating interference free.

Targeted analysis can also clarify or identify the following:

- Proper, fault-free operation of the WLAN
- Occurrence of interference
- Display or identify the bands with interference
- Strength of the interference signal
- Regularity or frequency of the interference signal
- Type, and possibly source, of the interference signal

The WLAN-related frequency ranges are subject to spectral analysis. Results are displayed graphically, i. e. in the form of real-time diagrams or real-time overviews of frequencies and interference. However, graphical analyses of a spectral range are open to some freedom of interpretation. A scenario such as the following would therefore be fairly commonplace. You ascertain that the frequency currently being used is being subjected to interference that is continual and of constant signal strength. However, you are not able to ascertain unequivocally which room or building the signal is coming from, nor the type of equipment which is transmitting the interfering signal.

6.3.1 Functions of the software module

The "Spectral Scan" software module enables you to run a spectral analysis directly on the access point. There is no need to purchase any additional software or hardware as the integrated functionality can be used to analyze the frequency ranges and bands in question. This gives you a graphical overview of the frequency response characteristics within your WLAN at all times so that you can detect interference and safeguard against it.

Clicking on the menu option **Extras > Spectral scan** in WEBconfig opens the window shown below:

Spectral Scan

Interfaces	Radio-Bands	Subbands	
WLAN-1:	2.4GHz/5GHz ▼	Band-1+2+3 ▼	Start
			▼
			Band-1+2+3
			Band-1
			Band-2
			Band-3
			Band-1+2
			Band-1+3
			Band-2+3

This page is used to start and stop the spectrum analyser.

Depending on the current state of the analyser, there will be different buttons and selections available:

Selection "Radio-Bands"
This selection defines which radio bands will be analysed once the spectrum analyser is started. In case it is running already the selection will be shown greyed-out.

Selection "Subbands"
If 5 GHz is selected as one of the radio bands the selection of subbands will be displayed to allow further specification of the frequency range to be analysed. The selection will be shown greyed-out if the spectrum analyser is running already.

Button "Start"
The spectrum analyser is started on the respective WLAN module by pressing this button. For each selected frequency band one additional window will be opened to display the results of the spectrum analyser. As long as the spectrum analyser is active, the WLAN module is unavailable for data transfers.

Button "Stop"
Stopping the spectrum analyser will revert the state of the WLAN module to the previous settings.

Button "Show"
This button will open one window for each selected frequency band to display the results of the spectrum analyser.

ⓘ When the WLAN module is disabled (**Setup > Interfaces > WLAN > Operational**), a message is displayed and the spectral scan cannot be started. Configure the access point for "Base station" operation or ensure that a WLAN controller configures the access point.

The following entries, buttons and selection menus are available here:

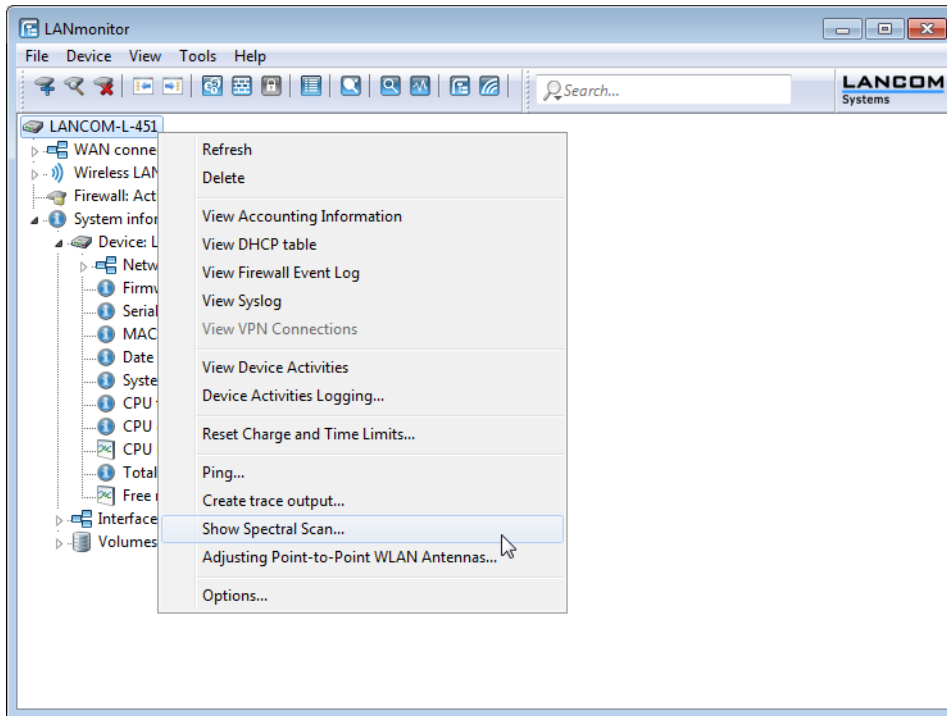
- **Interfaces:** Shows the selected WLAN module for analysis.
- **Radio bands:** Use this selection menu to set which frequency band(s) you wish to analyze. The relevant field is grayed out once the spectral scan has started on this module.
- **Sub-bands:** This selection menu is only enabled if '5GHz' or '2.4GHz/5GHz' is selected in **Radio bands**. You are then able to specify which sub-bands of the 5GHz band are included in the analysis.
- **Start:** Clicking this button starts the spectral scan on the relevant WLAN module. A separate window opens for each of the selected frequency bands.
- **Stop:** This buttons ends the analysis. The WLAN module then returns to the previous mode and is available again with its usual functionality.

ⓘ This button is only shown once the module has been started.

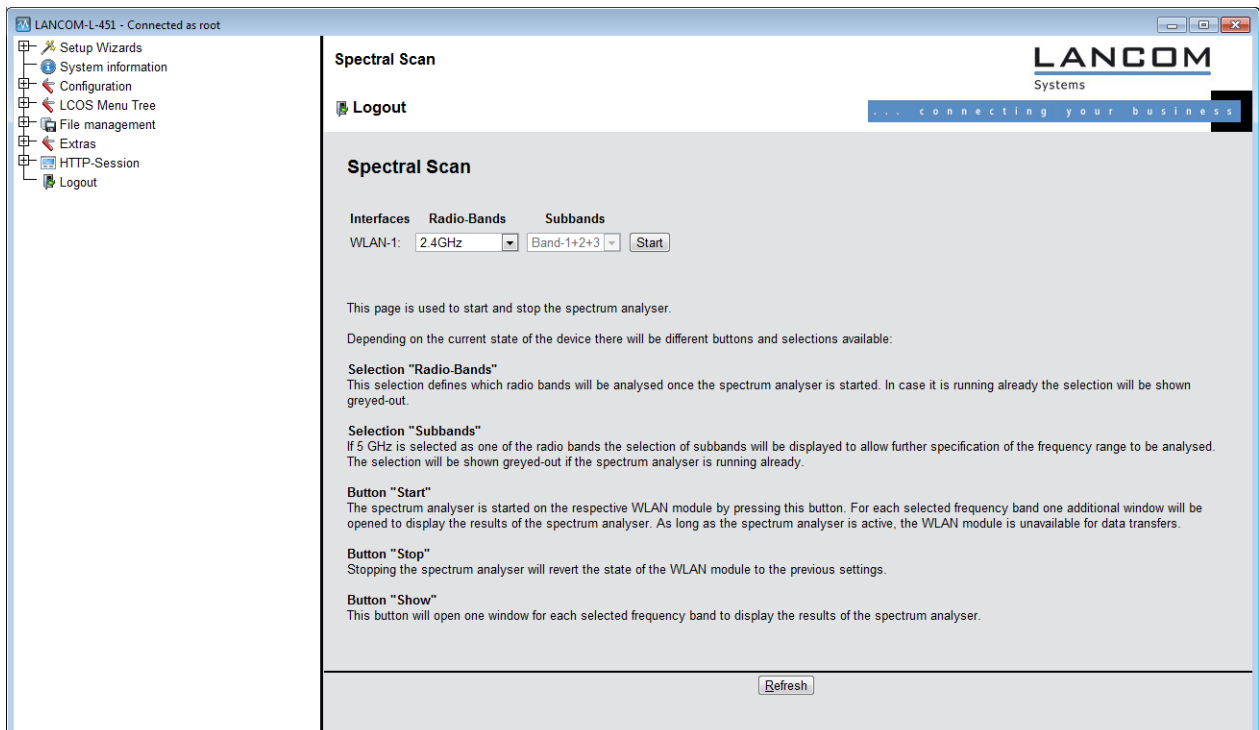
- **Show:** Once the spectral scan has started, click this button to open a window for each selected frequency band. Click the button repeatedly to open multiple windows.

6 WLAN

The spectral scan can also be started from the LANmonitor. To do this, right-click the relevant device in the list and select **Show spectral scan** in the context dialog.



A browser window opens showing you the same entries, buttons and selection menus as those in WEBconfig.



⚠ During the analysis, the WLAN module being analyzed does not send any data or transmit any SSID.

-
- ! The "Spectral Scan" function is supported by LANCOM access points of the L-4xx series, L-32x series, and the models 1781AW, 1781EW and 1780EW-3G only.

6.3.2 Spectral scan analysis window

-
- ! The spectral scan is displayed in a browser application. For this to work properly, your browser must support the latest version of WebSockets, and the HTML5 element `<canvas>`. The browser in LANmonitor meets all of these requirements.

In the separate analysis window of the spectral scan, there are different ways to show the frequencies and frequency ranges together with the potential interference. The following buttons are available at the top of the window:

- **Current:** Shows or hides the curve of the values being measured.
- **Maximum:** Shows or hides the maximum values of the ongoing spectrum scan in relation to the currently set history range.
- **Average:** Shows or hides the average values of the ongoing spectrum scan in relation to the currently set history range.
- **History:** Shows or hides the values last measured.
- **Number of history values:** Determines the number of results last measured that are displayed. You are able to show at least the last 5 and at most the last 50 measuring points for every frequency.
- **Last channel:** Shows or hides the channel last used.
- **Frequency:** Switches the display on the X-axis between WLAN channel and frequency.

The window contains two graphical views showing the readings in a different manner. The top diagram shows on the Y-axis the signal strength in dBm, and on the X-axis either the WLAN channel or the relevant frequency. The lower diagram contains the analysis progression over time in the form of a waterfall diagram, with the Y-axis showing the time and the X-axis again showing the WLAN channel or the relevant frequency. These view formats depict both continuous and occasional interference on the frequencies, so helping you to take appropriate action to improve the connection (e. g. by changing the channel or identifying and eliminating the interference source). For example, certain interference sources such as microwave devices, DECT telephones (working in the 2.4GHz frequency range) and audio-video transmitters exhibit very typical transmit patterns that occur prominently in both diagrams.

On the lower border of the window is a slider denoted **Time slider**. This enables you to extend or limit the time period analyzed in the waterfall diagram. Alternatively, you can use the input box to the right of the slider to select how many readings you would like to display in the waterfall diagram. The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached.

Below are some example analysis results showing graphically other settings in a different way:

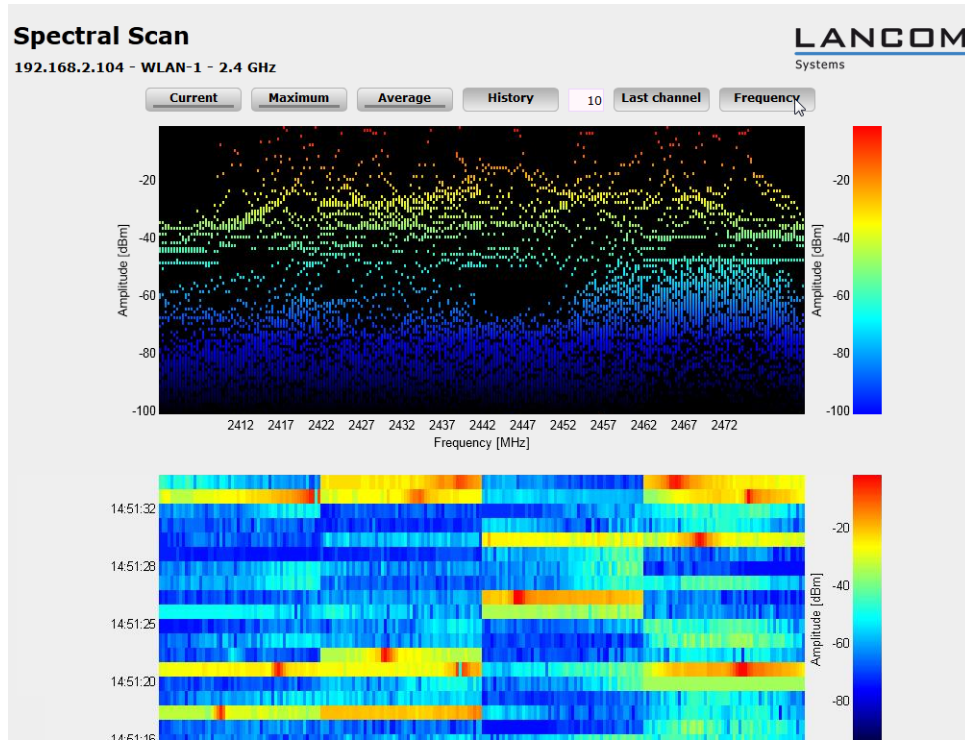


Figure 1: Spectral scan, frequency display of the last 10 history values

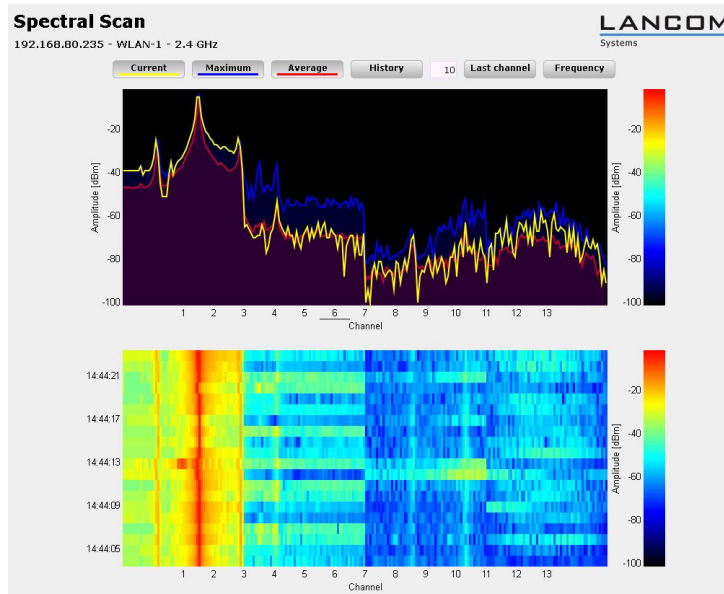


Figure 2: Spectral scan, channel display of Current, Maximum and Average, interference from radio camera

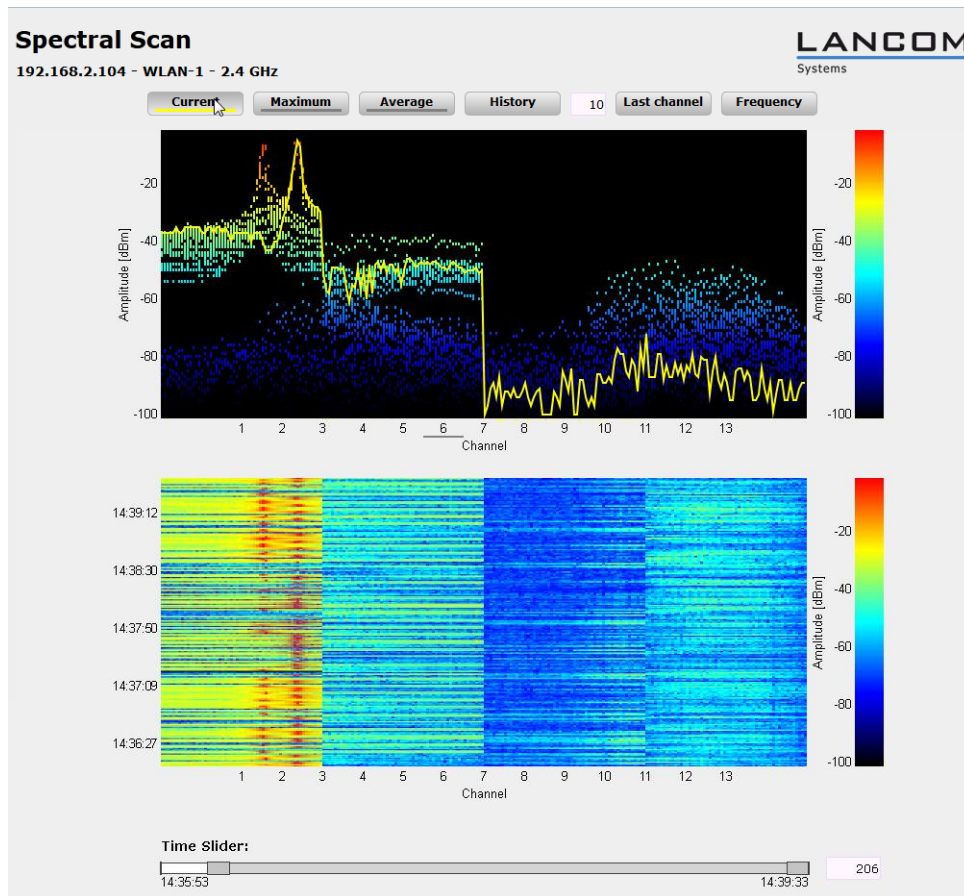


Figure 3: Spectral scan, channel display of Current, last 10 history values and "Time Slider", interference from baby phone

6.3.3 Enhancements to LANmonitor

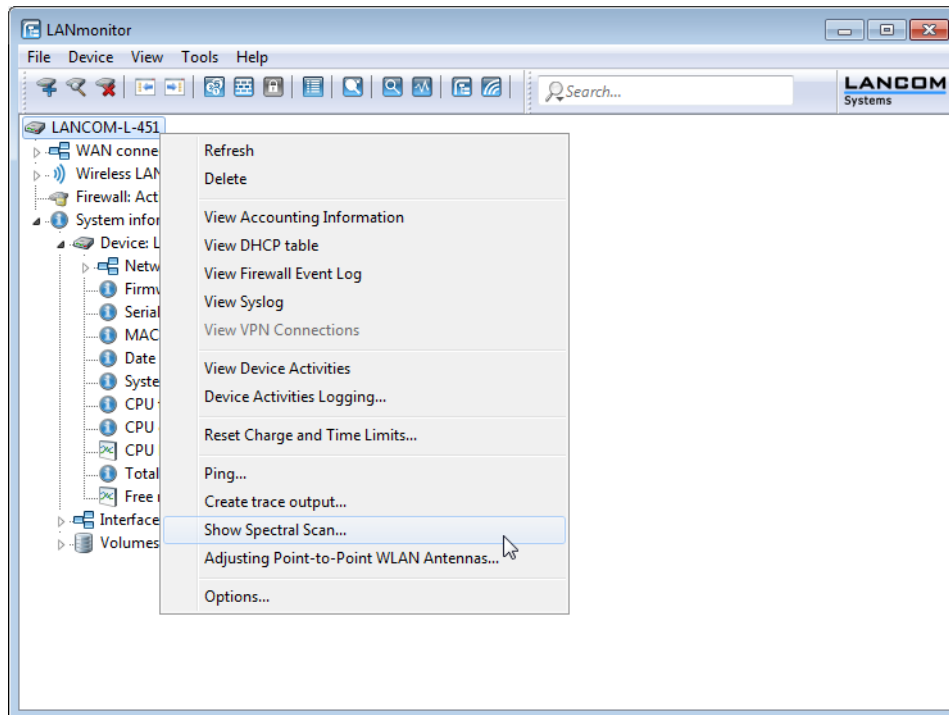
LANmonitor application concepts

This section outlines different application concepts for LANmonitor, such as using SNMP to query CPU and memory utilization, or performing spectral scans.

Spectral scan

The "Spectral Scan" software module enables you to run a spectral analysis directly on the access point. There is no need to purchase any additional software or hardware as the integrated functionality can be used to analyze the frequency ranges and bands in question. This gives you a graphical overview of the frequency response characteristics within your WLAN at all times so that you can detect interference and safeguard against it.

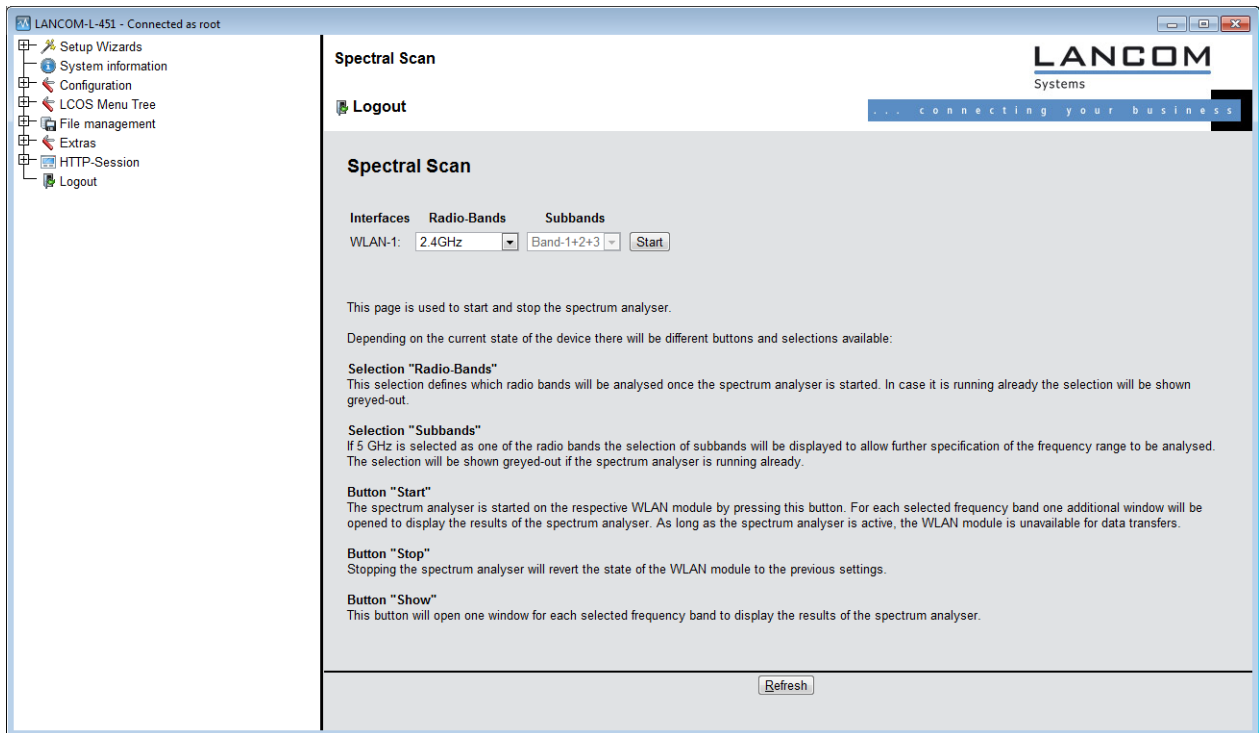
Right-click the relevant device in the list and select **Show spectrum analyzer** in the context dialog.



The following entries, buttons and selection menus are available here:

- **Interfaces:** Shows the selected WLAN module for analysis.
 - **Radio bands:** Use this selection menu to set which frequency band(s) you wish to analyze. The relevant field is grayed out once the spectral scan has started on this module.
 - **Sub-bands:** This selection menu is only enabled if '5GHz' or '2.4GHz/5GHz' is selected in **Radio bands**. You are then able to specify which sub-bands of the 5GHz band are included in the analysis.
 - **Start:** Clicking this button starts the spectral scan on the relevant WLAN module. A separate window opens for each of the selected frequency bands.
 - **Stop:** This buttons ends the analysis. The WLAN module then returns to the previous mode and is available again with its usual functionality.
-
- ! This button is only shown once the module has been started.
- **Show:** Once the spectral scan has started, click this button to open a window for each selected frequency band. Click the button repeatedly to open multiple windows.

! Please refer to Section [Spectral scan analysis window](#) for further information on the diagrams displayed.



! During the analysis, the WLAN module being analyzed does not send any data or transmit any SSID.

! The "Spectral Scan" function is supported by LANCOM access points of the L-4xx series, L-32x series, and the models 1781AW, 1781EW and 1780EW-3G only.

6.3.4 Additions to the Setup menu

Operation mode

All LANCOM wireless devices can be operated in various modes.

SNMP ID:

2.23.20.7.3

Telnet path:

Setup > Interfaces > WLAN > Operational

Possible values:

Access Point: As a base station (access point), the device establishes the link to a wired LAN for the WLAN clients.

Station: As a station (client), the device itself locates the connection to another access point and attempts to register with a wireless network. In this case the device serves to connect a wired device to a base station over a point-to-point link.

Managed AP: As a managed access point, the device searches for a central WLAN controller from which it can obtain a configuration.

Probe: In 'Probe' mode, the spectral scan uses the radio module of the access point. The device cannot transmit or receive data in this mode. On startup of the spectral scan, the device automatically switches to 'Probe' mode so that this setting need not be configured manually.

Default:

LANCOM Wireless Router: Access Point

LANCOM Access Points: Managed AP

Probe settings

This table contains the settings for the spectral scan.

 The device cannot transmit or receive data in this mode.

SNMP ID:

2.23.20.15

Telnet path:

Setup > Interfaces > WLAN

Ifc

Opens the settings for the physical WLAN interface.

SNMP ID:

2.23.20.15.1

Telnet path:

Setup > Interfaces > WLAN > Probe-Settings

Possible values:

Selection from the available physical WLAN interfaces.

Radio bands

Here you can select which frequency bands should be analyzed by spectral scanning.

SNMP ID:

2.23.20.15.2

Telnet path:

Setup > Interfaces > WLAN > Probe-Settings

Possible values:

2.4GHz

5GHz


2.4GHz/5GHz

Default:

2.4GHz

Subbands 2.4GHz

This setting determines which subbands of the 2.4GHz frequency are to be analyzed.

 The spectral scan only takes this field into account when either '2.4GHz' or '2.4GHz/5GHz' is set in **Radio bands**.

SNMP ID:

2.23.20.15.3

Telnet path:**Setup > Interfaces > WLAN > Probe-Settings****Possible values:**

Band-1

Band-2

Band-1+2

Default:

Band-1

Channel list 2.4GHz

Specify in this field the list of channels for the spectral scan in the 2.4GHz frequency band. Individual channels are separated with commas.

There is no need to change the default values of the spectral scan for operations. The spectral scan examines 20MHz-wide frequency bands at a time. Due to the 5MHz gaps between the individual 20MHz-wide channels in the 2.4GHz radio band, the channels specified result in a continuous scan of the entire 2.4GHz radio band. In the 5GHz band, the channel bandwidth is also 20MHz, and the individual channels lie next to each other with no overlapping. When no channels are specified, all channels are scanned which results in a complete scan in the 5GHz band.

SNMP ID:

2.23.20.15.4

Telnet path:**Setup > Interfaces > WLAN > Probe-Settings****Possible values:**

Max. 48 characters


from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./:;<=>?[]^_0123456789

Default:

1, 5, 9, 13

Subbands 5GHz

This setting determines which subbands of the 5GHz frequency are to be analyzed.

 The spectral scan only takes this field into account when either '5GHz' or '2.4GHz/5GHz' is set in **Radio bands**.

SNMP ID:

2.23.20.15.5

Telnet path:**Setup > Interfaces > WLAN > Probe-Settings****Possible values:**

Band-1

Band-2

6 WLAN

Band-1+2

Default:

Band-1

Channel list 5GHz

In this field, specify the list of channels for the spectral scan in the 5GHz frequency band. Individual channels are separated with commas.

SNMP ID:

2.23.20.15.6

Telnet path:

Setup > Interfaces > WLAN > Probe-Settings

Possible values:

Max. 48 characters

from ABCDEFGHIJKLMNOPQRSTUVWXYZ@{}~!\$%&'()+-./,:;<=>?[]^_0123456789

Default:

Blank

Channel dwell time

Here you set the number of milliseconds the spectral scan dwells on a channel.

The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached. The default value is generally adequate. Only lower the value when you need a more accurate resolution, and when the performance of your browser and PC is high enough to process the faster display of the readings.

SNMP ID:

2.23.20.15.7

Telnet path:

Setup > Interfaces > WLAN > Probe-Settings

Possible values:

Max. 10 characters

from 0 to 9

Default:

250

6.4 WLAN band steering

The IEEE 802.11 standard contains virtually no criteria by which a WLAN client should select the access point for a connection. While there are general guidelines according to which preference is given to an access point with a higher RSSI value (i. e. the received signal strength), for example, WLAN clients do not, in practice, adhere strictly to these definitions or the general guidelines. If both 2.4GHz and 5GHz are used to broadcast an SSID, there is normally no way of influencing the client as regards the preferred frequency band.

The steering of WLAN clients is based on the principle that many clients determine the available access points by means of an active scan. Active scanning here means that a client sends probe requests containing the network ID to which

the client is to connect. Access points with this ID then send a test response, enabling the client to create a list of available access points. The vast majority of WLAN clients only connect to access points from which they have received a probe response, and this can be used to steer their selection process.

There are multiple, sometimes very advanced, criteria for steering. One of these criteria relates to the wireless frequency ranges used for client communication. Modern dual-band WLAN clients are expected to prefer the 5GHz frequency band over the (now) overcrowded 2.4GHz band. Band steering is the term given to purposefully assigning a WLAN client a particular frequency band or range.

The list of detected or "seen" clients contains all clients from which the access point has received a test request packet. In combination with the radio frequency on which the WLAN client sends the test request, this list is one of the bases on which the access point decides whether to respond to the request or not.

Other criteria depend on the reported client IDs and the configuration of the devices. It may be the case, for example, that fewer SSIDs are reported on the preferred frequency band than are on the one with the lower preference. Similarly, too low a transmit strength when SSIDs are reported can result in the client not receiving any probe responses at all on the preferred frequency band. For the latter scenario, it is important to ensure that the access point does not suppress probe responses on the less favored frequency band. The minimum signal strength responsible here can be set in the following ways :

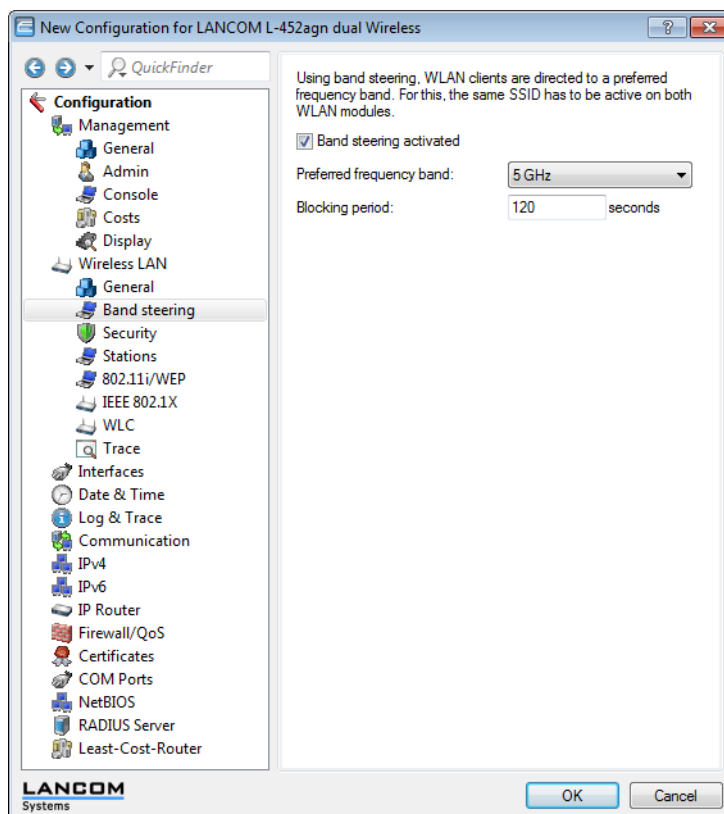
- LANconfig: **Wireless LAN > General > Logical WLAN settings > Network > Minimum client signal strength**
- WEBconfig: **Setup > Interfaces > WLAN > Network > Minimum station strength**

In LANconfig you can use **Wireless LAN > Band steering** to enable and manage the access point's band steering function.

6.4.1 Enhancements to LANconfig

Band steering

This dialog enables you to configure the settings for band steering in LANconfig.



The following functions are available in **Wireless LAN > Band steering**:

- **Band steering enabled**: Enables or disables this function.
- **Preferred frequency band**: Specifies the frequency band to which the device steers WLAN clients. Possible values:
 - **2.4GHz**: The device routes clients to frequency band 2.4GHz.
 - **5GHz**: The device routes clients to frequency band 5GHz.
- **Block time**: The time for which the access point steers the WLAN client to the preferred frequency band. The default value is 120 seconds.

6.4.2 Additions to the Setup menu

Client steering

This is where you determine the 'WLAN band steering' settings of the WLAN clients registered at the access point.

SNMP ID:

2.12.87

Telnet path:

Setup > WLAN

Operating

This option enables 'client steering' in the access point.

SNMP ID:

2.12.87.1

Telnet path:

Setup > WLAN > Client-Steering

Possible values:

Yes

No

Default:

No

Criteria

Determine here the criteria by which the access point controls the WLAN client.

SNMP ID:

2.12.87.2

Telnet path:

Setup > WLAN > Client-Steering

Possible values:

Radio-Band

Default:

Radio-Band

Preferred band

Set here the preferred frequency band that the access point steers the WLAN client to.

SNMP ID:

2.12.87.3

Telnet path:

Setup > WLAN > Client-Steering

Possible values:

5GHz

2.4GHz

Default:

5GHz

Probe request ageout seconds

Set the time (in seconds) that the WLAN client connection should be stored in the access point. When this time expires, the access point deletes the entry from the table.



This value should be set low if you are using clients in the WLAN that, for example, often switch from dual-band to single-band mode.

SNMP ID:

2.12.87.3

Telnet path:

Setup > WLAN > Client-Steering

Possible values:

Max. 10 characters

From 0 to 9

Special values:

0: The visible probe requests are deemed invalid immediately.

Default:

120

6.4.3 Additions to the Status menu

Seen clients**SNMP ID:**

1.3.45

Telnet path:

Status > WLAN > Client

This table contains the following status values:

Num-ProbeRsp-OK

Number of probe responses sent to and received by this client.

Num-ProbeRsp-Bad

Number of probe responses sent to and not received by this client (Tx errors).

Num-ProbeRsp-suppressed

Number of probe responses, which were sent to this client either because its signal strength was below the threshold or because band steering suppressed the response.

Band

Displays the WLAN band on which the client last communicated.

6.5 STBC / LDPC

6.5.1 Basics

Data transfers according to the IEEE-802.11n standard are performed using MIMO technology (multiple input, multiple output). The sender transmits data packets concurrently over multiple, spatially separated antennas, meaning that reflections and the resulting interference have little effect on the signal. However, the gain in throughput is less with each additional antenna, and the performance requirements for signal processing are increased.

Low Density Parity Check (LDPC)

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Space Time Block Coding (STBC)

The function 'STBC' (Space Time Block coding) additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

6.5.2 Additions to the Setup menu

Use STBC

Here you activate the use of STBC for data transfer per logical network (SSID).

 If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

SNMP ID:

2.23.20.2.23

Telnet path:

Setup > Interfaces > WLAN > Transmission

Possible values:

Yes

No


Default:

Yes (If the WLAN chipset supports STBC)

No (If the WLAN chipset does not support STBC)

Use LDPC

Here you activate the use of LDPC for data transfer per logical network (SSID).

 If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

SNMP ID:

2.23.20.2.24

Telnet path:

Setup > Interfaces > WLAN > Transmission

Possible values:

Yes

No

Default:

Yes (If the WLAN chipset supports STBC)

No (If the WLAN chipset does not support STBC)

6.5.3 Additions to the Status menu

Rx-STBC

This parameter indicates whether the detected remote station can receive data streams in STBC mode, and how many.

SNMP ID:

1.3.32.60

Telnet path:

Status > WLAN > Station-table

Possible values:

none

One

Two

Three

LDPC

This parameter indicates whether the selected WLAN interface supports LDPC encoding.

SNMP ID:

1.3.32.61

Telnet path:

Status > WLAN > Station-table

6 WLAN

Possible values:

Yes

No

Tx-STBC

This parameter indicates whether the detected remote station is capable of transmitting with STBC.

SNMP ID:

1.3.34.38

Telnet path:**Status > WLAN > Scan-Results****Possible values:**

Yes

No

Rx-STBC

This parameter indicates whether the detected remote station can receive data streams in STBC mode, and how many.

SNMP ID:

1.3.34.39

Telnet path:**Status > WLAN > Scan-Results****Possible values:**

none

One

Two

Three

LDPC

This parameter indicates whether the detected remote station can interpret LDPC-encoded data packets.

SNMP ID:

1.3.34.41

Telnet path:**Status > WLAN > Scan-Results****Possible values:**

Yes

No

Rx-STBC

This parameter indicates whether the detected remote station can receive data streams in STBC mode, and how many.

SNMP ID:

1.3.36.1.41

Telnet path:**Status > WLAN > Interpoints > Access-point-list****Possible values:**

none
One
Two
Three

LDPC

This parameter indicates whether the selected WLAN interface supports LDPC encoding.

SNMP ID:

1.3.36.1.42

Telnet path:**Status > WLAN > Interpoints > Access-point-list****Possible values:**

Yes
No

Rx-STBC

This parameter indicates whether the detected remote station can receive data streams in STBC mode, and how many.

SNMP ID:

1.3.43.51.38

Telnet path:**Status > WLAN > Client > Interfaces****Possible values:**

none
One
Two
Three

LDPC

This parameter indicates whether the selected WLAN interface supports LDPC encoding.

SNMP ID:

1.3.43.51.39

Telnet path:**Status > WLAN > Client > Interfaces****Possible values:**

Yes
No

Tx-STBC

This parameter indicates whether the detected remote station is capable of transmitting with STBC.

SNMP ID:

1.3.44.38

Telnet path:

Status > WLAN > Competing-networks

Possible values:

Yes

No

Rx-STBC

This parameter indicates whether the detected remote station can receive data streams in STBC mode, and how many.

SNMP ID:

1.3.44.39

Telnet path:

Status > WLAN > Competing-networks

Possible values:

none

One

Two

Three

LDPC

This parameter indicates whether the detected remote station can interpret LDPC-encoded data packets.

SNMP ID:

1.3.44.41

Telnet path:

Status > WLAN > Competing-networks

Possible values:

Yes

No

Rx-STBC

This parameter indicates how many data streams the selected WLAN interface can receive when the **STBC** option is enabled.

If **0** is displayed, the WLAN interface does not support STBC.

SNMP ID:

1.3.55.34

Telnet path:**Status > WLAN > WLAN-Parameter****Possible values:**

none

One

Two

Three

LDPC

This parameter indicates whether the selected WLAN interface supports LDPC encoding.

SNMP ID:

1.3.55.35

Telnet path:**Status > WLAN > WLAN-Parameter****Possible values:**

Yes

No

6.6 LANCOM-specific UUID information element for access points

As of LCOS version 8.80, LANCOM access points transmit a LANCOM-specific UUID device identifier.

6.6.1 UUID info element for LANCOM WLAN access points

All current LANCOM access points have multi-SSID capability. This means that they can simultaneously present different 'virtual' access points to their WLAN clients.

For devices with two radio modules (dual radio), the BSSIDs relate to the logical networks on the corresponding radio module. However, the MAC addresses of the two radio modules are completely independent of one another. Consequently, logical networks with different BSSIDs cannot be unequivocally related to a single device.

However, for the planning and monitoring of networks, it is often desirable to be able to relate logical networks to their respective devices (or radio modules).

LANCOM access points support an Aironet-compatible information element that contains the name of the device as assigned to it by the administrator. The transmission of this information is optional and many operators disable it for security reasons because they want to publish as little information as possible about the access point on the network.

Thus, this information either does not appear for network monitoring at all or, depending on the setting, the information may not identify the device as a LANCOM access point.

Besides this, LANCOM access points possess a UUID (universally unique identifier), which is calculated from the device type and serial number and can identify the device uniquely on the network. By using encryption when generating the UUID, the device type or serial number can only be inferred with considerable effort (brute-force attack for all types of devices and serial numbers).

Transmission of the UUID can be switched on or off independent of the radio module and logical network.

Additions to the Setup menu

Include UUID

Here you can determine whether the corresponding radio module should transfer its UUID.

SNMP ID:

2.23.20.1.17

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:

Yes

No

Default:

Yes

6.7 DFS

This section contains information about DFS (Dynamic Frequency Selection).

6.7.1 DFS4

As of LCOS version 8.80 all devices transmitting on the 5GHz WLAN frequencies support the standard ETSI EN 301 893 V1. 6. 1 ("DFS4").

6.7.2 Function and the history of development


For the DFS method (Dynamic Frequency Selection) required for 5 GHz WLANs, an unused frequency is automatically selected, for example, to avoid interference from radar systems or to distribute WLAN devices as evenly as possible over the entire frequency band. Occasionally, however, signals from weather radar stations cannot be identified reliably.

For this reason the European Commission is extending the requirements of the standards ETSI EN 301 893 V1.3.1 and ETSI EN 301 893 V1.4.1 to additionally avoid the use of three channels (120, 124 and 128) in subband 2 of the 5 GHz band, and not to allow use of these bands for automatic channel selection until a process to auto-detect weather radar station signals is made available. The versions EN 301 893 V1.3 and EN 301 893 V1.4 are referred to as "DFS2"

In the middle of 2010 the new version ETSI EN 301 893 V1.5.1 came into force, which was accompanied by changes in the usage of WLAN frequencies in the ranges 5.25 to 5.35 GHz and 5.47 to 5.725 GHz. The new Version 1.5.1 regulates the DFS (Dynamic Frequency Selection) method for the protection of radar stations from WLAN systems working in this frequency range. By using DFS to detect certain patterns in the radio signals received, it is now possible to detect active radar stations, and WLAN systems can automatically switch their operating channel. To differentiate from previous regulations, the new standard EN 301 893-V1.5 for the updated DFS is referred to as "DFS3".

A pulse pattern can generally be described in terms of its pulse rate, pulse width and the number of pulses. Former DFS technology was only able to detect fixed radar patterns as defined by the various combinations of pulse rates and pulse widths which were stored in the WLAN device. According to DFS3, the device is now able to recognize changing pulse rates and pulse widths as radar patterns. Furthermore, two or three different pulse rates may be used within a radar signal.

The version ETSI EN 301 893 V1.5.1 (DFS-3) expires on 01/01/2013. The new version ETSI EN 301 893 v1.6.1 (known as "DFS4"), which also detects shorter radar pulses, applies thereafter.

 The recognition of weather radar stations (channels 120, 124 and 128 in the 5.6 to 5.65 MHz frequency range) is subject to special conditions. The DFS implementation in LCOS does not support the more stringent recognition conditions. Therefore, these three channels will be omitted from newer versions of LCOS.

Additions to the Setup menu

Preferred DFS scheme

All WLAN systems that have been put into operation since EN 301 893-V1.6 came into effect are required to use DFS4 in the 5GHz band.

Here you can select DFS2 (EN 301 893-V1.3), DFS3 (EN 301 893-V1.5) or DFS4 (EN 301 893-V1.6).

SNMP ID:

2.23.20.8.20

Telnet path:

Setup > Interfaces > WLAN > Radio-settings > Preferred-DFS-Scheme

Possible values:


EN 301 893-V1.3

EN 301 893-V1.5

EN 301 893-V1.6

Default:

EN 301 893-V1.6

 When upgrading from a firmware version older than LCOS version 8.80 to an LCOS version 8.80 or higher, the existing setting of DFS3 (EN 301 893-V1.5) remains in effect.

6.8 PMK caching in the WLAN client mode

When establishing a connection from a WLAN client to an access point operating with 802.1x-authentication, the two stations negotiate a shared key, known as the Pairwise Master Key (PMK), for the subsequent encryption. In applications with mobile WLAN clients (laptops in large offices, moving objects with WLAN connections in the industrial sector), the WLAN clients often change the access points via which they are logged in to the WLAN network. And although WLAN clients roam back and forth between different access points, in most cases these tend to be the same ones.

Access points typically save a negotiated PMK for a certain period of time. WLAN devices in WLAN client mode also store PMKs. As soon as a WLAN client starts a login procedure for which a connection already existed, the WLAN client can directly transfer the existing PMK to the access point. In this way, the two remote stations skip the PMK negotiation phase while establishing the connection, and the WLAN client and access point establish the connection much faster.

The WLAN client stores the negotiated PMK for the duration set under *Default lifetime*.

6.8.1 Additions to the Setup menu

PMK caching

Enables PMK caching in WLAN client mode

SNMP ID:

2.23.20.3.15

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

Yes

No

Default:

No

PMK-Caching

Manage PMK-caching here.

SNMP ID:

2.12.85

Telnet path:

Setup > WLAN > PMK-Caching

Default lifetime

Specifies the duration in seconds that the WLAN client stores the negotiated PMK.



Make sure that the time set here matches the session timeout in the accept message that the access point or RADIUS server sends to the WLAN client. Once this time has expired, the access point or RADIUS server requires a re-authentication.

SNMP ID:

2.12.85.1

Telnet path:

Setup > WLAN > PMK-Caching

Possible values:

0 to 4294967295

Default:

0

Special values:

0: The negotiated PMK expires immediately.

6.8.2 Additions to the Status menu

PMK caching

This directory contains the status of the PMK caches.

SNMP ID:

1.3.60

Telnet path:

Status > WLAN > PMK-Caching

Contents

This table contains all entries of the PMK caches.

SNMP ID:

1.3.60.1

Telnet path:

Status > WLAN > PMK-Caching > Content

Authenticator

This entry contains the MAC address of the authenticating access points.

SNMP ID:

1.3.60.1.1

Telnet path:

Status > WLAN > PMK-Caching > Content

Supplicant

This entry contains the MAC address of the authenticating WLAN client.

SNMP ID:

1.3.60.1.2

Telnet path:

Status > WLAN > PMK-Caching > Content

User name

This entry contains the user name, which the RADIUS server sends to the access point for access permission.

 If the RADIUS server does not transmit a user name, this field is left blank.

SNMP ID:

1.3.60.1.4

Telnet path:

Status > WLAN > PMK-Caching > Content

VLAN-ID

This entry contains the VLAN-ID, which the RADIUS server sends to the access point for access permission.

 If the RADIUS server does not transmit a VLAN-ID, this field is left blank.

SNMP ID:

1.3.60.1.4

Telnet path:

Status > WLAN > PMK-Caching > Content

Lifetime

This entry contains the lifetime of the PMKs in seconds. It is calculated from the validity of the session, which the RADIUS server transmitted with the access permission.

The value is 0 seconds if the RADIUS server did not transmit a duration or the PMK does not have a validity period.

SNMP ID:

1.3.60.1.5

Telnet path:**Status > WLAN > PMK-Caching > Content****Lifetime**

This entry shows whether a PMK has expired. If this is the case, the access point no longer accepts PMK-caching or authentication attempts with this PMK. Instead, it will launch a new 802.1x authentication.

SNMP ID:

1.3.60.1.6

Telnet path:**Status > WLAN > PMK-Caching > Content****Source**

This entry indicates how the WLAN client obtained the PMK:

- **Unknown:** The source is unknown. This entry should not occur in normal operation.
- **Authentication:** PMK is the result of a normal 802.1x-authentication between WLAN-client and access point.
- **Pre-Authentication:** PMK is the result of a normal 802.1x-pre-authentication between the WLAN client and another access point.

SNMP ID:

1.3.60.1.7

Telnet path:**Status > WLAN > PMK-Caching > Content**

6.9 Pre-authentication in WLAN-client mode

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the access point previously. The WLAN client uses pre-authentication to reduce the time to logon to the access point at the first logon attempt.


Usually, a WLAN client carries out a background scan of the environment to find existing access points that it could connect to. Access points that support WPA2/802.1x can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1x authentication as follows:

- The WLAN client logs on to the new access point via the infrastructure network, which interconnects the access points. This can be an Ethernet connection or a WDS link (wireless distribution system), or a combination of both connection types.
- A pre-authentication is distinguished from a normal 802.1x authentication by the differing Ethernet protocol (EtherType). This allows the current access point and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new access point and the WLAN client.



The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.

- When the client wants to connect to the new access point, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the *PMK caching*.

 On the client side, the number of concurrent pre-authentications is limited to four. This minimizes the network load on the central RADIUS server in network environments with large numbers of access points.

6.9.1 Additions to the Setup menu

Pre-authentication

Enables pre-authentication support for the corresponding WLAN.

 In order to be able to use pre-authentication, PMK caching must be enabled.

SNMP ID:

2.23.20.3.16

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

Yes

No

Default:

No

6.10 Time-staggered roaming for dual-radio client WLAN modules

If a dual-radio client moves from a WLAN cell to an adjacent cell, multi-radio handover coordination ensures that a WLAN module remains connected to the current access point until the second WLAN module is successfully logged in to the new WLAN cell.

If this function is enabled and there are one or more WLAN modules in the registration phase, the WLAN client locks the registration of the WLAN module with an existing connection. This prevents both of the modules simultaneously attempting to log in to the new cell, which would cause both WLAN connections to be lost.

If the locked WLAN module loses the connection before one of the other modules has negotiated a new connection, the client of this module unlocks it to negotiate a new connection.

If the WLAN module has successfully logged in to the new WLAN cell, this connection remains open for a minimum period, so that the access point of the new cell has enough time to update its network entries.

6.10.1 Additions to the menu system

Dual roaming

Here is where you manage the roaming behavior of devices with multiple WLAN modules.

SNMP ID:

2.12.80

Telnet path:

Setup > WLAN > Dual-Roaming

Group

Determines whether all WLAN modules participate in dual-roaming.

SNMP ID:

2.12.80.1

Telnet path:

Setup > WLAN > Dual-Roaming

Possible values:

Off

WLAN-1 + WLAN-2

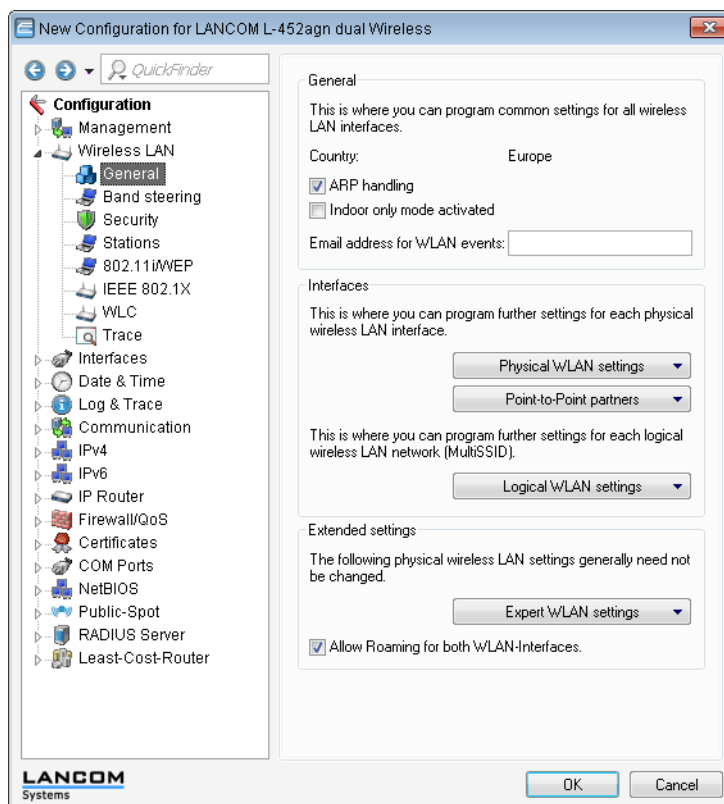
Default:

Off

6.10.2 Enhancements to LANconfig

Time-staggered roaming for dual-radio client WLAN modules

Time-staggered roaming is enabled under **Wireless LAN > General > Extended settings > Allow roaming for both WLAN interfaces.**



6.11 Greenfield mode for access points with IEEE 802.11n

For access points that comply with the IEEE 802.11n standard, the physical WLAN settings provide the option to allow or restrict data transmission according to the IEEE 802.11n standard.

Along with the selection of the individual a/b/g standards and a selection of mixed operating modes, the access points provide the option of using the Greenfield mode. Once activated in the physical WLAN settings for a WLAN interface, the Greenfield mode only allows WLAN clients that support the IEEE 802.11n standard to associate with the corresponding logical WLANs (SSIDs). Other WLAN clients that only work with the standards IEEE 802.11a/b/g cannot associate with these WLANs.

The IEEE 802.11n standard only allows connections that are either encrypted with WPA2/AES or unencrypted. WEP- and TKIP-based encryptions are not allowed in IEEE 802.11n. Please be aware of the following restrictions depending on the actual physical and logical WLAN settings:

- If, in the Physical settings, you activate support of a mixed-mode which includes the IEEE 802.11n standard and individual WLAN clients on a logical network only support WEP encryption, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with WEP.
- If, in the Encryption settings for a logical WLAN network, you enable not only AES session keys but also TKIP session keys, then the access point will use only the AES session key for this WLAN, because TKIP is not supported by IEEE 802.11n.
- If, in the Encryption settings for a logical WLAN network, you enable only TKIP session keys, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with TKIP.

6.12 Separate RADIUS server for each SSID

If you operate RADIUS for the central administration of accounts and access credentials in your wireless network, then the access point forwards requests for the authorization and accounting to the RADIUS server by default. If you are using a WLAN controller for access point management, then the controller can forward RADIUS requests from all of these access points to the RADIUS server.

In some cases, the operator of access points or WLAN controllers may wish to use a different RADIUS server for each logical wireless network (SSID). This may be the case, for example, when multiple customers share the same technical WLAN infrastructure but use their own authentication systems (e.g. with Wireless as a Service – WaaS).

In these cases, you have the option to choose a separate RADIUS profile for each logical WLAN (i.e. each SSID). The RADIUS profile contains all of the necessary information to use the appropriate RADIUS server, including the optional backup solution.

6.12.1 Additions to the menu system

RADIUS server profiles

By default, the WLAN controller forwards requests for account and access administration to the RADIUS server. In order for the access points to contact the RADIUS server directly, you define the necessary RADIUS profiles in this table. When setting up logical wireless networks (SSIDs), you have the option of choosing a separate RADIUS profile for each SSID.

SNMP ID: 2.37.35

Telnet path: /Setup/WLAN-Management

Name

Name of the RADIUS profile. This name is used to reference the RADIUS profile in the logical WLAN settings.

SNMP ID: 2.30.3.1

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 16 characters

Default: Blank

Access IP

IP address of the RADIUS server that authenticates user data. In the default setting with the IP address of 0.0.0.0, the access point sends RADIUS requests to the WLAN controller.

SNMP ID: 2.37.35.7

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Valid IP address.

Default: 0.0.0.0

Access port

Port of the RADIUS server that authenticates user data.

SNMP ID: 2.37.35.8

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 5 numbers

Default: 1812

Access secret

Password for the RADIUS server that authenticates user data.

SNMP ID: 2.37.35.9

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 32 characters

Default: Blank

Access loopback

Here, you can optionally configure a sender address for the RADIUS server that authenticates user data. This is used instead of the sender address otherwise selected automatically for the destination address. If you have configured loopback addresses, you can specify them here as sender address.

SNMP ID: 2.37.35.10

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Various forms of entry are accepted:
- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

 If there is an interface called "DMZ", its address will be taken in this case.

- LBO... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank

Access protocol

Protocol for communication between the access point and the RADIUS server that authenticates the user data.

SNMP ID: 2.37.35.11

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- RADSEC
- RADIUS

Default: RADIUS

Account IP

IP address of the RADIUS server that carries out the accounting of user activities. In the default setting with the IP address of 0.0.0.0, the access point sends RADIUS requests to the WLAN controller.

SNMP ID: 2.37.35.2

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Valid IP address.

Default: 0.0.0.0

Account port

Port of the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.3

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 5 numbers

Default: 1813

Account secret

Password for the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.4

Telnet path: /Setup/WLAN-Management/RADIUS-Server-Profiles

Possible values:

- Max. 32 characters

Default: Blank**Account loopback**

Here, you can optionally configure a sender address for the RADIUS server that carries out the accounting of user activities. This is used instead of the sender address otherwise selected automatically for the destination address. If you have configured loopback addresses, you can specify them here as sender address.

SNMP ID: 2.37.35.5**Telnet path:** /Setup/WLAN-Management/RADIUS-Server-Profiles**Possible values:**

- Various forms of entry are accepted:
- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ

 If there is an interface called "DMZ", its address will be taken in this case.

- LBO... LBF for the 16 loopback addresses.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Default: Blank**Account protocol**

Protocol for communication between the access point and the RADIUS server that carries out the accounting of user activities.

SNMP ID: 2.37.35.6**Telnet path:** /Setup/WLAN-Management/RADIUS-Server-Profiles**Possible values:**

- RADSEC
- RADIUS

Default: RADIUS**Backup**

Name of the backup RADIUS profile. This name is used to reference the backup RADIUS profile in the logical WLAN settings. The WLAN controller uses the settings from the backup RADIUS profile when the primary RADIUS server for authentication or accounting does not respond to queries.

SNMP ID: 2.30.3.12**Telnet path:** /Setup/WLAN-Management/RADIUS-Server-Profiles**Possible values:**

- Max. 16 characters

Default: Blank

Network profiles

Here you define the logical WLAN networks for activation and operation via the associated access points (APs).

SNMP ID: 2.37.1.1

Telnet path: /Setup/WLAN-management/AP-configuration

RADIUS profile

Here you enter the name of the RADIUS profile containing the information about the RADIUS server used for the authentication of the user data and the accounting of user activity.

SNMP ID: 2.37.1.1.35

Telnet path:/Setup/WLAN-Management/AP-Configuration/Networkprofiles

Possible values:

- Max. 16 characters

Default: Blank

6.12.2 Enhancements to LANconfig

Setting up the RADIUS profiles

In LANconfig, the settings for the RADIUS profiles in the WLAN controller are to be found under **WLAN Controller > Profiles > RADIUS profiles**.

RADIUS profiles - Edit Entry

Name:

Backup profile:

Authentication server

IP address:

Port:

Secret: Show

Source address:

Protocol:

Accounting server

IP address:

Port:

Secret: Show

Source address:

Protocol:

Selecting a RADIUS profile for a logical WLAN

In LANconfig, selecting the RADIUS profile for a logical WLAN in the WLAN Controller is done with the menu item **WLAN Controller > Profiles > Logical WLAN networks**.

7 Public Spot

7.1 Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

7.1.1 Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

```
http://<Geräte-URL>/cmdpbspotuser/  
?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

comment

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

```
&comment=<Inhalt1>:<Feldname1>;<Inhalt2>:<Feldname1>;  
...;<Inhalt5>:<Feldname5>
```

If there is just one comment field per user, then the comment is entered as follows:

```
&comment=<Comment>
```



Special characters such as German umlauts are not supported.



The maximum number of characters for the comment parameter is 191 characters.

print

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

printcomment

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

nbguests

The number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

defaults

Use default values

The wizard replaces missing or incorrect parameters with default values.

expiretype

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

```
&expiretype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- Value1: Expiry type (absolute, relative, absolute and relative, none)
- Value2: Expiration period of the voucher

If these parameters are omitted or set with incorrect values the wizard will apply the default values.

ssid

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

unit

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- Value1: Unit used to measure runtime. Possible values are: Minute, hour, day
- Value2: Runtime

timebudget

Time budget

If this parameter is omitted, the wizard uses the default value.

volumebudget

Volume budget

If this parameter is omitted, the wizard uses the default value.

multilogin

Multiple login

If you specify this parameter, the user can login multiple times with his/her user account. If omitted, then multi-login is disabled by default.



If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

7.2 Public Spot user administration

The Setup Wizards provide you with an easy method of managing Public Spot users.

7.2.1 Adding new Public Spot users with a single click

In WEBconfig, you can register new Public Spot users with the setup wizard **Create Public Spot Account**. This wizard is preset with default values, so you can set up a new user with a single click on **Save & Print**. By clicking on **Save & CSV export** the wizard provides you with the voucher data as a CSV file for download.

The following settings can be configured if required:

- **Starting time for account:** Sets the time when the voucher becomes valid. Possible values are:
 - **First login (default):** The time starts running when the user logs in for the first time
 - **Immediately:** The time starts running when the user is created
- **Validity period:** Enter the overall time period within which the voucher can remain valid.

 - ⓘ If the access is to be valid immediately, it is not possible to enter a validity period.
- **Duration:** Set how long access is to be available after registration or the first login.
- **SSID (network name):** Select the wireless LAN network for which the access applies. The default network name is already highlighted. This SSIDs listed here are managed in the SSID table.

 - ⓘ Press the "Ctrl" key to select multiple entries.
- **Number of vouchers:** Specify how many vouchers you want to create at a time (default: 1).
- **Time budget (minutes):** Specify the amount of time after which access to the Public Spot is closed.

 - ⓘ Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).
- **Volume budget (MByte):** Specify the available data volume after which access is closed.
- **Comment (optional):** Add a comment.
- **Prints comment on voucher:** Check this option if the comment is to appear on the voucher.
- **Print:** Check this option to print the vouchers as soon as they are registered (default: on)

 - ⓘ If this option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.
- **Multiple logins:** Enabling this option allows a user to login multiple times at the Public Spot with his/her user account (default: off).

You can configure the default values that are to be used when creating new Public Spot accounts in the following menus:

- LANconfig: **Public Spot > Public Spot Wizard**
- WEBconfig: **LCOS Menu Tree > Setup > Public-Spot module > Add user wizard**

7.3 Set case-sensitive for user names

You can specify whether the RADIUS server and the user wizard should check user names for upper and lower case letters.

7.3.1 RADIUS server

For each user, the RADIUS server stores the case-sensitive parameter in the user table, which determines if the RADIUS server should check user names for upper and lower case when they log in. Depending on the setting, this may mean that user names are not unique.

7 Public Spot

For example, three users registered on the Public Spot that each have a valid **Case-sensitive** setting can be present in the user table:

- User 1: Testuser, case-sensitive: Yes
- User 2: testuser, case-sensitive: No
- User 3: TESTUSER, case-sensitive: No

When the user Testuser wants to login, the RADIUS server must be able to discriminate which user wants to log in. It selects the user from the table according to the following priorities:

1. Entries with case-sensitivity enabled (case-sensitive: yes) have the highest priority.
2. Next, the RADIUS server checks the station mask entries in the respective user settings (**Setup > RADIUS > Server > Users**) in this order:
 - a. **Calling station ID mask:** An entry without wildcards ("?" or "**") has a higher priority than an entry with wildcards. A blank mask is the same as a wildcard ("**").
 - b. **Called station ID mask:** An entry without wildcards ("?" or "**") has a higher priority than an entry with wildcards. A blank mask is the same as a wildcard ("**").
3. If there are still conflicts, the RADIUS server selects the upper entry in the table.

Under **Setup > RADIUS > Server > Users > Case sensitive** you can specify whether the RADIUS server should evaluate the case sensitivity of the selected user name.

7.3.2 Public Spot Wizard

When registering a new Public Spot user, the Public Spot Wizard stores in the respective user profile whether or not the login is case-sensitive.

The following settings for the Public Spot Wizard can be made in **Setup > Public-Spot-Module > Add-User-Wizard**:

- **Case-sensitive:** Here you determine whether the wizard requires case-sensitivity for newly registered users. The default value is "Yes".
- **Hide case-sensitive checkbox:** If the Public Spot administrator should not be able to change the case-sensitive setting when running the wizard, you can use this option to hide the check box in the Public Spot Wizard. The default value is "Yes".

7.3.3 Additions to the Setup menu

Case sensitive

This setting determines whether the RADIUS server handles the user name case-sensitive.

SNMP ID:

2.25.10.7.17

Telnet path:

Setup > RADIUS > Server > Users

Possible values:

Yes

No

Default:

Yes

User name case sensitive

This setting determines whether the name of the newly created Public Spot user is case-sensitive.

SNMP ID:

2.24.19.12

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard

Possible values:

Yes

No

Default:

Yes

Hide case-sensitive checkbox

This setting determines whether the option for the case-sensitive input of user names is visible in the Public-Spot add-user wizard.

SNMP ID:

2.24.19.13

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard

Possible values:

Yes

No

Default:

Yes

7.4 Delegation of user account creation for Public Spots

Devices operating a Public Spot provide users with time-limited access to wireless networks. Until now an administrator account was necessary to create a login on a device with the Public Spot. For employees at a hotel reception desk, for example, you can set up an administrator account that only has the function rights to create Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests for access to the wireless network.

However, the easy voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network from the homepage of the Public Spot, and send it to themselves by e-mail or SMS (text message). To send SMS/text messages the device uses an external SMS provider which can charge the fees to the Public-Spot operator if desired.

7.4.1 Additions to the Setup menu

Authentication mode

Your device supports different types of authentication for network access with a Public Spot. To start with, you can specify whether a user needs to log in at all. The Public Spot stores the credentials in the user table. If you choose to use a registration procedure, you have two options:

- Login is performed with either a user name and password, or additionally with the physical or MAC address. In this case the administrator communicates the access credentials to the user by printout.
- Alternatively, access credentials can be sent automatically to users registering for first time either by e-mail or SMS (text message).

SNMP ID:

2.24.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Mode

Possible values:

None

User+password

MAC+user+password

E-mail

E-mail2SMS

Default:

Email2SMS

Authentication modules

In this menu option you define individual parameters for using the network login, and you specify how and with what parameters the authentication is performed and the login data is transmitted.

SNMP ID:

2.24.41

Telnet path:

Setup > Public-Spot-Module > Authentication-Module

E-mail authentication

This menu specifies the settings for authentication to the network and transmission of the credentials. The latter is done by e-mail.

SNMP ID:

2.24.41.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication**

Domain-List

With this list, you can specify whether you want e-mails from certain e-mail providers to be generally accepted or rejected. Use the "Add" button to add individual providers to the list. With the *Black-White-Domain-List* you determine whether you accept or reject a provider.



Please note that a Public Spot operating with an empty domain list will black-list (reject) all domains.

SNMP ID:

2.24.41.1.9

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Domain-List****Possible values:**

Valid e-mail domains (such as @hotmail.com) with a maximum of 150 characters.

Default:

Blank

User must accept GTC

This parameter is used to specify whether a user has to accept the general terms and conditions of use in order to be able to access the network.

SNMP ID:

2.24.41.1.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > E-mail-Authentication > User-Must-Accept-GTC****Possible values:**

Yes

No

Default:

Yes

Subject

Enter the subject line of the e-mail that is sent.

SNMP ID:

2.24.41.1.3

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Subject

Possible values:

Max. 250 characters

Default:

Your Public Spot Account

Black-White-Domain-List

In this menu you have the possibility to add your own list of domains for e-mail providers as a "blacklist" or as a "whitelist". Set the menu to "blacklist", if you want to completely block the listed providers. Use "Whitelist" to generally allow the listed providers.

SNMP ID:

2.24.41.1.8

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Black-White-Domain-List

Possible values:

Blacklist

Whitelist

Default:

Blacklist

Limit e-mails per hour

Enter the maximum number of e-mails sent within one hour to Public-Spot users with login data.

SNMP ID:

2.24.41.1.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > E-mail-per-hour-limit

Possible values:

Max. 5 numbers

Default:

100

Local e-mail address

Enter the sender e-mail address for the e-mail that is sent.

SNMP ID:

2.24.41.1.6

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Local-E-mail-Address

Possible values:

Valid e-mail address with a maximum of 150 characters.

Default:

Blank

Maximum request attempts

With this parameter you specify how many different credentials can be requested for a MAC address within one day.

SNMP ID:

2.24.41.1.5

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Max-Request-Attempts

Possible values:

Max. 5 numbers

Default:

3

Name

Enter the sender name for the e-mail that is sent.

SNMP ID:

2.24.41.1.7

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Name

Possible values:

Max. 150 characters

Default:

Blank

Body

With this parameter you can specify the contents of the e-mail, where \$PSpotPasswd is the variable for the generated password.

SNMP ID:

2.24.41.1.4

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Text

Possible values:

Max. 500 characters

Default:

Your password for LANCOM Public Spot is \$PSpotPasswd.

E-mail2Sms-Authentication

This menu specifies the settings for authentication to the network and transmission of the credentials. The latter is done by SMS.

SNMP ID:

2.24.41.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication****Allowed country codes**

You can specify the country codes in this list that are permitted for foreign telephone numbers, which can be useful to exclude certain countries.

SNMP ID:

2.24.41.2.11

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Allowed-Country-Codes****Possible values:**

Country name and the corresponding country code without the plus sign or leading zeros.

Default:

Blank

User must accept GTC

This parameter is used to specify whether a user has to accept the general terms and conditions of use in order to be able to access the network.

SNMP ID:

2.24.41.2.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > User-Must-Accept-GTC****Possible values:**

Yes

No

Default:

Yes

Subject

Enter the subject line of the e-mail that is sent. Keep in mind any formatting specifications for the SMS gateway.

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PSpotUserMobileNr` for the user's mobile phone number
- `$PSpotPasswd` for the user's password generated by the Public Spot



The Public Spot transmits the user's mobile phone number set with the variable `$PSpotUserMobileNr` without any leading zeros to the SMS gateway. If the SMS gateway expects a certain string for the country code (e.g. "00" or "+"), then enter this prefix in front of the variable.

SNMP ID:

2.24.41.2.3

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Subject****Possible values:**

Max. 250 characters

Default:Your password for LANCOM Public Spot is `$PspotPasswd`.**Limit e-mails per hour**

Enter the maximum number of e-mails sent within one hour to Public-Spot users with login data.

SNMP ID:

2.24.41.2.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > Email2SMS-Authentication > Limit-e-mail-per-hour****Possible values:**

Max. 5 numbers

Default:

100

Gateway e-mail address

Here you enter the address of your e-mail2SMS gateway for sending the credentials via SMS message. Keep in mind any formatting specifications for the SMS gateway.

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PspotUserMobileNr` for the user's mobile phone number

SNMP ID:

2.24.41.2.13

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Gateway-E-mail-Address****Possible values:**

Valid e-mail address of the gateway with maximum 150 characters. .

Default:

Blank

Local e-mail address

Enter the sender e-mail address for the e-mail that is sent.

SNMP ID:

2.24.41.2.5

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Local-E-mail-Address

Possible values:

Max. 150 characters

Default:

Blank

Maximum request attempts

With this parameter you specify how many different credentials can be requested for a MAC address within one day.

SNMP ID:

2.24.41.2.4

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Max-Request-Attempts

Possible values:

Max. 5 numbers

Default:

3

Name

Enter the sender name of the SMS.

SNMP ID:

2.24.41.2.6

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Real-Name

Possible values:

Max. 150 characters

Default:


Blank

Body

This parameter sets the contents of the sent e-mail. Keep in mind any formatting specifications for the SMS gateway.

You can use the following variables provided that the your e-mail2SMS gateways allows or requires them:

- `$PSpotUserMobileNr` for the user's mobile phone number
- `$PSpotPasswd` for the user's password generated by the Public Spot

 The Public Spot transmits the user's mobile phone number set with the variable `$PSpotUserMobileNr` without any leading zeros to the SMS gateway. If the SMS gateway expects a certain string for the country code (e.g. "00" or "+"), then enter this prefix in front of the variable.

SNMP ID:

2.24.41.2.12

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Body

Possible values:

Max. 512 characters

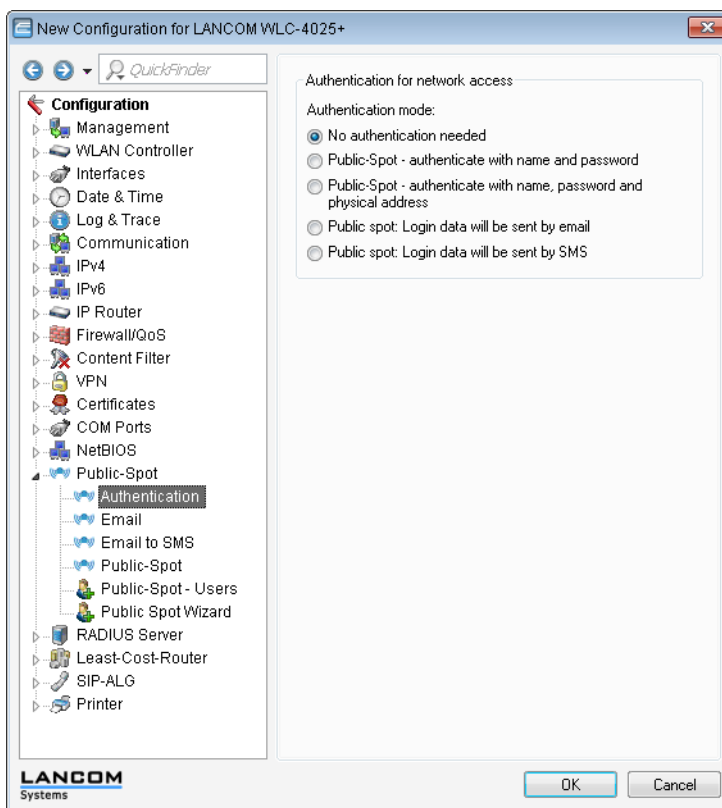
Default:

#Key#Route#From#

7.4.2 Enhancements to LANconfig

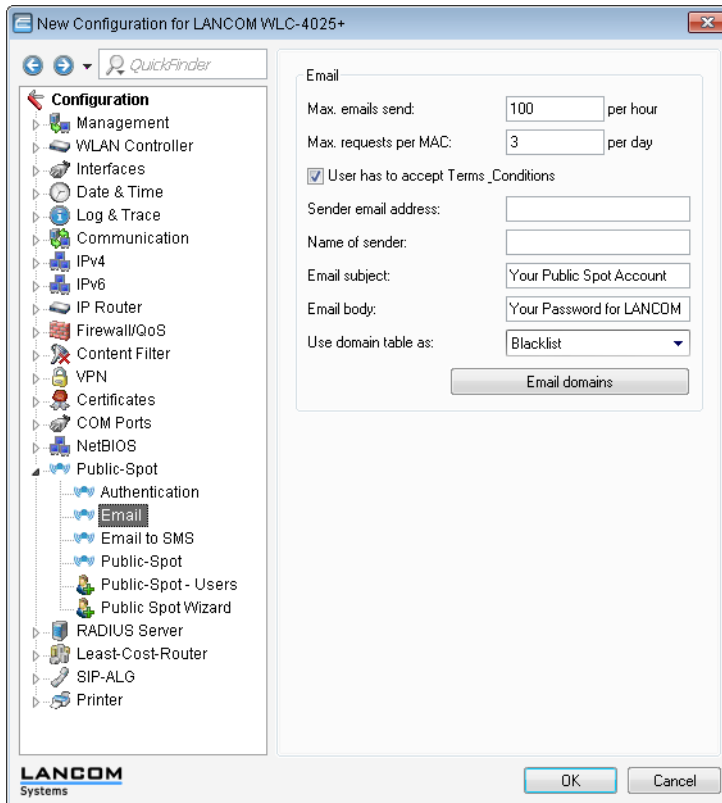
Authentication

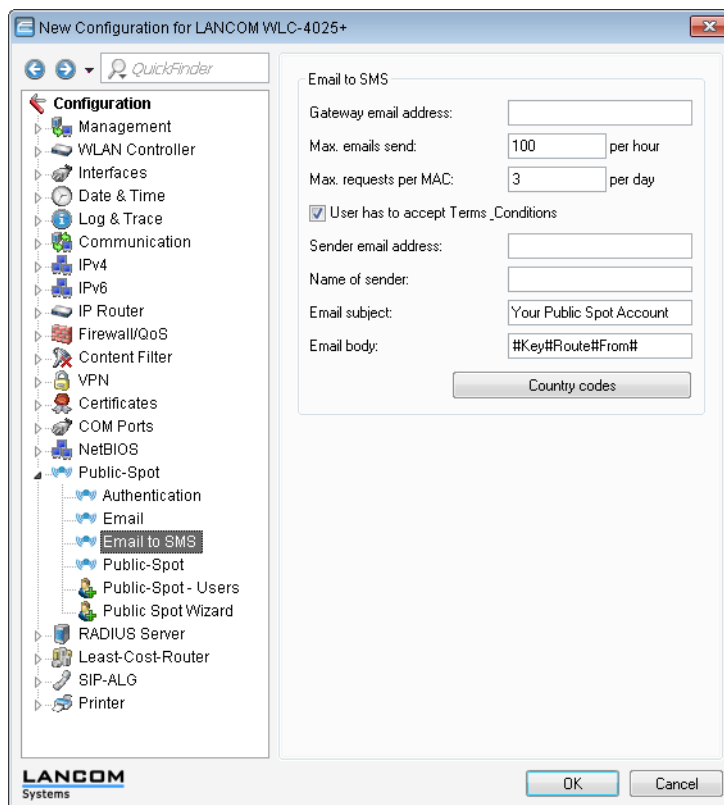
In this window, specify the settings for authentication to the network and transmission of the credentials.



E-mail/SMS

In this sequence of dialogs you define the settings for sending credentials via e-mail or SMS.





7.5 DNS snooping

You can allow the Public Spot users to access web pages, web servers, or entire networks on the Public Spot even without registering or signing in. You register the corresponding addresses here:

- LANconfig: **Public Spot > Public Spot > Allow access without authentication > Free networks**
- WEBconfig: **Setup > Public-Spot-Module > Free-networks**

Web services with a high number of users distribute the requests for data to multiple servers for better utilization. This means that two DNS queries for the same hostname (e.g. "www.google.com") can lead to two different IP addresses.

When you enter a host name, the Public Spot is assigned multiple valid IP addresses by the corresponding DNS server, but it only stores one for future requests from Public Spot users. If a different IP address for the same host name is allocated to the user by a different server for a subsequent request, the Public Spot blocks this connection because this IP address is not stored as the authenticated one.

In order for Public Spot users to be able to connect to the requested host despite changing IP addresses, the Public Spot analyzes the user's DNS queries and stores the returned IP address with the host name, the valid time to live (TTL), the age and the data source as a free destination address in the table **Status > Public Spot > Free-Hosts** for subsequent use.

The entries in this table will expire after the time period defined in the DNS response (TTL). When the limits are very low (e.g. 5 seconds), you can avoid locking out Public Spot users immediately after a request by setting a minimum validity under **Setup > Public Spot-Module > Free-Hosts-Minimum-TTL**.

7.5.1 Additions to the Setup menu

Free hosts minimum TTL

The configuration of the Public Spots can allow users to visit unlocked web pages, web servers or networks, free of charge and without requiring a login. The access point directs the visitors to the IP addresses corresponding to the host name. The access point saves the host names and the corresponding IP addresses in the state tables **Status > Public-Spot > Free-hosts** and **Status > Public-Spot > Free-networks**.

This value determines the time in seconds for which the addresses in the status table **Free hosts** are valid (TTL: "Time to live").

SNMP ID:

2.24.32

Telnet path:**Setup > Public-Spot-Module > Free-Hosts-Minimum-TTL****Possible values:**

Max. 10 characters

Special values:

0: The validity period is set by the duration in the DNS response (TTL).

Default:

300

7.5.2 Additions to the Status menu

Free networks

The **Free networks** table under **Status > Public-Spot** has been removed as of LCOS version 8.80. You will find the list of hosts, sub networks and IP addresses that are freely available for the Public Spot user in the tables **Status > Public-Spot > Free-Hosts** and **Status > Public-Spot > Free -Networks**.

Free networks

This table contains a list of all networks currently used by Public Spot users (with **address** and **mask**), which are registered in **Setup > Public-Spot-Module > Free-networks**, and which include a complete subnet address (i.e., a netmask other than 255.255.255.255).

SNMP ID:

1.44.31

Telnet path:**Status > Public-Spot**

Free hosts

This table contains a list of all networks currently accessible to Public Spot users. It shows both the "static" as well as "dynamic" entries:

- Static: The static entries are currently used hosts, which are registered in the setup table **Setup > Public-Spot-Module > Free-networks** with an IP address, and netmask 255.255.255.255. If you delete the corresponding entry in the setup table, you also delete the entry in the status table.
- Dynamic: The dynamic entries are the result of the analysis of DNS responses.

SNMP ID:

1.44.32

Telnet path:**Status > Public-Spot**

7.6 XML interface

In order to be able to cover a wide range of Public Spot scenarios, the default authentication method of name and password is not sufficient by itself. Access and accounting models using key cards, dongles or prepaid credit cards often require additional access data, which the Public Spot in this form would be unable to manage.

The implemented XML interface connects the Public Spot and an external gateway. It directs the user data only to the gateway that handles the authentication and accounting, and it only sends information about the duration and limits of the user access to the Public Spot.

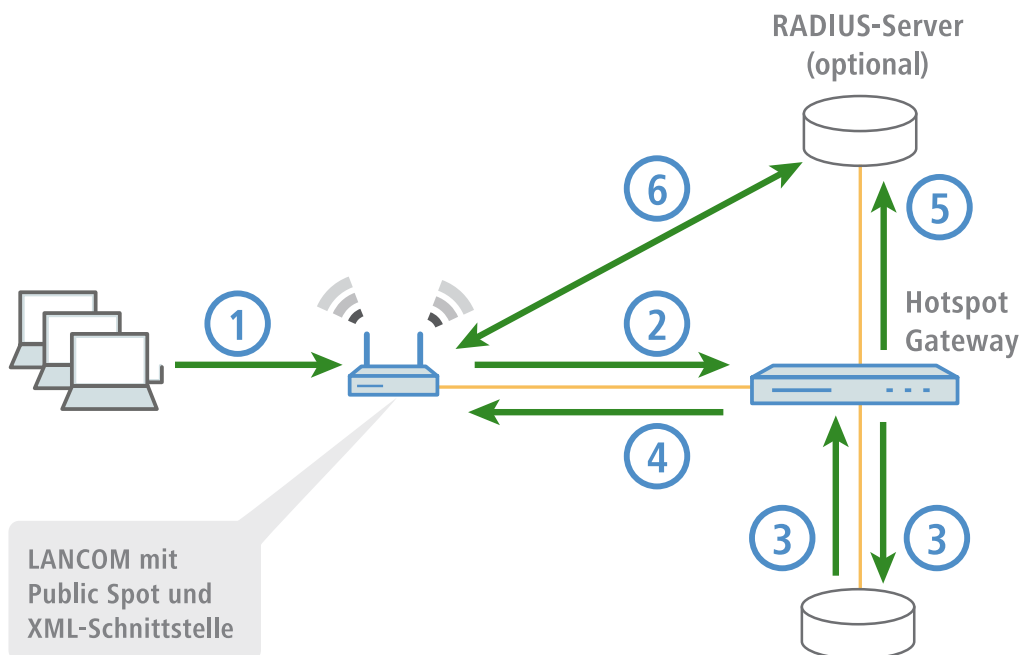
In this case, the Public Spot only performs the following tasks:

- Forward the user requests
- Restrict unauthorized access attempts
- Accept gateway commands to start and stop a session
- Accounting for sessions, if applicable

Since it is not realistic to implement all existing, and at times very specific scenarios with the associated gateway commands on the Public Spot, the XML interface was designed to be flexible and multi-purpose.

7.6 Function

The communication between the XML interface and external gateway is processed as follows:



1. The user connects to the Public Spot's WLAN and sends an HTTP request to the Public Spot.

- The Public Spot forwards the login procedure's HTTP request to the external hotspot gateway. The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

The Public Spot forwards the MAC address of the requesting Public Spot client to the external gateway. To implement this, navigate to **Public-Spot-Module > Page-Table**, set the **Type** to "Redirect" and suffix the **URL** with the parameter `?myvar=%m`.

Example: `http://192.168.1.1/?myvar=%m`

In this case, `myvar` is a freely selectable variable. The variable `%m` is vital here, as the Public Spot replaces this with the client's MAC address when forwarding the request.

- The hotspot gateway checks the user's credentials and, if applicable, it can contact further systems to charging to credit card, for example.
- The hotspot gateway sends an XML file with the user data to the Public Spot's XML interface. The external hotspot gateway contacts the device with the Public Spot XML interface using the URL `http://<Device-URL>/xmlauth`.


The Public Spot's XML interface analyses this file and initiates the corresponding actions. In the case of a login request, the XML interface inserts the user and the corresponding MAC address into the list of logged-on Public Spot users. In the case of a logout request, the XML interface removes the user from this list again. At the same time, the XML interface confirms the request by sending a corresponding XML file to the hotspot gateway.

In order for the Public Spot to be able to process the instructions in the XML file, a special administrator must be set up on the device who has the function right "Public-Spot -XML-interface". This hotspot gateway logs in to the Public Spot with this admin account.

While the user is logged in to the Public Spot, the XML interface and hotspot gateway can exchange status information about the current session in the form of XML files.

If the user has exhausted his online quota, the hotspot gateway will send a stop command to the XML interface, and then the Public Spot locks further access for that user. The XML interface also confirms that the login is blocked by sending the corresponding XML file to the hotspot gateway.

- If the additional use of a RADIUS server is enabled, the hotspot gateway optionally creates a user in a RADIUS server.
- The Public Spot sends relevant data to the RADIUS server throughout the session, for example to facilitate the accounting of the Public Spot usage. By default, the Public Spot uses its internal RADIUS server for this. If necessary, you can configure the device running the Public Spot to conduct forwarding to an external RADIUS server.

 Communications between the Public Spot and a hotspot gateway with the use of XML is not standardized. Configure the hotspot gateway according to the instructions in the [Commands](#) section in order for the Public Spot and hotspot gateway exchange the XML messages in the required form. XML messages are exchanged invisibly without a graphical user interface. You can use tools such as [cURL](#) to test the exchange of messages.

7.6 Setting up the XML interface via WEBconfig

The following section describes how to set up the XML interface.

 You need to have the "Supervisor" permission in order to create another administrator account.

- Log on to the WEBconfig home page as an Administrator.
- Go to **LCOS menu tree > Setup > Config > Admins** and click on **Add**.

3. Create a new administrator with the function right "Public Spot XML-interface". Save your entries with **Send**.

LCOS Menu Tree

- Setup
- Config

Admins

- Administrator: xml_admin (max. 16 characters)
- Password: (max. 16 characters)
- (Repeat) Password: (max. 16 characters)
- Active: Yes
- Access-Rights: none
- Function-Rights:
 - Basic-Wizard
 - Security-Wizard
 - Internet-Wizard
 - RAS-Wizard
 - Provider-Selection
 - LANLAN-Wizard
 - Time-Setting
 - Device-Search
 - WLAN-Linktest
 - Rollout-Wizard
 - WLAN-Wizard
 - Dynamic-DNS-Wizard
 - SSH-Command
 - Public-Spot-Xml-Interface
 - Public-Spot-User-Management-Wizard

Send Reset

This is the administrator account that the gateway uses to send XML files to the Public Spot XML interface.

4. Go to the screen **LCOS menu tree > Setup > Public-Spot-Module > XML-Interface** and enable the XML interface and, if necessary, the RADIUS authentication.
5. Go to **LCOS Menu Tree > Setup > Public-Spot-Module > Free-networks** and click on **Add**.
6. Enter the host name or IP address for the login page of the gateway to allow the Public Spot user to use its services. Enter "255.255.255.255" for the netmask. Save the entries by clicking on **Send**.
When defined as a free network, the user has direct access to the login page of the gateway without having to login to the Public Spot first.
7. Configure the gateway so that it sends the user's session data to the Public Spot XML interface as an XML file. Contact your service provider for questions regarding the configuration of the gateway.

7.6 Analyzing the XML interface using cURL

The following section describes the analysis of the XML interface with the open-source software cURL.

Client for URL, or cURL, is a command line application use for transferring files on a network without the use of a Web browser or FTP client. "cURL" is a component of many Linux distributions and is also available for other operating systems.

! To analyze the XML interface using cURL, you need an administrator account with the function right "Public-Spot-XML-interface" for the Public Spot.

1. First download cURL and install or unpack it.
2. Start cURL with the console command `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`
The parameters have the following meaning:

@filename

Path and name of the local XML file, e.g. the login request from the *examples*.

user

Username with the function right titled "Public-Spot-XML-interface". The XML feature does not work without this authentication.

pass

User password.

myhost

IP address or DNS name of LANCOM with the Public Spot XML interface

3. With Telnet you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

7.6.1 Commands

The XML interface can process three types of requests and responses:

- Login
- Logout
- Status


An XML file can contain several requests or answers.

Login

If the external gateway sends a "Login" request in an XML file, the Public Spot activates online access for the corresponding user. A "Login" request contains the attribute `COMMAND= "RADIUS_LOGIN"`.

If the Public Spot does not use a RADIUS server, a "login" request prompts it to store the user and the associated MAC address directly in the internal Status table. As a result, the user is immediately authenticated in future, and there is no need to display a login page for entering the username and password.

When you operate a RADIUS server, a 'login' request can only be successfully processed if the login data of the corresponding user already exists on the RADIUS server.

 The Web API in the Public Spot provides you with a convenient tool for creating new Public Spot users on the LANCOM's internal RADIUS server. Further information about this is available in the Reference Manual under the section "Public Spot".

The XML interface can process the following XML elements for a request:

SUB_USER_NAME

User name

SUB_PASSWORD

User password

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Login" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_STATUS

The current user status. The following values are possible:

- RADIUS_LOGIN_ACCEPT: Login okay
- RADIUS_LOGIN_REJECT: Login rejected

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

Some examples of XML files are given below:

Login request

The external gateway sends the data for the start of a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

The Public Spot enables 'user2350' in the internal Status table.

Login response:

The XML interface sends a confirmation about the start of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
  COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout

If the external gateway sends a "Logout" request in an XML file, the Public Spot blocks the corresponding user's online access. A "Logout" request contains the attribute `COMMAND="RADIUS_LOGOUT"`.

The XML interface can process the following XML elements for a request:

SUB_USER_NAME

User name

If the LANCOM receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then this user is logged out.

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Reason for the user to log off

The XML interface then sends the gateway a "Logout" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_STATUS

The current user status. The following values are possible:

- RADIUS_LOGOUT_DONE: Logout successful
- RADIUS_LOGOUT_REJECT: Logout rejected

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Reason for blocking access

Some examples of XML files are given below:

Logout request

The external gateway sends the command for ending a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout response:

The XML interface sends a confirmation about the end of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2">
```

```

COMMAND= "USER_STATUS" >
  <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
  <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
  <SUB_USER_NAME>user2350</SUB_USER_NAME>
  <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>

  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>

```

Status

The external gateway queries the current status of a user from the Public Spot with a "Status" request. A "Status" request contains the attribute `COMMAND="RADIUS_Status"`.

The XML interface can process the following XML elements for a request:

SUB_USER_NAME

User name

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Status" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

SUB_STATUS

The current user status. The following values are possible:

- `RADIUS_STATUS_DONE`: Status request successful
- `RADIUS_STATUS_REJECT`: Status request rejected, e.g. unknown user or MAC address

SESSION_TXBYTES

Current sent data volume

SESSION_RXBYTES

Current received data volume

SESSION_TXPACKETS

Number of data packets sent so far

SESSION_RXPACKETS

Number of data packets received so far

SESSION_STATE

Current status of the session

SESSION_ACTUAL_TIME

Current time

Some examples of XML files are given below:

Status request

The external gateway sends the command for a status request to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status response:

The XML interface sends a status message to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE ID="WLC-4006_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SESSION_ID>2</SESSION_ID>
    <SESSION_TXBYTES>0</SESSION_TXBYTES>
    <SESSION_RXBYTES>0</SESSION_RXBYTES>
    <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
    <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
    <SESSION_STATE>Authenticated</SESSION_STATE>
    <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

7.6.2 Additions to the Setup menu

XML interface

Configure the XML interface here.

SNMP ID:

2.24.40

Telnet path:

Setup > Public-Spot-Module > XML-interface

Operating

Enable the XML interface here.

SNMP ID:

2.24.40.1

Telnet path:**Setup > Public-Spot-Module > XML-interface****Possible values:**

Yes


No

Default:

No

Radius authentication

This item enables or disables authentication by a RADIUS server when using the XML interface of the Public Spot.

 The additional authentication by RADIUS server is only active if the Public Spot's XML interface is enabled (see [XML interface](#)).

SNMP ID:

2.24.40.2

Telnet path:**Setup > Public-Spot-Module > XML-interface****Possible values:**

Yes: The Public Spot forwards the request to the internal RADIUS server, or a RADIUS re-direct transfers it via a realm to an external RADIUS server.

No: No additional authentication necessary

Default:

Yes

7.7 Multiple logins

You now have the ability to allow Public Spot users to sign in to one account or into the WLAN with multiple devices simultaneously. This could be necessary for a group of people (such as a family) that has multiple devices, which they would like to use to simultaneously access the Internet.

To enable this feature, define the number of concurrent devices in the table **Max. concurrent logins table**. Here you can enter multiple values, which you can confirm in the second step with the **Create Public Spot account** wizard in the menu named like the table.

Please note that, using Telnet, the **Disallow multiple logins** parameter has to be set to **no**. In LANconfig this parameter is found under **Public Spot > Public Spot - Users > Allow multiple logins**.

7.7.1 Enabling multiple logins in the Public Spot Wizard

When you invoke the Wizard **Create Public Spot account**, you will see the menu item **Max concurrent logins**. The values shown here correspond to the numbers that you previously entered in the table of the same name. The values are shown within the phrase "Only ... device(s)".

7 Public Spot

Select the maximum number of concurrent devices that can have access to the account or to the WLAN for the corresponding user.

192.168.2.101 - Create Public Spot Account

Starting time for account	first login
Validity period: voucher expires after	365 days (max. 10 characters)
Duration	1 Day(s)
Max-Concurrent-Logins	Only 3 Device(s)

7.7.2 Additions to the Setup menu

Max. concurrent logins table

With this table you can set the number of devices that can simultaneously access each account; this is done by entering one or several values. By entering different values (e.g. 1, 3, 4, 5) you can respond to the needs of different users or user groups.

SNMP ID:

2.24.19.14

Telnet path:

Setup > Public Spot module > Add User Wizard > Max-concurrent-logins-table

Possible values:

Max. 5 numbers

Default:

0, 3, 10

Special values:

0 enables an unlimited number of logins for a single account.

7.8 Wizard for basic Public Spot configuration

As of LCOS version 8.80, a special Public Spot wizard assists you with the quick and easy setup of a Public Spot for simple scenarios.

7.8.1 Basic settings

The instructions for the basic settings are divided into three separate sections:

- The first section describes how to set up a Public Spot for local user administration, whereby the users are manually entered into the local user management system via LANconfig or WEBconfig.
-
- ⓘ To set up a Public Spot for a simple application scenario, you can start the corresponding wizard, which assists you in configuring the Public Spot.
 - The second section shows how to use the Public Spot Wizard with which new employees can be easily created without the need for additional administrator rights.
 - The third section describes the centralized management of user data on a RADIUS server.

To a certain extent these sections are dependent on one another, and ideally you should work through them in sequence.

7.8.2 Tutorials for setting up and using Public Spots

The following tutorials describe examples of how the Public Spot option can be implemented.

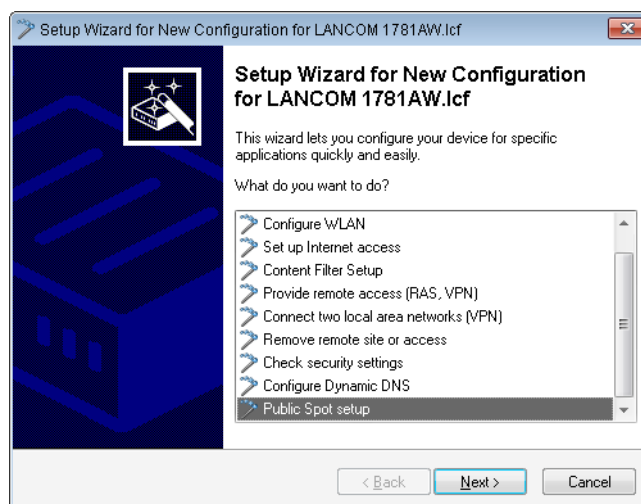
Basic installation of a Public Spot for simple scenarios

This tutorial describes how to use the Public Spot Wizard to perform a basic Public Spot installation.

Configuration via LANconfig

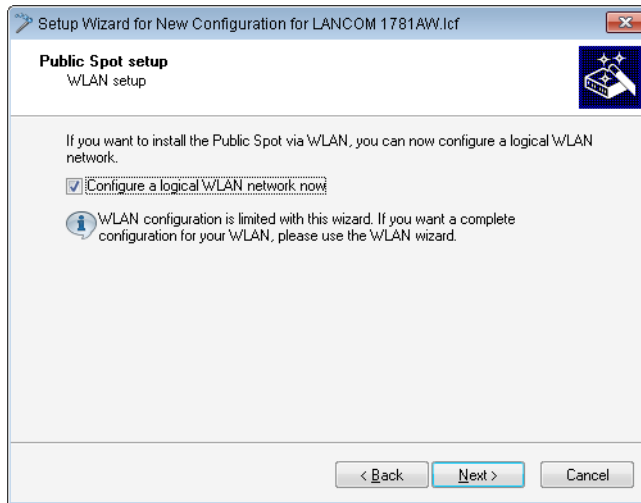
The following section describes the basic installation of a Public Spot with LANconfig.

-
- ! You need to have the "Supervisor" permission to be able to assign Public Spot management to an employee.
-
- ! The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.
1. Start LANconfig, for example from the Windows start menu with **Start > Programs > LANCOM > LANconfig**.
 2. Select the device on which you want to set up a Public Spot.
 3. Start the Setup Wizard with **Device > Setup wizard**, select the action **Public Spot** and then click on **Next**.

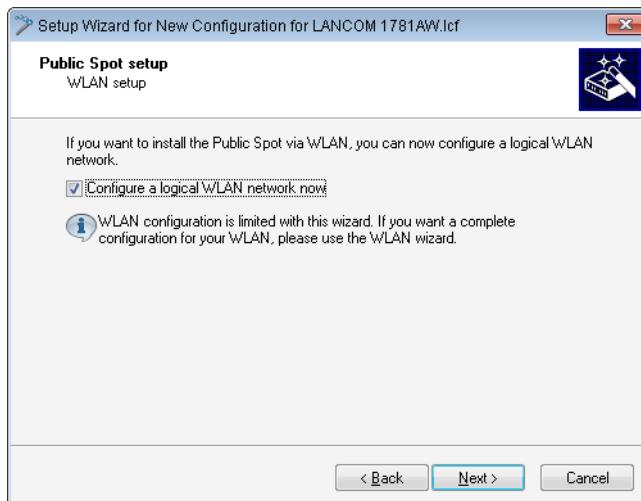


7 Public Spot

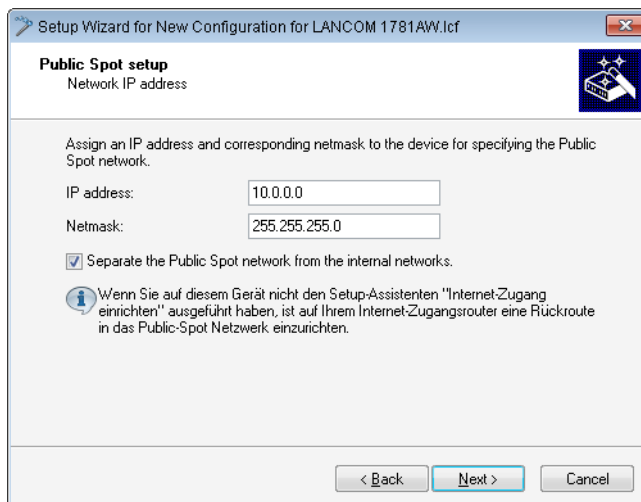
4. If you want the Public Spot to be available over WLAN, enable the corresponding option and then click **Next**.



5. Select the logical WLAN network for the Public Spot and enter the desired SSID. Click on **Next**.



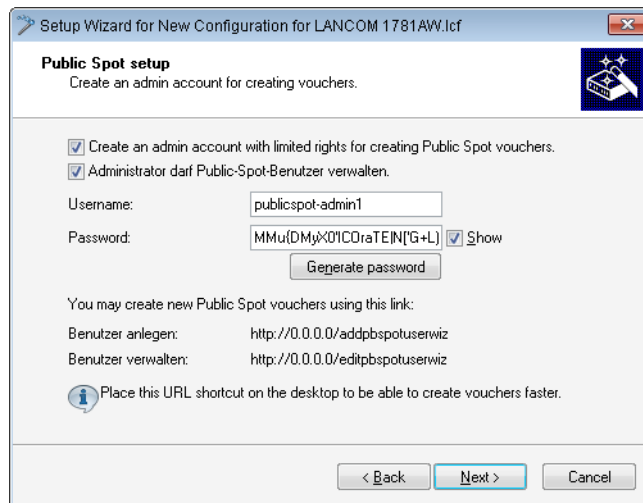
6. Enter the IP address and the subnet mask, and then click **Next**.



To do this, select the corresponding interface from the drop-down list, and then assign an IP address and a netmask.

If you want to separate the Public Spot network from internal networks for security reasons, check the corresponding option.

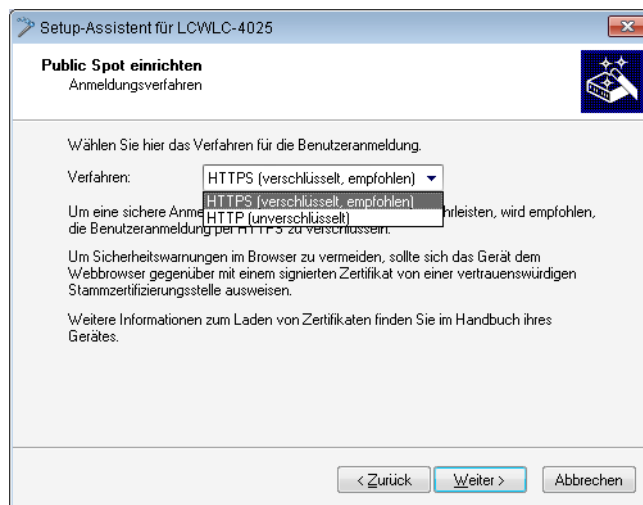
- If necessary, create a Public Spot administrator, who can manage Public Spot users. To continue, click on **Next**.



You can choose whether or not the administrator can manage existing users only or also create new users.

- ! Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to orange, and when it is very secure the background turns white.

- Select the procedure for user login.



You can select **HTTPS** or **HTTP** in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.

- The click **Next** and finally **Finish** to complete the basic installation of the Public Spot. The Setup Wizard will now send the settings to the device.

7.9 Distinct function rights

When you create a new administrator you can now specify whether the administrator can only create new Public Spot users or can manage them as well. Make these settings by clicking on the corresponding function rights in the **Admins** menu individually or jointly.

7.9.1 Additions to the Setup menu

Function rights

Each administrator has "function rights" that determine personal access to certain functions such as the Setup Wizards. You assign these function rights when you create a new administrator.

If you create a new administrator via Telnet, the following hexadecimal values are available to you. By entering one or more of these values with **set** you set the function rights.

In WEBconfig you assign the function rights by selecting the appropriate check boxes in the menu shown below.

SNMP ID:

2.11.21.3

Telnet path:

Setup > Config > Admins

Possible values:

- 0x00000001: The user can run the Basic Wizard.
- 0x00000002: The user can run the Security Wizard.
- 0x00000004: The user can run the Internet Wizard.
- 0x00000008: The user can run the Wizard for selecting Internet providers.
- 0x00000010: The user can run the RAS Wizard.
- 0x00000020: The user can run the LAN-LAN link Wizard.
- 0x00000040: The user can set the date and time (also applies for Telnet and TFTP).
- 0x00000080: The user can search for additional devices.
- 0x00000100: The user can run the WLAN link test (also applies for Telnet).
- 0x00000200: The user can run the a/b Wizard.
- 0x00000400: The user can run the WTP Assignment Wizard.
- 0x00000800: The user can run the Public Spot Wizard.
- 0x00001000: The user can run the WLAN Wizard.
- 0x00002000: The user can run the Rollout Wizard.
- 0x00004000: The user can run the Dynamic DNS Wizard.
- 0x00008000: The user can run the VoIP Call Manager Wizard.
- 0x00010000: The user can run the WLC Profile Wizard.
- 0x00020000: The user can use the integrated Telnet or SSH client.
- 0x00001000: The user can run the Public-Spot User management Wizard.

Default:

Blank

7.9.2 Enhancements to LANconfig

Specifying functional rights for new administrators

If you want to set up a new administrator, the button **Other administrators** on the dialog **Admin** determines whether the new administrator can use the Public Spot Wizard to create new users only, or to manage them as well. In the frame "function rights" there are two boxes for these settings, which are both labeled "Public spot Wizard(...)".



7.10 Additions to the Setup menu

7.10.1 Free networks

In addition to freely available web servers, you can define other networks which your customers can access without having to log on. As of LCOS version 8.80 you also have the option to enter the hostname using wildcards.

SNMP ID:

2.24.31

Telnet path:

Setup > Public-Spot-Module > Free -Networks

Host name

With this input field in the **Free networks** table, you can define a server, network, or individual web pages, which customers may use without a login. Here you can enter either an IP-address or a host name, both of which allow the use of wildcards. This allows you to enter values such as "203.000.113.*", "google.??*" or "*.wikipedia.org". The table is dynamic and the display is adjusted according to the number of host names and IP addresses that you enter.

SNMP ID:

2.24.31.1

Telnet path:

Setup > Public-Spot-Module > Free-networks > Host-name

Possible values:

Max. 64 Characters, including letters, numbers, hyphens, periods (.), and wildcards (?, *).

Default:

Blank

Mask

Enter the associated netmask here. If you wish to authorize just a single workstation with the previously specified IP address, enter 255.255.255.255 here. If you wish to authorize a whole IP network, enter the corresponding netmask.

SNMP ID:

2.24.31.2

Telnet path:

Setup > Public-Spot-Module > Free-networks > Mask

Possible values:

Max. 15 characters

Default:

0.0.0.0

8 Routing and WAN connections

8.1 Default mode in the DSLoL interface

As of LCOS version 8.80, the DSLoL interface is set to the default mode 'Exclusive'.

8.1.1 Additions to the Setup menu

Mode

This item selects the mode in which the WAN interface is operated. In automatic mode, all PPPoE frames and all data packets belonging to a connection established over the DSLoL interface (as configured in the IP parameter list) are routed via the DSLoL interface (WAN). All other data packets are treated as normal LAN packets. In exclusive mode, the LAN interface operates as a WAN interface only.

SNMP ID:

2.23.4.6

Telnet path:

Setup > Interfaces > DSLoL-Interface

Possible values:

Auto

Exclusive

Default:

Exclusive

9 Diagnosis

9.1 SYSLOG accounting is disabled by default

In the SYSLOG server table, you define which system information is sent by the device to the defined SYSLOG server, and with which SYSLOG level. By default, this table includes 8 entries for the destination IP address 127.0.0.1, which represents the internal SYSLOG device memory.

```
root@:/Setup/SYSLOG/Server
> 1
```

Idx.	IP-Address	Source	Level	Loopback-Addr.
0001	127.0.0.1	04	00	INTRANET
0002	127.0.0.1	01	1f	INTRANET
0003	127.0.0.1	10	02	INTRANET
0004	127.0.0.1	40	08	INTRANET
0005	127.0.0.1	02	0a	INTRANET
0006	127.0.0.1	08	08	INTRANET
0007	127.0.0.1	20	00	INTRANET
0008	127.0.0.1	80	01	INTRANET

By default, the device does not send any SYSLOG messages to SYSLOG's internal memory for the sources 04 (clock time) and 20 (accounting).

9.2 Boot-persistent SYSLOG, event log and boot log

As of LCOS version 8.80, you can save SYSLOG, event log, and boot log messages so that they are available even after rebooting the device (boot persistent).

9.2.1 Additions to the Setup menu

Backup interval

This parameter defines the interval in hours for the boot-persistent storage of SYSLOG messages to the flash memory of the device.

SNMP ID: 2.22.6

Telnet path: /Setup/SYSLOG

Possible values:

- 1 to 99

Default: 2

Backup active

Enables the boot-persistent storage of SYSLOG messages to the flash memory of the device.

SNMP ID: 2.22.7

Telnet path: /Setup/SYSLOG

Possible values:

- Yes
- No

Default: Yes

Maximum message age

This parameter defines the maximum period for retaining SYSLOG messages in the internal SYSLOG memory of the device in hours. After this period expires the device automatically deletes the obsolete SYSLOG messages if auto-delete is activated under [Remove old messages](#).

SNMP ID: 2.22.9

Telnet path: /Setup/SYSLOG

Possible values:

- 1 to 99

Default: 24

Remove old messages

This parameter enables deletion of the SYSLOG messages in the device after the period set for [Maximum-message-age](#).

SNMP ID: 2.22.10

Telnet path: /Setup/SYSLOG

Possible values:

- Yes
- No

Default: No

Save bootlog

This parameter enables or disables the boot-persistent storage of SYSLOG messages to the flash memory of the device. Bootlog information is not lost even when restarting after a loss of mains power.



If necessary, you can delete the persistent bootlog memory with the CLI command [deletebootlog](#).

SNMP ID: 2.11.71

Telnet path: Setup/Config

Possible values:

- Yes
- No

Default: Yes

9.2.2 Enhancements to command-line commands

Delete bootlog

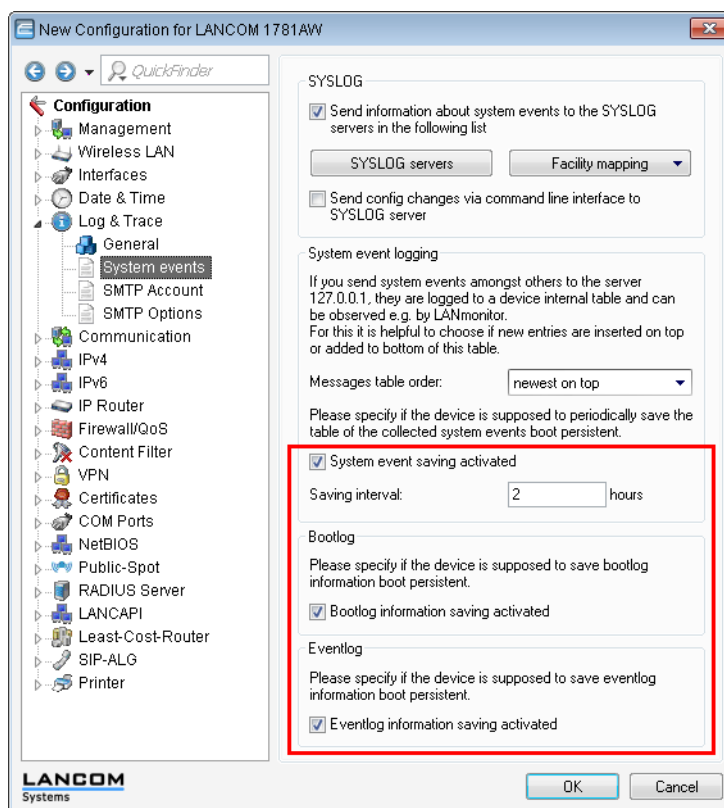
The bootlog saves the information about the boot processes of the device. With the parameter *Save-Bootlog* you can optionally enable persistent storage of the bootlogs.

By entering the command `deletebootlog` anywhere on the command line you can delete the contents of the persistent bootlog storage, if necessary.

9.2.3 Enhancements to LANconfig

Boot-persistent SYSLOG, event log and boot log

In LANconfig, the settings for the boot-persistent SYSLOG, event log and boot-log messages are to be found under **Log & Trace > System events**.



9.3 Logging configuration changes made via the command line

To meet the increased security requirements of network infrastructures, the devices are capable of logging to SYSLOG any changes to the configuration made via the command line interface. Configuration changes include any changes to the configuration parameters, executing actions, and uploading files such as certificates.

The devices write the following information to the SYSLOG:

- User name

- Name of the modified menu item or the executed action
- New value (or a notice that the change was not successful, e.g. due to a lack of permission)

9.3.1 Additions to the Setup menu

Log CLI changes

This parameter enables logging of the commands entered on the command line. Enable this parameter to log an entry in the internal SYSLOG memory when a command is entered on the command line of the device.



This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

SNMP ID: 2.22.8

Telnet path: /Setup/SYSLOG

Possible values:


- Yes
- No

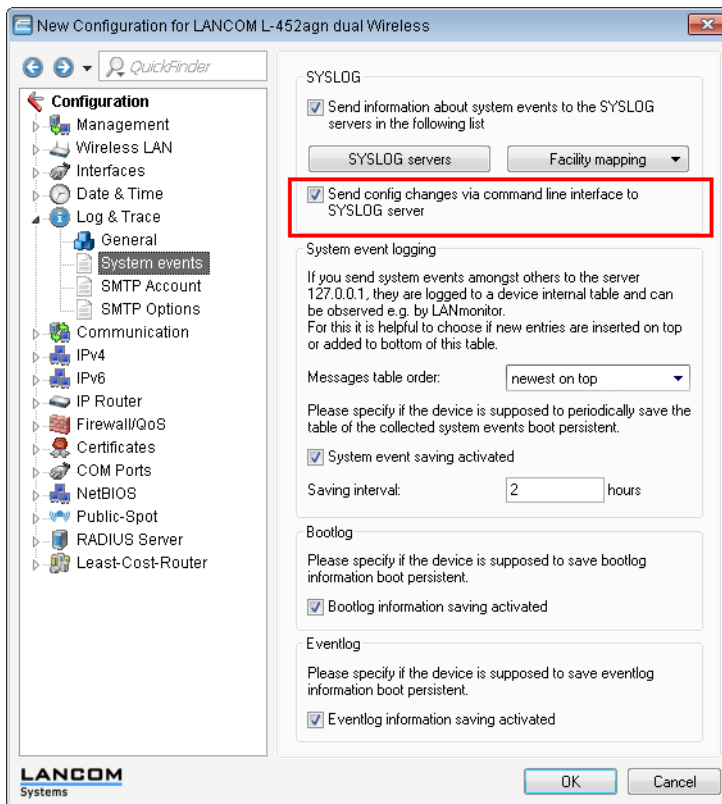
Default: No

9.3.2 Enhancements to LANconfig

Sending configuration changes made with the command line to the SYSLOG server

In LANconfig, the settings for logging configuration changes made via the CLI console are to be found under **Log & Trace > System events**.

 This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.



9.4 SYSLOG: Change to the default order

As of LCOS version 8.80, the SYSLOG table show the latest messages at the top by default. You can reverse the sorting order if you wish.

9.4.1 Additions to the Setup menu

Message table order

This item determines the order in which the messages table is displayed.

SNMP ID: 2.22.5

Telnet path: /Setup/SYSLOG

Possible values:

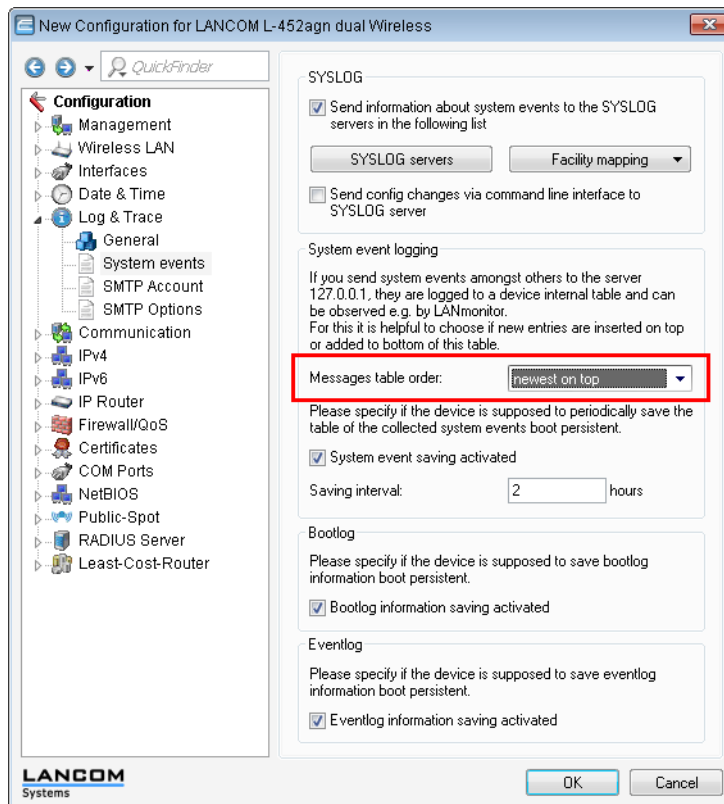
- Oldest on top
- Newest on top

Default: Newest-on-top

9.4.2 Enhancements to LANconfig

Order of the system events

In LANconfig, the settings for the order in which system events are displayed are to be found under **Log & Trace > System events**.



9.5 Packet capturing

In order to capture packets for the analysis of errors or problems, the command line tool **lcoscap** has been made available as of LCOS version 8.60. This command enables the capture of packets and writes the results to a file that you can open and analyze using a tool like Wireshark.

With LCOS version 8.80 an additional and more convenient method has been introduced: A new menu in WEBconfig allows you to set various parameters and capture data packets from selected interfaces, which can then be analyzed in a results file.

This method offers you several advantages:

- You do not need any special software, because you can run WEBconfig on any Web browser.
- There is no need to input any CLI commands. Instead, you work with a convenient menu.
- If you use WEBconfig over HTTPS, the confidentiality and security of captured traffic is guaranteed.

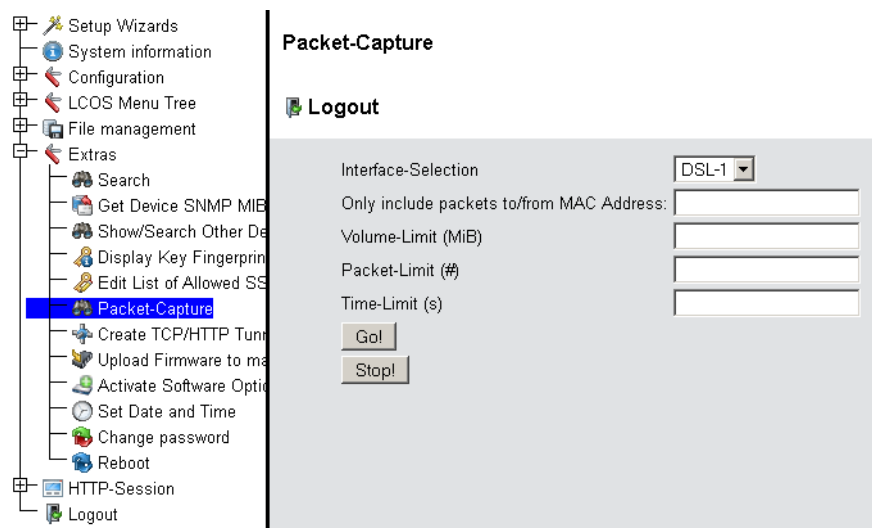
The new feature is to be found under **Extras > Packet capture**. After you set the parameters and click on **Go!** you create a file that you can save anywhere and open with Wireshark, for example.

9.5.1 Enhancements to WEBconfig

Packet capturing

The **Extras > Packet capture** function offers you a simple way to record data packets from different interfaces and then analyze them. Note that the possible settings can vary depending on the device type. You have more settings for WLAN devices than for devices without WLAN functionality.

The figure below shows the dialog for a WLAN device. In this case, there are two additional, WLAN-specific parameters.



To specify the output file the following general menu items are available:

- **Interface selection:** Use this drop-down menu to choose the interface that you want to record data packets for.
- **Only include packets to/from MAC address:** If you only want to record data packets for a particular physical address within the selected interface, you can specify it here.
- **Volume limit (MiB):** Enter the maximum volume of the recorded packages in Mebibytes.
- **Packet limit (#):** Here you can set the maximum number of packages to be recorded.
- **Time limit (s):** Enter the maximum time in seconds, after which the recording ends.

Click on **Go!** to start the recording process. After a certain period of time (depending on the connection speed), a window opens for you to save the generated files. You can now save the file locally with the suffix `.cap`. By default, the file name is composed of the description and interface associated with the device for which the data packets were recorded (e.g. `LCWLC-4025-LAN-2.cap`). You can change the name when saving or later.

You can stop a recording at any time by clicking on **Stop!**. This can be useful, for example, if you want to correct or customize the parameters that you already entered.

! If you start recording without setting any limits, the device keeps recording the packets until you manually stop the process by clicking on **Stop**.

9.6 Trace output for the XML interface

As of LCOS version 8.80, you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

This parametercauses the following message in the trace:
XML-Interface-PbSpot	Messages from the Public Spot XML interface

9.7 Ping command for IPv6

As of LCOS version 8.80, you can use the command `ping -6` (or the alias `ping6`) to send an ICMP ECHO_REQUEST to a host on an IPv6 network.

For IPv6, the scope of parameters is of central importance: IPv6 requires a link-local address (`fe80::/10`) to be assigned to every network interface (logical or physical) on which the IPv6 protocol is enabled, so you must specify the scope when pinging a link-local address. This is the only way that the ping command knows which interface it should send the package to. A percent sign (%) separates the name of the interface from the IPv6 address.

Examples:

`ping -6 fe80::1%INTRANET`

Pings the link-local address "fe80::1", which can be reached via the interface or network "INTRANET".

`ping -6 2001:db8::1`

Pings the global IPv6 address '2001:db8::1'.

The meaning of the optional parameters is explained in the following table:

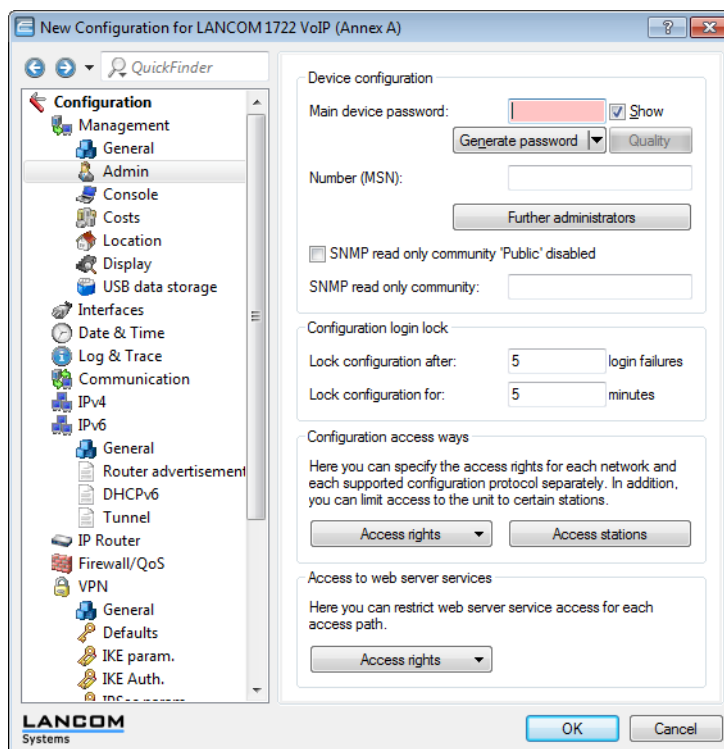
Parameters	Meaning
<code>-6 <IPv6 address>%<scope></code>	Performs a ping command to the link-local address via the interface specified by <code><scope></code> .

10 LCMS

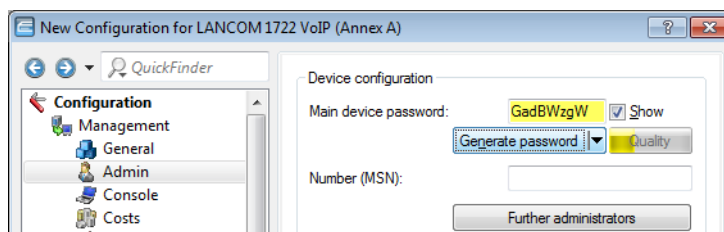
10.1 Enhancements to LANconfig

10.1.1 Creating a password in LANconfig

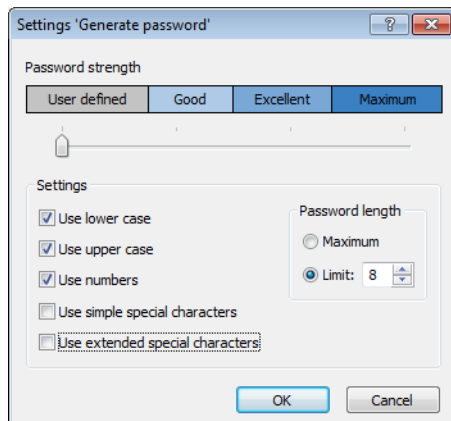
LANconfig provides the option to automatically generate a password at all points in the configuration, which require the input of a password or a passphrase.



Enable the option **Show** next to the box for entering the password. Then click on the button **Generate password** to create a password suggestion.




Optionally click the arrow next to the **Generate password** button to open the dialog box for the password policy settings.



Use the slider to set the desired password strength. With the **User defined** setting, you can define the maximum password length and the required character types. The settings **Good**, **Very good** and **Maximum** are predefined settings with reasonable, non-modifiable values.

After making your changes, click on the **Generate password** button again to create a new password proposal in line with your password guidelines.

 LANconfig stores the current settings in this dialog box for the current user.

10.1.2 Internal browser in LANconfig

Until now, LANconfig opened WEBconfig in the system's default browser. As of LCOS version 8.80, you have the option of starting LANconfig's own internal browser as an alternative.

Enhancements to LANconfig

LANconfig menu structure

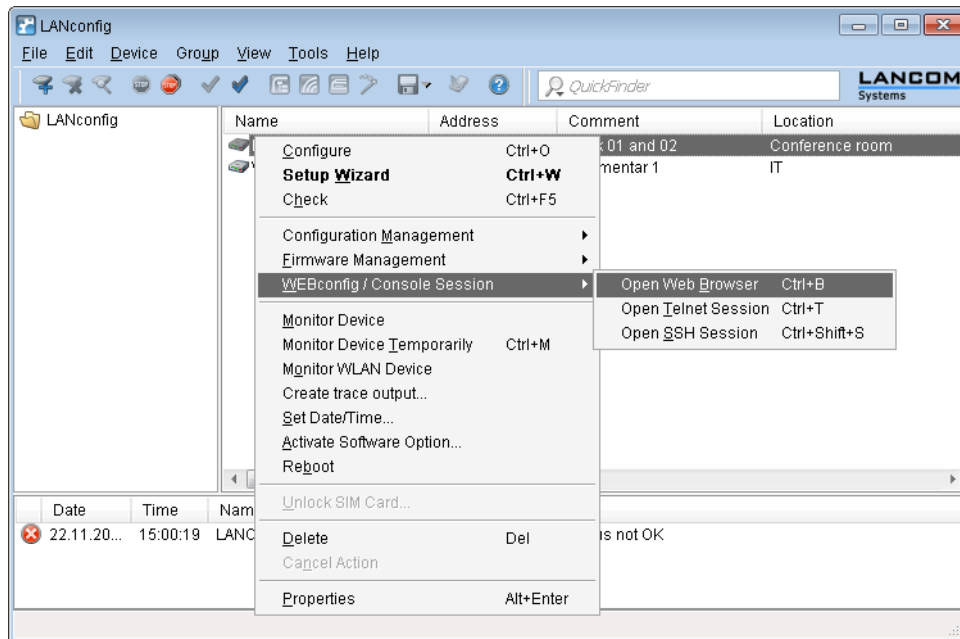
Using the menu bar, you can manage devices and their configurations, and you can customize the appearance and functioning of LANconfig.

Device

Under the menu item **Device** you can edit the configurations of devices connected to the network, organize firmware updates and monitor device connections.

The functions in the **Device** menu are only offered for selection if at least one device has been chosen from the list of devices. The menu can also be called by clicking on a device with the right mouse button when it is marked.

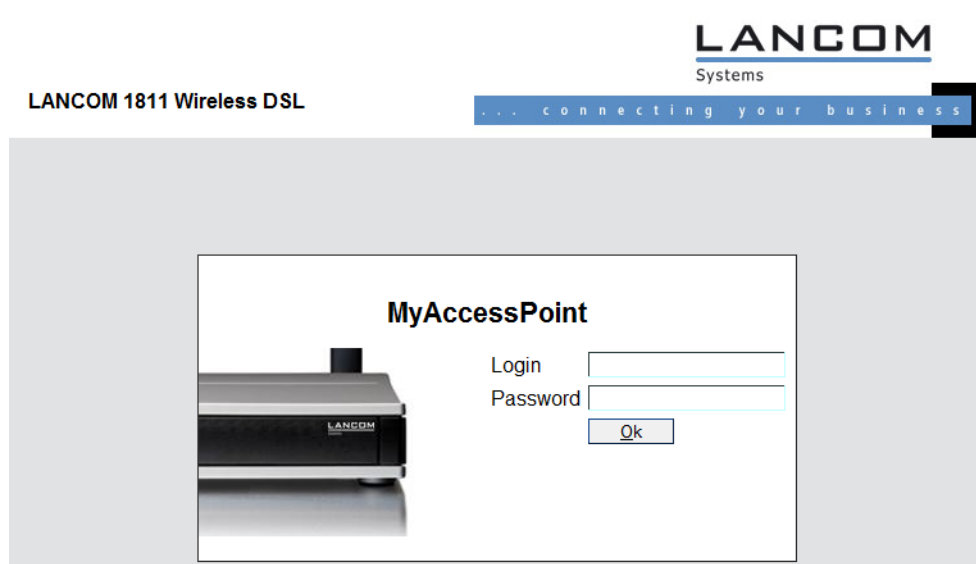
WEBconfig / console session



You can select the following actions under **Device > WEBconfig / console session**:

Open web browser

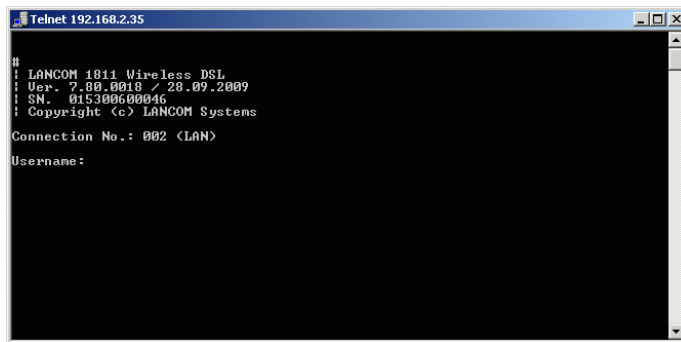
Opens the web browser for the device marked.



! Under **Tools > Options > Extras > Browser used to display WEBconfig**, you choose whether LANconfig should use the system default browser or its own internal browser.


Open Telnet session

Opens the telnet session.



Open SSH session

Opens a configuration session with an SSH client.

 For Telnet and SSH connections, you must specify the programs that LANconfig should use to connect to the device. Set these items under **Tools > Options > Extras > External programs**.

Extras

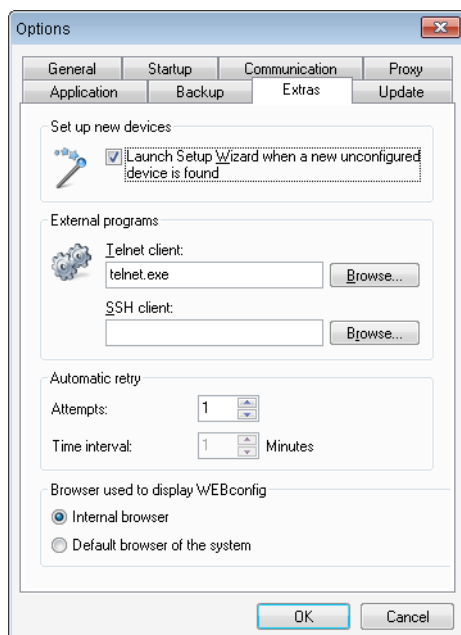
Clicking on **Tools > Options** opens up the dialog box for further optional settings. (You can also reach this dialog box by pressing F7).

Options

Under the menu item **Options** you can invoke additional functions, for example to communicate with connected devices, invoke external applications, or carry out automatic searches for firmware updates.

Extras

This dialog window allows you to make **additional settings**.



Set up new devices

If this option is checked, LANconfig launches the Setup Wizard whenever it finds an unconfigured device.

External programs

This item determines the executable files for the Telnet client and the SSH client to be used by LANconfig for connections to the devices.

Automatic retry**Attempts**

Specify the number of attempts for a firmware or configuration upload.

You can set a number between 1 and 9999. LANconfig always attempts to make a connection. If this fails a retry is attempted after the defined interval. The operation is retried until LANconfig reaches the number of defined attempts or until the operation succeeds. LANconfig may terminate the retries if a situation arises in which completion is unlikely without external intervention. This may be when the device cannot open a file, for example.

Time interval

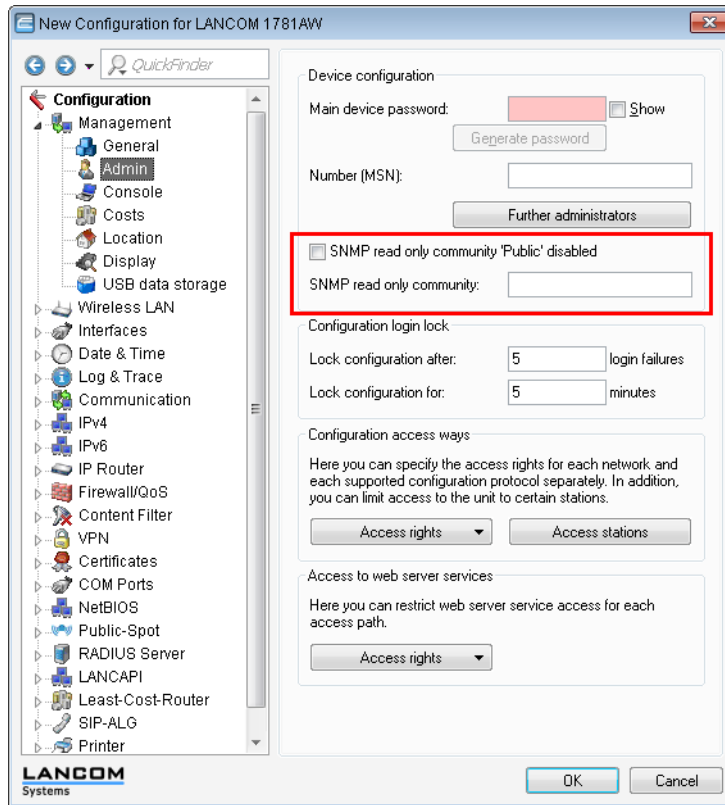
Enter the time interval in minutes between two attempts to upload the firmware or configuration. You can set an interval between 1 and 9999.

Browser used to display WEBconfig

This item sets the default browser used by LANconfig to display WEBconfig. You can choose between your operating system's default browser and LANconfig's internal browser, LCCEF (LANCOM Chromium Embedded Framework).

10.2 Setting the SNMP read-only community 'Public'

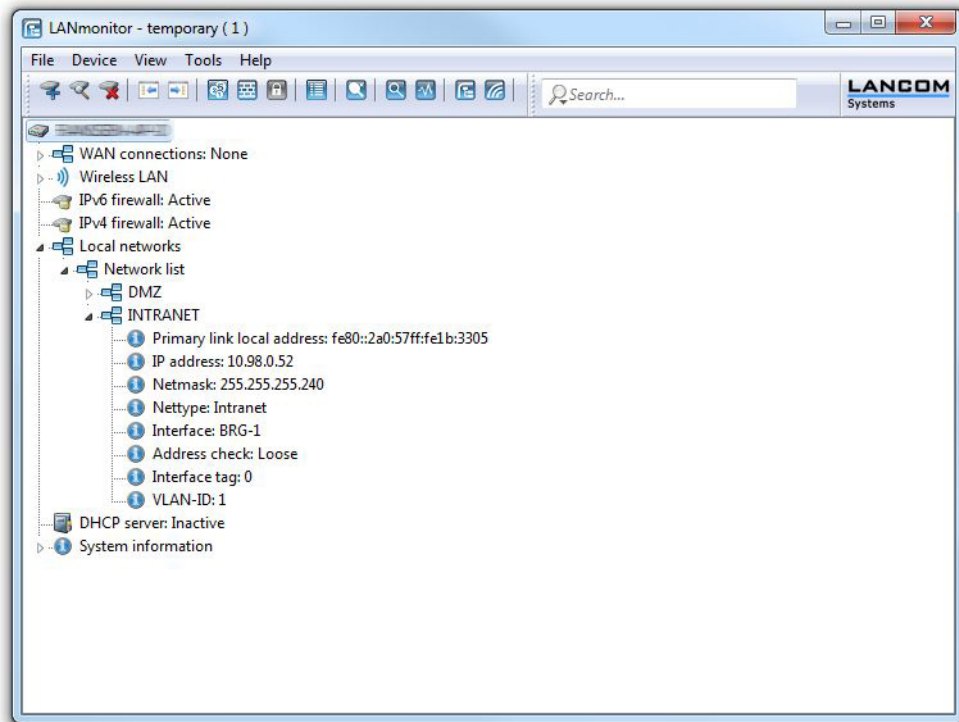
In LANconfig, the setting for the SNMP read-only community 'Public' is to be found under **Management > Admin**.



10.3 Enhancements to LANmonitor

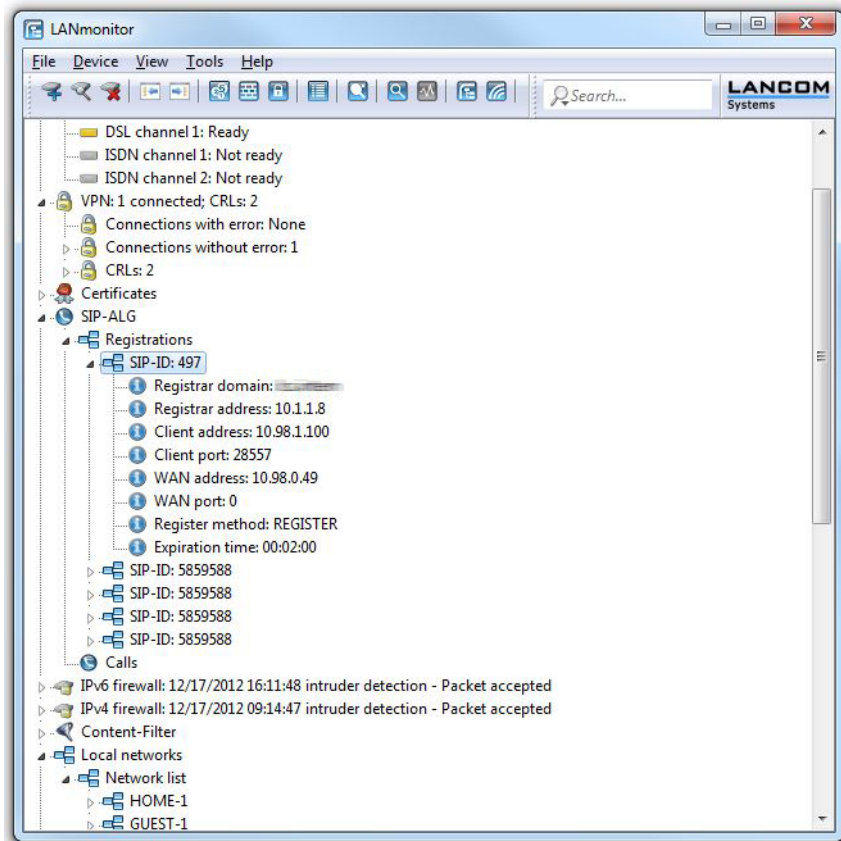
10.3.1 Display local IPv6 addresses

As of LCOS version 8.80, LANmonitor can display the IPv6 addresses of local networks. This display function is available in various places within the menu.



10.3.2 Displaying PBX lines in the SIP ALG

As of LCOS version 8.80, LANmonitor displays the PBX lines separately with the registration method **Options** in the section **SIP ALG > Registrations**.



10.3.3 Displaying the active Ethernet ports

As of LCOS version 8.80, LANmonitor allows you to display the operating status of the Ethernet ports.

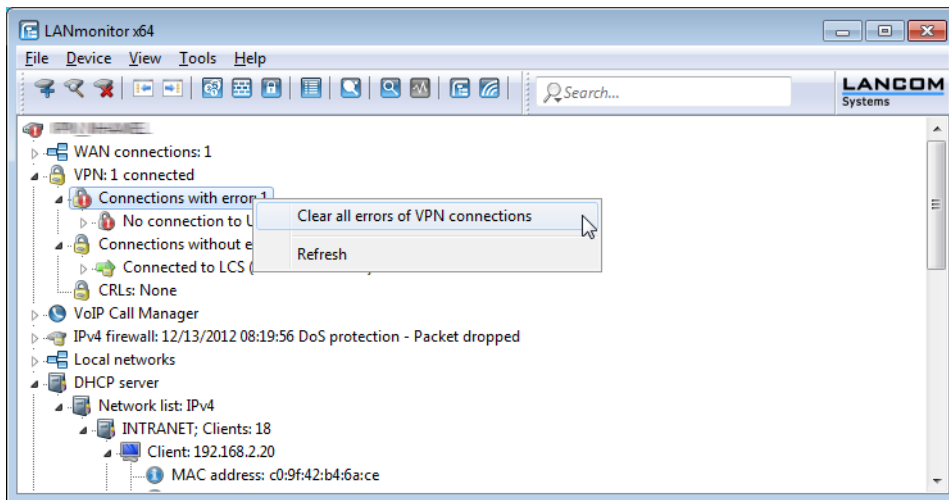
The menu item **System information > Interfaces > Ethernet ports** shows whether ports are in operation and, if so, which network the port is assigned to (e.g. LAN-1 after the port name).



10.3.4 Delete all VPN connection failures

As of LCOS version 8.80, LANmonitor gives you the option of deleting all of the VPN connection errors with just one click.

To do this, navigate to the area of LANmonitor for VPN connections, right-click on the entry **Connections with error: x** and select **Clear all VPN connection errors**.



10.3.5 Display of the GPS time

As of LCOS version 8.80, LANmonitor gives you the option to display the time received from the GPS network. Navigate to the **GPS** section for the device in LANmonitor. The current GPS time is displayed under **Timestamp**.



11 Virtual Private Networks - VPN

11.1 Deleting all VPN errors with one command

As of LCOS 8.80, you have the ability to delete all of the VPN errors in a device with a single command.

11.1.1 Additions to the menu system

Additions to the Status menu

Delete conn errors

This action deletes all VPN connection failures in the device, i.e. all entries in the VPN connections list (**VPN > Connections > Status**) containing an error in the **Last error** column.

SNMP ID:

1.26.38

Telnet path:

Status > VPN

11.2 Default proposals for IKE and IPSec

The proposals for IKE and IPSec now support a key length of 256 bits in the default settings.



A firmware upgrade initially does not enable this change, so avoiding any problems for existing installations. To accept the changes, you must perform a reset of the device or reset the tables. For new devices with LCOS 8.62 or later, the new defaults are already active.

11.3 Selecting DH group 14 for VPN connections

The IKE and PFS group for VPN connections now support the DH group 14 with a key length of 2048.

11.3.1 Additions to the Setup menu

VPN

This menu contains the configuration of the Virtual Private Network (VPN).

SNMP ID: 2.19

Telnet path: /Setup

Aggressive mode IKE group default

This IKE group is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID: 2.19.11

Telnet path: /Setup/VPN

Possible values:

- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

Main mode IKE group default

This IKE group is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID: 2.19.14

Telnet path: /Setup/VPN

Possible values:

- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

Quick mode PFS group default

This IPSec group is used for simplified dial-in with certificates.

SNMP ID: 2.19.20

Telnet path: /Setup/VPN

Possible values:

- 0: No PFS
- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

Layer

Define other parameters for the individual VPN connections here.

SNMP ID: 2.19.7

Telnet path: /Setup/VPN

PFS group

Perfect Forward Secrecy (PFS) is a security feature of encryption algorithms. The PFS group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID: 2.19.7.3

Telnet path: /Setup/VPN/Layer

Possible values:

- 0: No PFS
- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

IKE group

The IKE group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID: 2.19.7.4

Telnet path: /Setup/VPN/Layer

Possible values:

- 1: MODP-768
- 2: MODP-1024
- 5: MODP-1536
- 14: MODP-2048

Default: MODP-1024

11.4 Replay detection

Replay detection is a feature of the IPSec standard for the detection of so-called replay attacks. In a replay attack, an unauthorized station logs data and sends this, either repeatedly or with a delay, to a remote site to simulate a different identity.

Replay detection defines a certain number of consecutive packets (a "window" with the length of "n"). Because the IPSec standard provides the packages with a continuous sequence number, the receiving VPN device can determine whether a packet contains a sequence number from the permitted window. If, for example, the current highest received sequence number is 10,000 and the window width is 100, then a sequence number of 9,888 is outside the permitted window.

Replay detection discards received packets if:

- they contain a sequence number before the current window, in which case they are seen as being too old, or if
- they contain a sequence number which has already been received by the VPN device, in which case replay detection evaluates this package as part of a replay attack

Please consider the following aspects when configuring the replay-detection window:

- If you select too large a window, then replay detection may overlook a replay attack
- If you make the window too small, replay detection may drop legitimate packets that became reordered during data transfer, so generating errors on the VPN connection

 You have to weigh-up the application of replay detection for your particular case. Only activate replay detection if the security of the VPN connection is more important to you than interference-free data transfer.

11.4.1 Additions to the menu system

Anti-replay window size

Used for detecting replay attacks, this parameter defines the size of the window (i.e. number of packets) within which a VPN device considers the sequential number of the received packets to be up-to-date. The VPN device drops packets that have a sequence number older than or duplicated within this window.

SNMP ID:

2.19.30

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

Max. 5 numbers

Default:

0

Special values:

A value of 0 disables replay detection.

11.5 myVPN



The LANCOM myVPN app offers you a very easy way to set up a VPN connection to your company network from your iPhone, iPad or iPod (or from any iOS device in general). The LANCOM myVPN app offers the following functions:

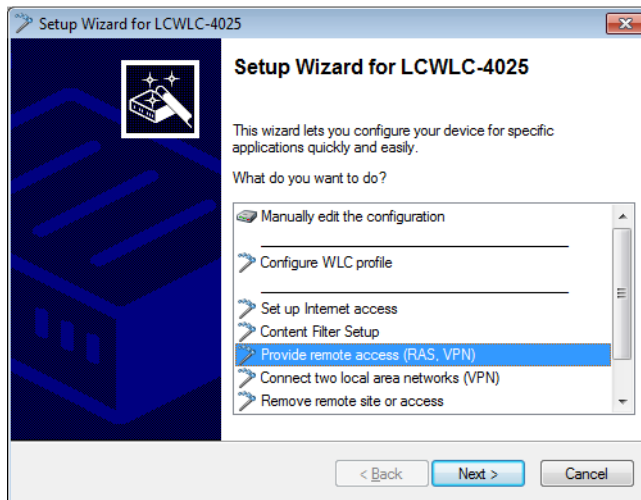
- Highly secure, mobile VPN connections
- Handles the complex VPN configuration of the VPN client integrated into iOS devices and of the LANCOM router
- PIN-protected authentication for VPN tunnel creation
- Access control with configurable firewall rules on the LANCOM VPN gateway
- LANCOM myVPN user management and automatic detection of myVPN-enabled LANCOM gateways
- For version 4.1 iOS devices and later

After its installation, the LANCOM myVPN app retrieves a VPN profile from your LANCOM VPN device and automatically configures all of the necessary settings on the iOS device. You can then use the internal features of the iOS to establish a VPN connection to your company network in just a few steps.

11.5 Using the Setup Wizard in LANconfig to set up a VPN profile for the LANCOM myVPN app

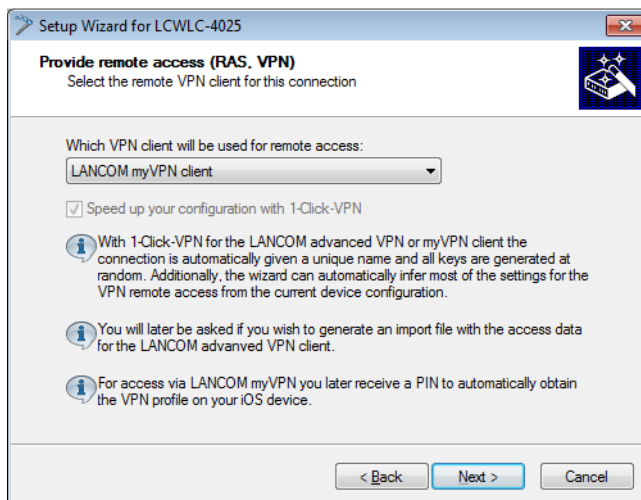
This is how to use the Setup Wizard to provide an access account for a VPN client on an iOS device:

1. Start LANconfig, for example from the Windows start menu with **Start > Programs > LANCOM > LANconfig**. LANconfig now automatically searches the local network for devices.
2. Choose the required device from the selection window in LANconfig and select the **Setup Wizard** button or use the menu under **Tools > Setup Wizard**.
3. Select the item **Provide remote access (RAS, VPN)** and then click on **Next**.

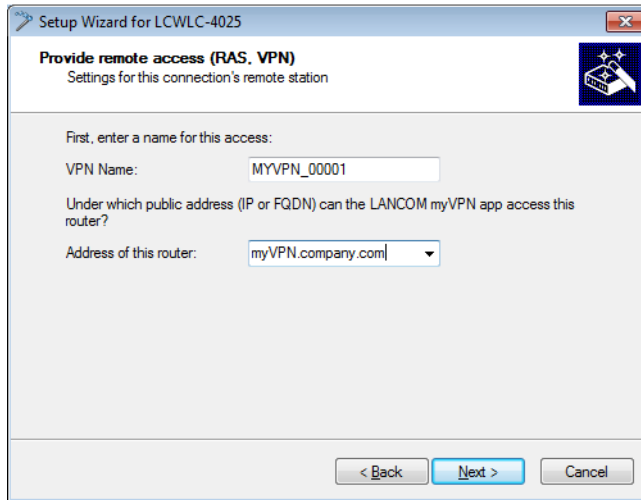


You can skip the following information dialog with **Next**.

4. From the drop-down list select the option **LANCOM myVPN client** and click on **Next**.

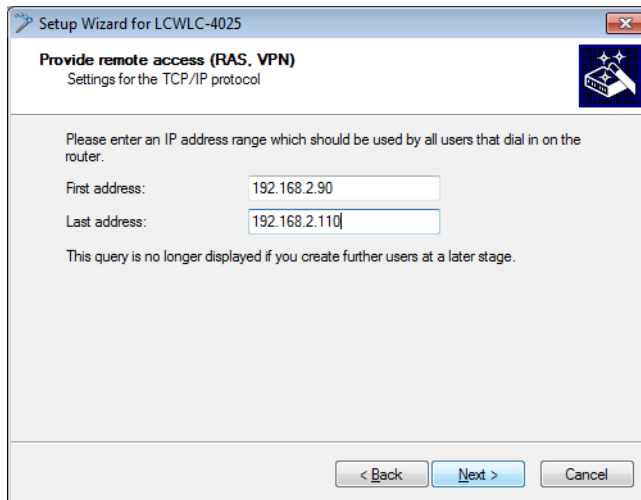


5. Enter a name for this access account and select the address at which the VPN client on the iOS device can reach the router from the Internet. To continue, click on **Next**.



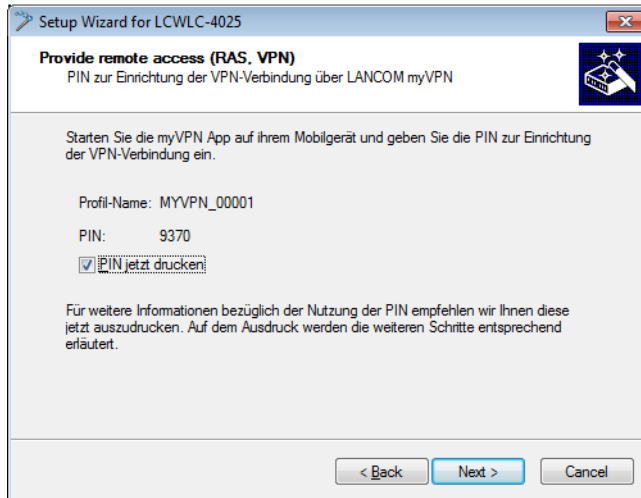
The Setup Wizard will suggest a name that you can accept if you wish.

6. If you have not yet configured a pool for allocating IP addresses to the connecting VPN devices, the wizard will prompt you the first time to specify a range of IP addresses for the pool in the following dialog. When connecting, the VPN device automatically assigns a free IP address to the iOS device from this pool.



- ⓘ If you have already configured a pool for allocating IP addresses to the connecting VPN devices, the VPN device automatically uses an address from the address pool, and the wizard skips the dialog shown here.

7. The Setup Wizard displays the profile name and the PIN that was auto-generated for the VPN client. If you want to print out the PIN now, select the option **Print PIN now**. Click on **Next**.



8. By clicking on **Finish** the Setup Wizard stores all the settings on the corresponding VPN device. If applicable, it then starts printing out the myVPN PIN.
The myVPN module now enabled on the selected VPN device. On your iOS device, you can now start the myVPN app and enter the PIN to retrieve the VPN profile.

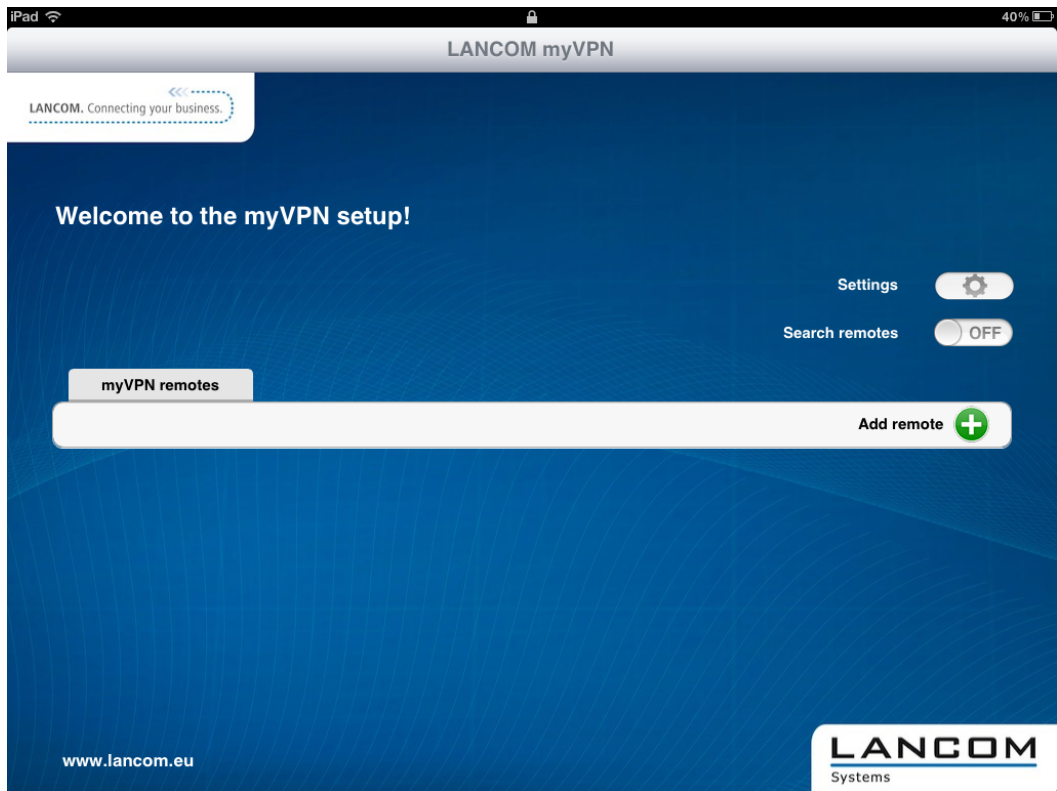
11.5 Retrieve the VPN profile with the LANCOM myVPN app

This is how you can use the LANCOM myVPN app on your iOS device to retrieve a VPN profile from a LANCOM VPN device:

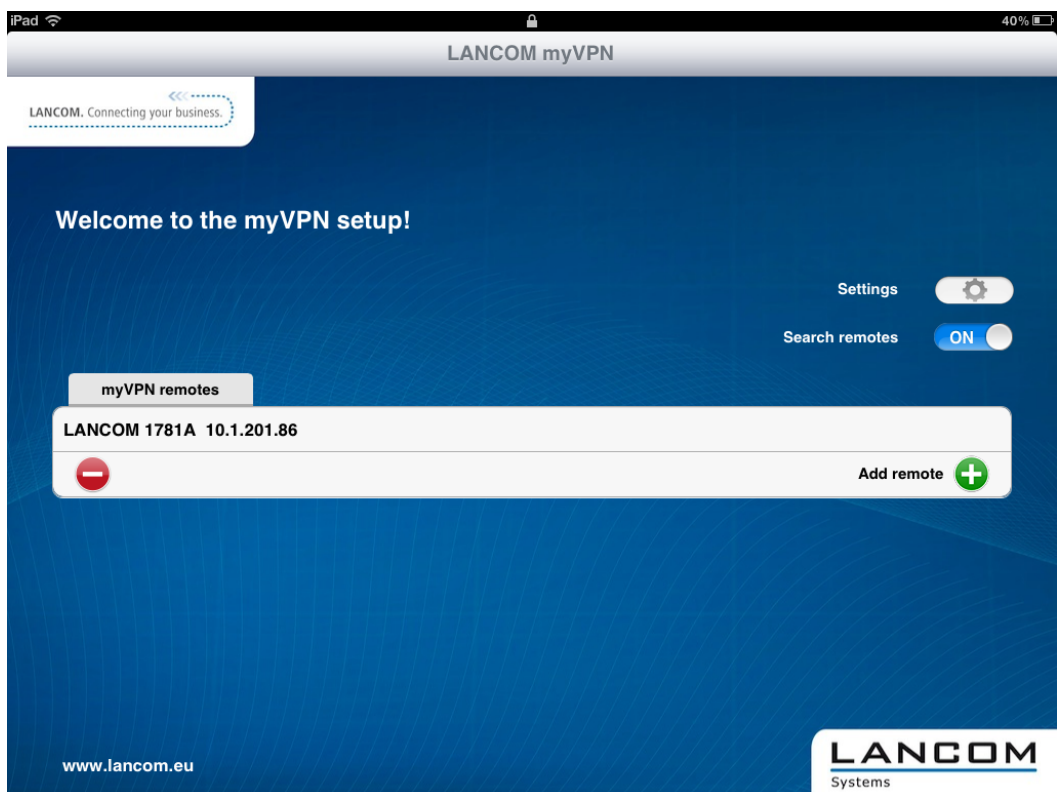
- ! The purpose of the LANCOM myVPN app is to set up the VPN client on iOS devices with the correct parameters and in a quick and easy fashion. The establishment of the VPN connection to the company network itself is handled directly by the VPN client in the iOS device.

1. Download the LANCOM myVPN app from the Apple App Store.

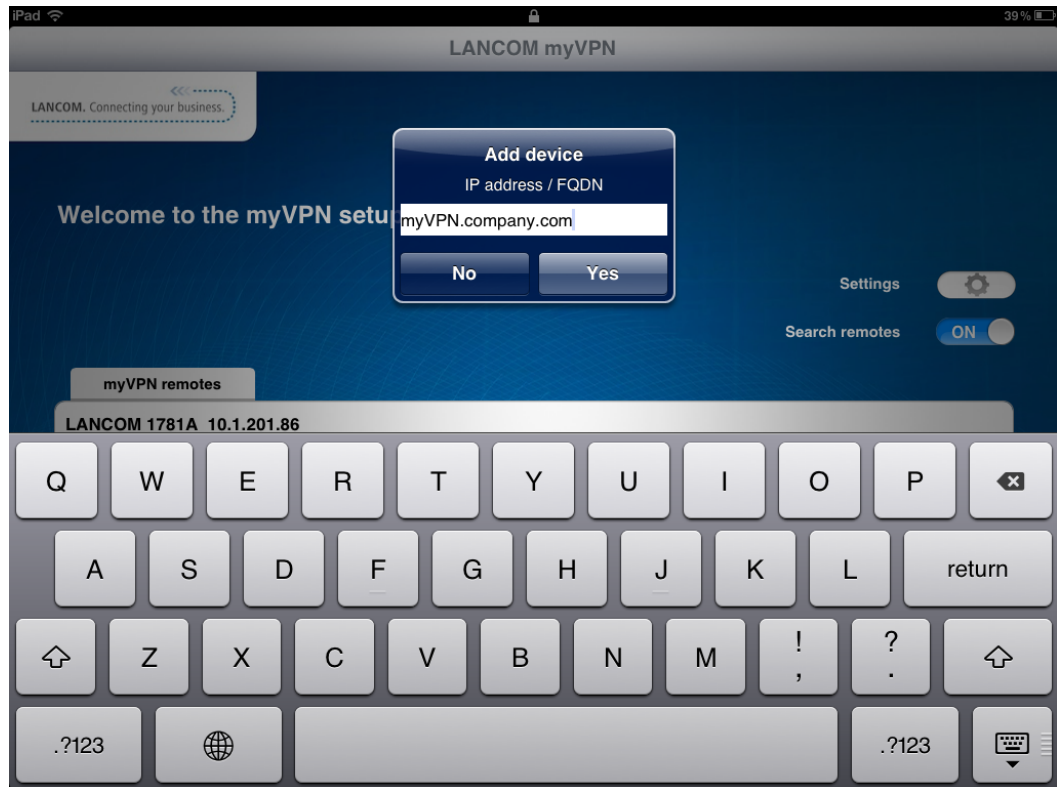
2. Open the app on your iPhone or iPad.



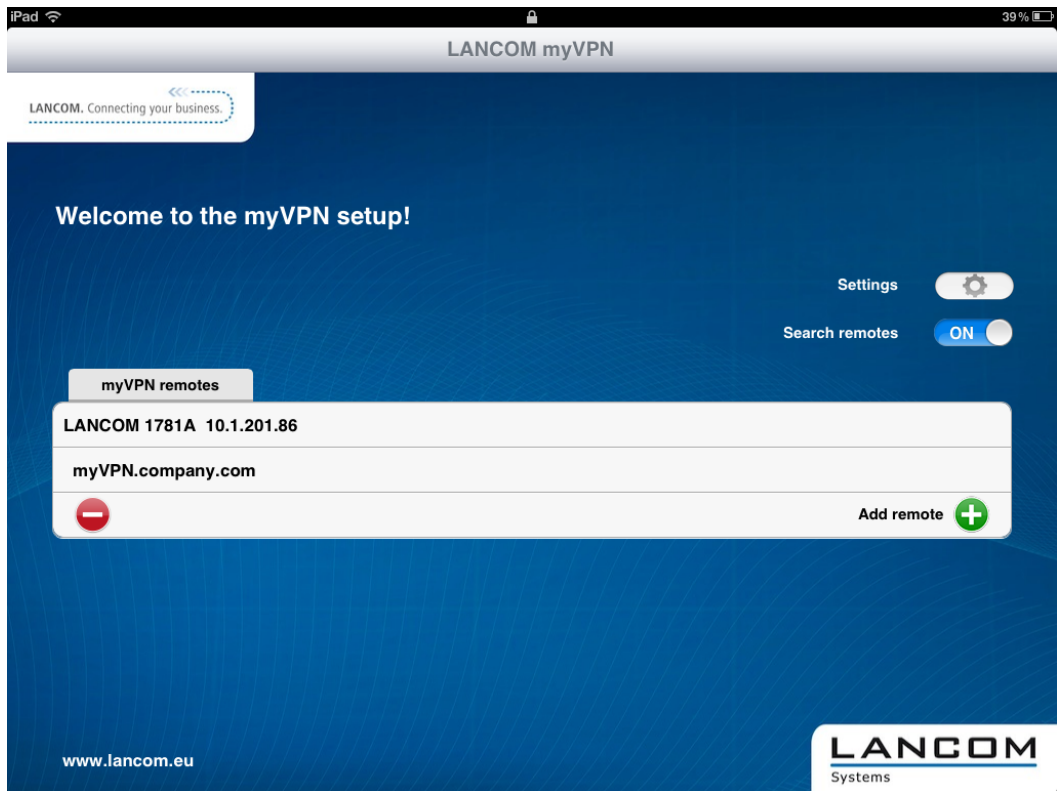
3. Optional: Enable the option **Automatic search** to find VPN devices with an activated LANCOM myVPN module, which are available to iOS devices via WLAN.



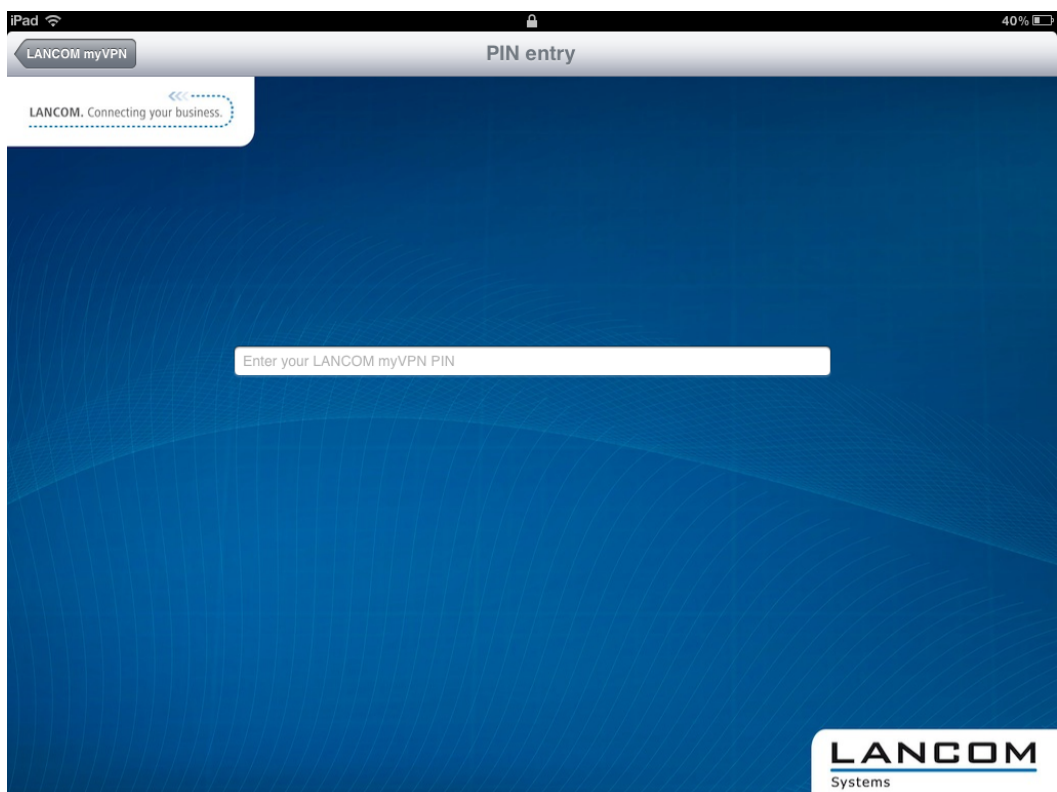
- ! The iOS device now lists all VPN devices which are accessible via WLAN and which have an active LANCOM myVPN module. However, the inclusion of an entry in this list does not necessarily mean that your iOS device can retrieve a LANCOM myVPN profile from this VPN device.
4. Optional: Select the option **Add device manually** to enter the IP address or name of VPN devices that the iOS device can access via an Internet connection (3G or WLAN). In the dialog that follows, enter the IP address or the name of the VPN device and confirm with **Yes**.



- The app now displays all VPN devices that offer profiles for the LANCOM myVPN app.



- Tap on the entry in the list to select the desired VPN device and then enter the PIN required for retrieving the VPN profile.

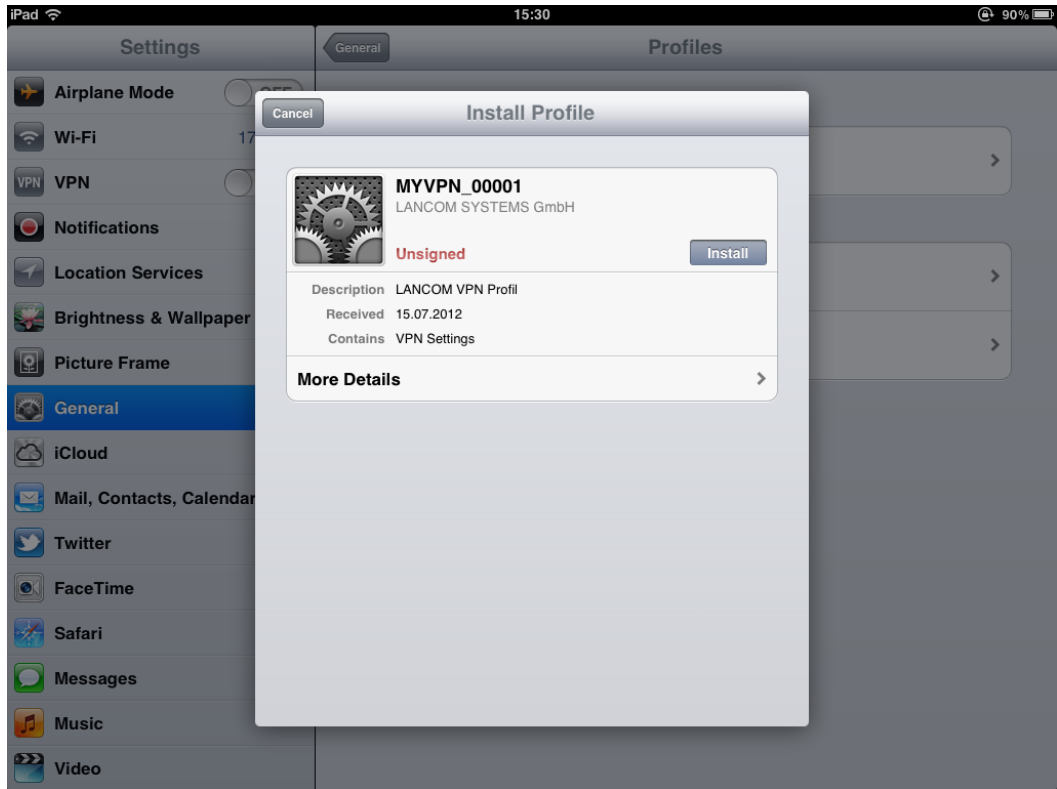


- ⓘ If you enter your PIN incorrectly 5 times, the myVPN module on the LANCOM VPN device will be completely locked for a specific time period. In this state, VPN connections remain possible for iOS devices that previously set up their VPN access accounts successfully. However, iOS devices cannot retrieve myVPN profiles from this VPN device so long as the lock is in place. An administrator can re-enable the myVPN module.

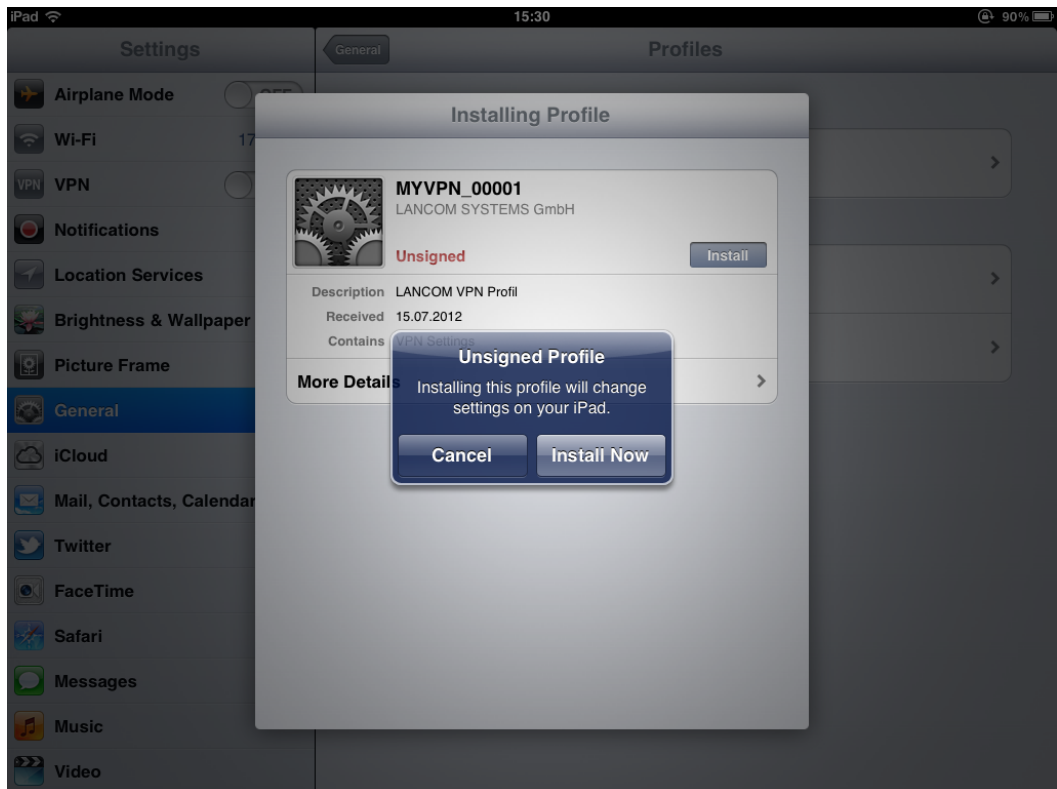
7. If the following dialog contains a notice about an unsigned certificate, simply confirm it with **Yes**.



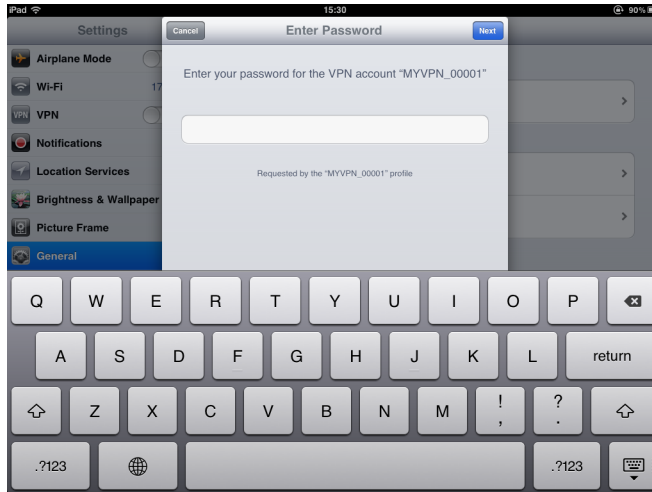
8. In the next dialog, confirm the request to install the profile with the **Install** button.



Confirm the necessary changes to the settings on your iOS device.

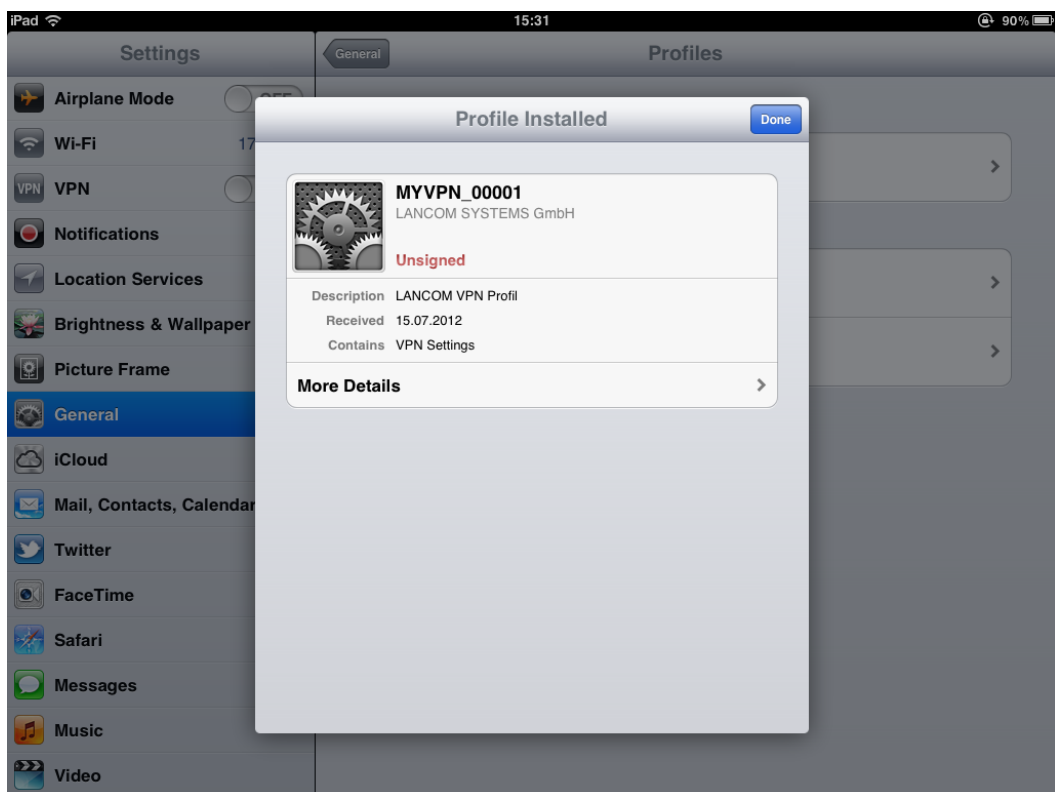


9. The next step of the installation routine is to enter the password for the VPN access account. By default, the VPN password is the PIN for the myVPN profile. If you enter the password for the VPN access account here, the iOS device can establish a VPN connection to your company network without requesting a password. If you leave the box for the VPN password empty, you will be asked for the VPN password every time you connect using the iOS device. Confirm your selection with the **Next** button.

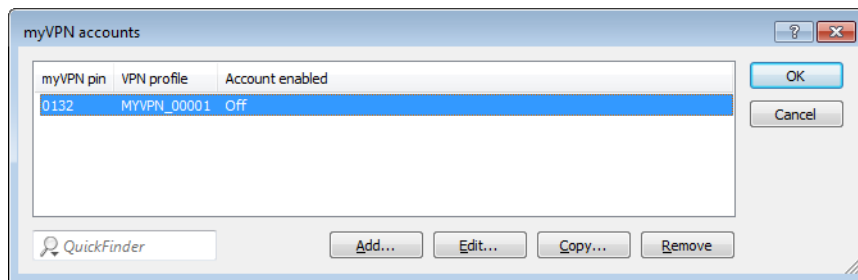


- ! For security reasons we recommend that you do **not** save the VPN access password on the device, but that you enter it each time you wish to connect.

10. The VPN profile is now fully installed on your iOS device and is ready for setting up a VPN connection to your company network. Confirm that the installation has been concluded by clicking on the **Complete** button.



Once installed on an iOS device, the LANCOM VPN device disables the installation routine for this myVPN profile. You can check your status with LANconfig by navigating to the configuration area **VPN > myVPN** and viewing the **myVPN accounts** list:

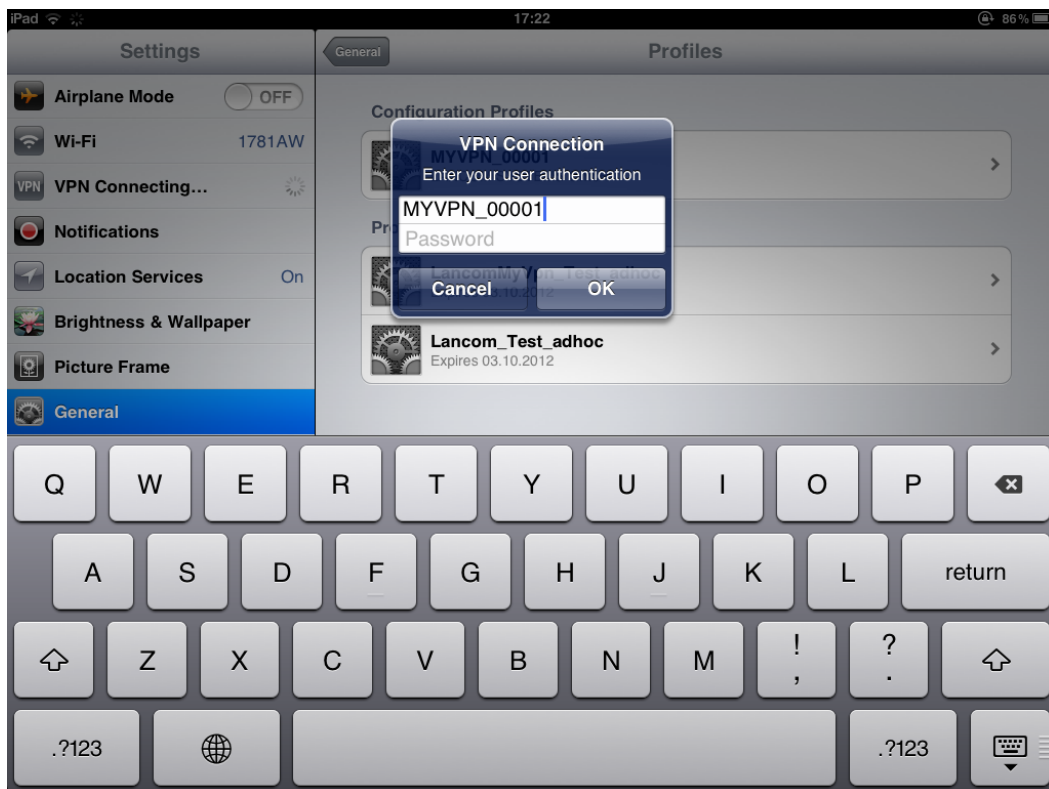


! By disabling the myVPN profile, other IOS device are prevented from installing the same myVPN profile and thus using the same VPN access credentials. However, disabling the myVPN profile has no effect on the VPN connection itself.

11.5 Opening and closing the VPN connection on the iOS device

After you have installed the VPN profile on your iOS device with the LANCOM myVPN app, you open and close the VPN connection to your company network as follows:

1. Enable the VPN tunnel in the configuration area **Settings** under the option **VPN**.
2. The following dialog already displays the user name from the myVPN profile. Enter the password for the VPN connection and confirm with **OK**.



! By default, the password for the VPN connection is the PIN for the myVPN profile.

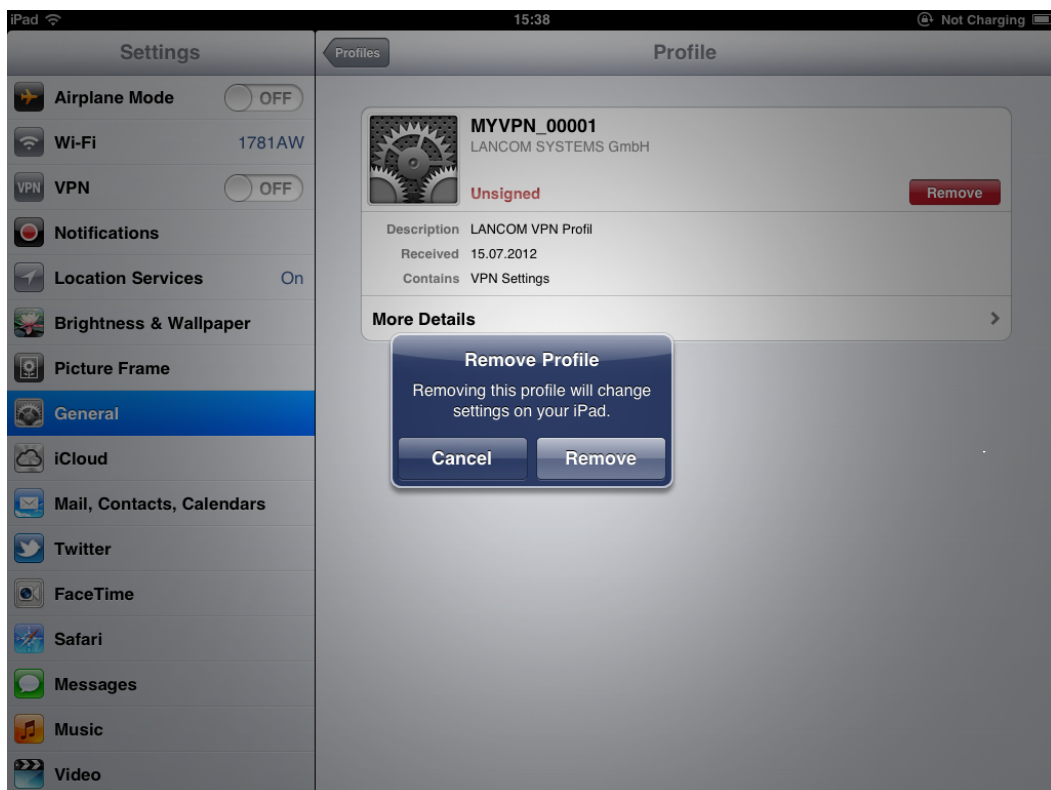
! The password does not have to be entered if you entered it while installing the myVPN profile for the VPN connection. In this case, this window is not displayed, and the connection will be established immediately.

3. Close the VPN connection on your iOS device in the configuration area **Settings** under the option **VPN**.

11.5 Deleting a VPN profile from the iOS device

To delete the VPN profile from your iOS device:

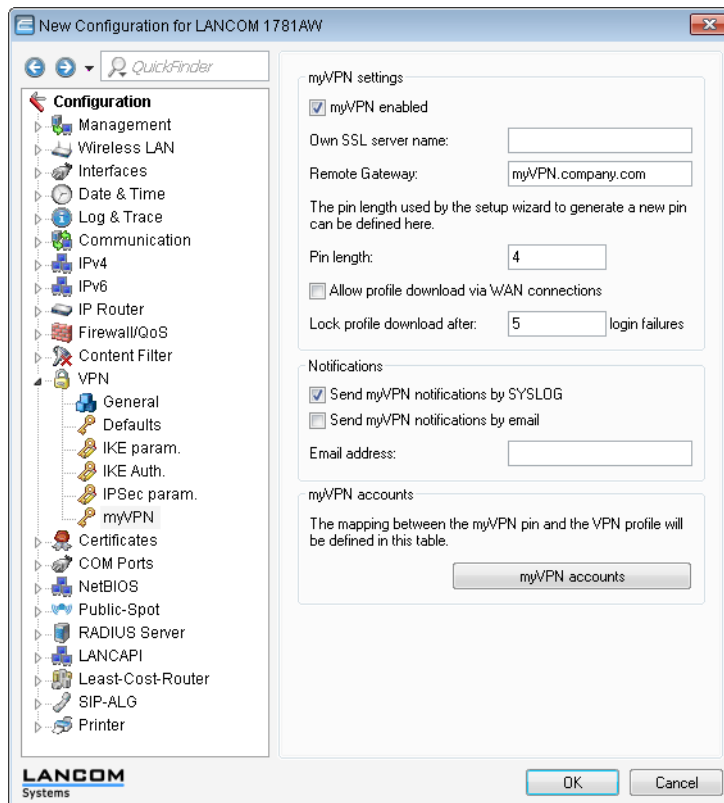
1. Navigate to **Settings > General > Profiles** to the list of available profiles on your iOS device.
2. Select the profile, click on **Delete** and confirm the action again in the next dialog with **Delete**.



11.5.1 Enhancements to LANconfig

Configuring the LANCOM myVPN app

Under **VPN > myVPN** you can manually adjust the settings for the LANCOM myVPN app.



Check the **myVPN enabled** box to allow the LANCOM myVPN app to load a VPN profile.

Specify the **Device name** here if a trusted SSL certificate is installed on this device. This ensures that the IOS device does not issue a warning about an untrusted certificate when the profile is retrieved.

Use the field **Remote gateway** to enter the WAN address of the router or its name as resolved by public DNS servers. If not found automatically, enter the remote gateway into the LANCOM myVPN app.

Specify the **PIN length** to be used by the setup wizard for generating new PINs (default = 4).

You can allow or prevent the **profile download via WAN connections**.

You can limit the number of login failures accepted by the myVPN app in the field **Lock profile download after**.

Activate the option **Send myVPN notifications by SYSLOG** to send messages about the myVPN app to SYSLOG.

Activate the option **Send myVPN notifications by e-mail** to send messages about the myVPN app to a specified e-mail address.

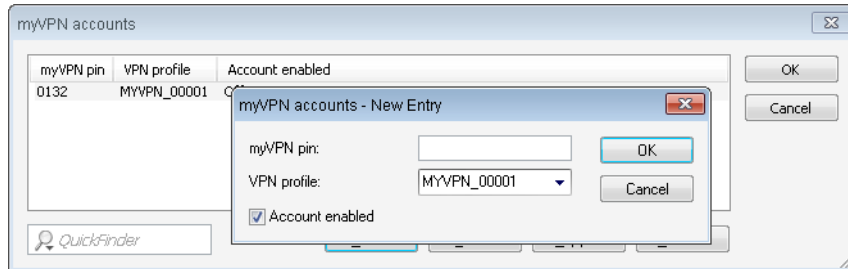
These messages include:

- Successful profile retrieval
- Disabled login for LANCOM myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

Specify the **E-mail address** to which messages about the LANCOM myVPN app are to be sent.

! E-mail must be configured on the VPN device.

The item **myVPN accounts** is used to assign the myVPN PIN to the VPN profiles.



Here you determine which **VPN profile** is to supply data to the myVPN app upon retrieval of the profile.

You set the myVPN PIN that is to be entered when the LANCOM myVPN app is to retrieve the profile.

! **Security notice:** As a security feature of myVPN, the repeated incorrect entry of a PIN causes the device to temporarily disable profile retrieval, and a notification is sent by SYSLOG and by e-mail. After three failed attempts, the device disables profile retrieval for 15 minutes. After five further failed attempts, profile retrieval is disabled for a day. In case of further failed attempts, the time periods vary. Manually releasing this lock resets the corresponding counter. Please also be aware that an attempt to retrieve the profile while access is deactivated (e. g. when the profile has previously been retrieved successfully) is also considered by the device to be a failed attempt.

You activate the profile by checking the **Account enabled** box.

! After the profile has been retrieved successfully, the device automatically disables the corresponding profile to avoid the repeated download by another device.

Once you save these settings to the device, the myVPN module is active on the selected VPN device. On your iOS device, you can now start the LANCOM myVPN app and enter the PIN to retrieve the VPN profile.

11.5.2 Additions to the menu system

myVPN

The "myVPN" function is used by devices with the iOS operating system to automatically retrieve VPN profiles and take over the configuration of the internal VPN client. You configure the VPN profile and the parameters for myVPN on the router. With the aid of the LANCOM myVPN app and a suitable PIN, you can configure your device for VPN connection in just a few easy steps.

More information on the myVPN app is available on the [LANCOM homepage](#).

SNMP ID:

2.19.28

Telnet path:

Telnet path: Setup > Vpn > myVPN

Operating

Use this switch to activate myVPN for this device.

SNMP ID:

2.19.28.1

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

Yes

No

Default:

No

PIN length

This item sets the length of new PINs generated by the setup wizard.

SNMP ID:

2.19.28.2

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

Maximum length: 12

Minimum length: 4

Default:

4

Device hostname

Enter the device name here if a trustworthy SSL certificate is installed on this device. This ensures that the IOS device does not issue a warning about an untrusted certificate when the profile is retrieved.

SNMP ID:

2.19.28.3

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

Max. 31 characters from

0-9

a-z

A-Z

#@[{}~!\$%&'()*+,-./:;<=>?[\^ _ `

Default:

Blank

Mapping

This table assigns the myVPN PIN to the VPN profiles.

SNMP ID:

2.19.28.4

Telnet path:

Telnet path:Setup > Vpn > myVPN

PIN

This is where you can store the PIN for retrieving the myVPN app profile.

The myVPN setup wizard also uses this PIN in the PPP list for the actual VPN login. If you change your PIN here, you must also change it in LANconfig under **Communication > Protocols > PPP-list** if you wish to avoid having a different PIN.



Security notice: As a security feature of myVPN, the repeated incorrect entry of a PIN causes the device to temporarily disable profile retrieval, and a notification is sent by SYSLOG and by e-mail. After three failed attempts, the device disables profile retrieval for 15 minutes. After three further failed attempts the device disables profile retrieval for 24 hours. In case of further failed attempts, the time periods vary. Manually releasing this lock resets the corresponding counter. Please also be aware that an attempt to retrieve the profile while access is deactivated (e. g. when the profile has previously been retrieved successfully) is also considered by the device to be a failed attempt.

SNMP ID:

2.19.28.4.1

Telnet path:

Telnet path:Setup > Vpn > myVPN > Mapping

Possible values:

Max. 12 digits from 1234567890

Default:

Blank

VPN profile

This setting determines which VPN profile the myVPN app should retrieve.

SNMP ID:

2.19.28.4.2

Telnet path:

Telnet path:Setup > Vpn > myVPN > Mapping

Possible values:

16 characters from

0-9

a-z

A-Z

@{ } ~ ! \$ % & ' () + , ; < = > ? [\] ^ _ .

Default:

Blank

Operating

This switch activates the profile retrieval by means of the myVPN app. After the profile has been retrieved successfully, the device automatically disables the corresponding profile to avoid the repeated download by another device.

SNMP ID:

2.19.28.4.3

Telnet path:**Telnet path: Setup > Vpn > myVPN > Mapping****Possible values:**

No

Yes

Default:

No

Re-enable login

The command `do re-enable-login` releases the lock that was caused by failed attempts. If required, this generates a message about the re-enabling via SYSLOG or e-mail.

SNMP ID:

2.19.28.5

Telnet path:**Telnet path: Setup > Vpn > myVPN****E-mail notification**

Enable this option to send messages about the myVPN app to a specific e-mail address. These messages include:

- Successful profile retrieval
- Disabled login for myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

SNMP ID:

2.19.28.6

Telnet path:**Telnet path: Setup > Vpn > myVPN****Possible values:**

No

Yes

Default:

No

E-mail address

Specify the e-mail address to which messages about the myVPN app are to be sent.

SNMP ID:

2.19.28.7

Telnet path:**Telnet path: Setup > Vpn > myVPN****Possible values:**

Max. 63 characters from

0-9

a-z

A-Z

@[!~!\$%&'()+-./:;<=>?[\]^_`

Default:

Blank

Syslog

Enable this option to send messages about the myVPN app to SYSLOG. These messages include:

- Successful profile retrieval
- Disabled login for myVPN due to too many failed attempts
- Re-enabling of the login (irrespective of whether this is done manually or if the specified time period has expired)

SNMP ID:

2.19.28.8

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

No

Yes

Default:

No

Remote gateway

Here you enter the WAN address of the router or its name as resolved by public DNS servers. If the myVPN app cannot find the remote gateway by means of automatic search, you should enter the gateway into the app as well.

SNMP ID:

2.19.28.9

Telnet path:

Telnet path:Setup > Vpn > myVPN

Possible values:

Max. 63 characters from

0-9

a-z

A-Z

#@[!~!\$%&'()+-./:;<=>?[\]^_`

Default:

Blank

Error count for login block

This parameter limits the number of failed logins for the myVPN application.

If the user exceeds the maximum number of failed attempts, the device will lock access for 15 minutes the first time, and for 24 hours the second time.

The console command `Re-enable-login` removes these blocks (see [Re-enable login](#)).

SNMP ID:

2.19.28.10

Telnet path:

Setup > Vpn > myVPN

Possible values:

5-30

Default:

5

Allow access from WAN

This parameter allows or prevents the user from downloading myVPN profiles from the WAN.

SNMP ID:

2.19.28.11

Telnet path:

Setup > Vpn > myVPN

Possible values:

Yes

No

Default:

Yes

12 Voice over IP - VoIP

12.1 Default setting for WAN registration of a SIP user

The default setting for the WAN registration of a SIP user has changed from 'yes' to 'no'.

12.1.1 Additions to the menu system

Access from WAN

This item determines whether and how SIP clients can register via a WAN connection.

SNMP ID:

2.33.3.1.1.8

Telnet path:

Setup > Voice-Call-Manager > Users > SIP-User > Users

Possible values:

Yes

No

VPN

Default:

No

13 LANCOM Content Filter

13.1 Concurrent user model in the content filter

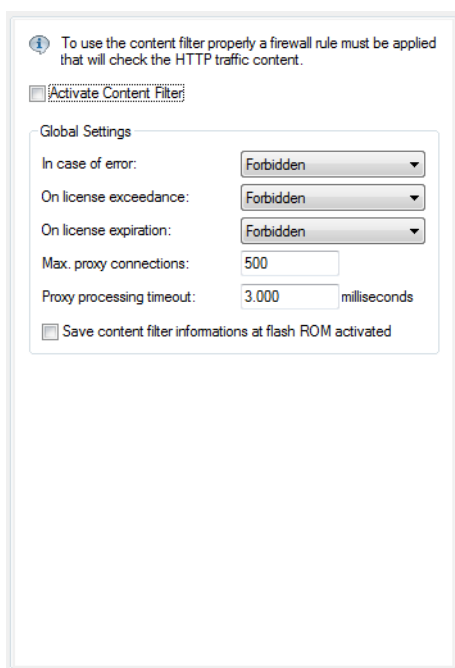
As of LCOS 8.80, the content filter supports a true concurrent user model. This model licenses the number of **concurrent** users of the content filter. In contrast to this, the previous "per-user model" licenses the number of all **potential** users.

Until now, the content filter retained a user in its internal user list for 24 hours. After using the content filter for the first time within a 24-hour period, the user is permanently listed and thus licensed.

As of LCOS 8.80, the content filter only maintains a user in its internal user list for 5 minutes. This change makes it possible for a changing selection of users to use the content filter. Your license now checks only the actual number of concurrent users (within the 5-minute period).

13.1.1 General settings

Global settings for the LANCOM Content Filter are made here:



LANconfig: Content Filter / General

WEBconfig: LCOS Menu Tree / Setup / UTM / Content-Filter / Global-Settings

- Operating

This is where you can activate the LANCOM Content Filter.

- Action-on-Error:

This is where you can determine what should happen when an error occurs. For example, if the rating server cannot be contacted, this setting either allows the user to surf without restrictions or access to the web is blocked entirely.

Possible values:

- Block, Pass

Default:

- Block

- Action on license exceedance:


This is where you can determine what should happen when the licensed number of users is exceeded. Users are identified by their IP address. The system keeps count of the IP addresses that connect via the LANCOM Content Filter. When the eleventh user establishes a connection with a 10-user license, no further checking is performed by the LANCOM Content Filter. Depending on this setting, the unlicensed user can either surf the web without restrictions, or access to the web is blocked entirely.

Possible values:

- Block, Pass

Default:

- Block

 The users of the content filter are automatically removed from the user list when no connection has been made from the IP address concerned via the content filter for 5 minutes.

- Action-on-License-Expiration:

The license to use the LANCOM Content Filter is valid for a certain period. You will be reminded of the license expiry date 30 days, one week and one day before it actually expires (at the e-mail address configured in LANconfig: Log & Trace / General).


This is where you can specify what should happen when the license expires (i.e. block everything or allow everything through). After the license expires, this setting either allows the user to surf the web without restrictions, or access to the web is blocked entirely.

Possible values:

- Block, Pass

Default:

- Block

 In order for the reminder to be sent to the specified e-mail address, you must configure the SMTP account.

- Max. proxy connections

This setting is for the maximum allowable number of simultaneous proxy connections. This limits the load that can be placed on the system. A notification is sent if this number should be exceeded. You can set the type of notification under **Content filter > Options > Events**.

Possible values:

- 0 to 999999 connections

Default:

- Depends on device

- Proxy processing timeout

Specifies the maximum time in milliseconds that the proxy can take for processing. A timeout error page is displayed if this time is exceeded.

Possible values:

13 LANCOM Content Filter

- 0 to 999999 milliseconds

Default:

- 3000 milliseconds

Special values:

- The value 0 sets no time limit. Values less than 100 milliseconds make no sense.

- Save content filter information to flash ROM activated

If you enable this option, you can additionally save the content filter information to the flash ROM memory of the device.

Default:

- Deactivated

13.2 New content filter category, Command/Control Server

As of LCOS 8.80, the content filter supports the new Web filter category Command and Control Server ("C&C server" for short). C&C servers monitor and control bots in a botnet.

13.2.1 Introduction


The LANCOM Content Filter enables you to filter certain content from your network, so preventing access to Internet pages with content that is illegal or offensive. It also enables you to stop private surfing on specific sites during working hours. This not only increases staff productivity and network security but also ensures that the full bandwidth is available exclusively for your business activities.

The LANCOM Content Filter is an intelligent content filter that works dynamically. It contacts a rating server that evaluates Internet sites reliably and accurately in accordance with the categories that you select.

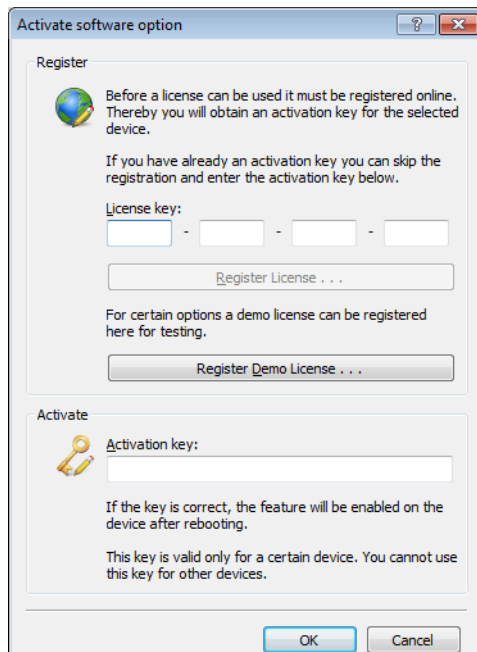
The LANCOM Content Filter operates by checking the IP addresses behind the URLs that are entered. For any given domain it is possible to differentiate according to the path, meaning that specific areas of a URL may be rated differently.

 It is not possible for users to avoid the LANCOM Content Filter website rating simply by entering the website's IP address into their browsers. The LANCOM Content Filter checks unencrypted (HTTP) and also encrypted Web pages (HTTPS).

The LANCOM Content Filter license you purchase is valid for a certain number of users and for a specific period (for one or three years). You will be informed of the expiry of your license in good time. The number of current users is monitored in the device, with the users being identified by their IP address. You can configure what should happen when the number of licensed users is exceeded: Access can either be denied or an unchecked connection can be made.

 You can test the LANCOM Content Filter on any router that supports this function. All you have to do is to activate a 30-day demo license for each device. Demo licenses are generated directly with LANconfig. Click on the device with the right-hand mouse key and select the context menu entry **Activate Software Option**. In the dialog that

follows, click on the button **Register demo license**. You will automatically be connected to the website for the LANCOM registration server. Simply select the required demo license and you can register your device.



All settings relating to categories are stored in category profiles. You select from predefined main and sub-categories in the LANCOM Content Filter: 59 categories are divided into 14 subject groups such as "Pornography, Nudity", "Shopping" or "Illegal Activities". You can activate or deactivate each of the categories that these groups contain. Sub-categories for "Pornography/Nudity" are, for example, "Pornography/Erotic/Sex" and "Swimwear/Lingerie".

When configuring these categories, administrators have an additional option of activating an override. When the override option is active, users may still access the forbidden site for a particular period of time by clicking on a corresponding button, but the administrator will be notified of this by e-mail, syslog, or SNMP trap.

The category profile, whitelist and blacklist can be used to create a content filter profile that you can assign to particular users by means of the firewall. For example you can create a profile called "Employees_department_A" and assign this to all of the computers in that department.

When you install the LANCOM Content Filter, basic default settings are created automatically. These only need to be activated for the initial start. You can subsequently customize the behavior of the LANCOM Content Filter to match your own requirements.

13.3 Additions to the menu system

13.3.1 Command/Control server

For each main category and the associated sub-categories, it is possible to define whether the URLs are to be allowed, forbidden or allowed with override only.

Telnet path: /Setup/UTM/Content-Filter/Profiles/Category-Profiles

The category profile must subsequently be assigned to a content-filter profile (together with a timeframe) to become active.

Possible values:

13 LANCOM Content Filter

Allowed, forbidden, override

Default:

Forbidden