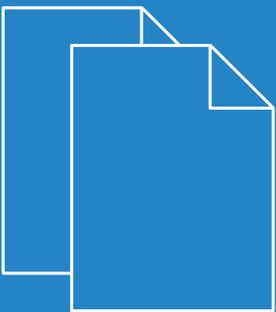


LCOS 10.12

Addendum



Contents

1 Addendum to LCOS version 10.12.....	5
2 WLAN management.....	6
2.1 RADIUS.....	6
2.1.1 Availability monitoring for external RADIUS servers.....	6
2.2 Coordinated channel selection for Wireless ePaper.....	12
2.2.1 Activation and configuration in LANconfig.....	13
2.2.2 Additions to the Status menu.....	14
2.2.3 Additions to the Setup menu.....	14
3 Wireless LAN – WLAN.....	19
3.1 Selectively allowing inter-station traffic for clients on the same VLAN.....	19
3.1.1 Configuration by LANconfig.....	19
3.1.2 Additions to the Setup menu.....	20
3.2 Starting an environment scan at a configurable time.....	21
3.2.1 Configuration by LANconfig.....	22
3.2.2 Additions to the Setup menu.....	24
3.3 Converting data streams from multicast into unicast.....	29
3.3.1 Configuration by LANconfig.....	30
3.3.2 The CLI 'show' command.....	31
3.3.3 Additions to the Setup menu.....	32
4 Routing and WAN connections.....	33
4.1 OSPF.....	33
4.1.1 Setting up OSPF with LANconfig.....	33
4.1.2 Show commands via CLI.....	44
4.1.3 Additions to the Setup menu.....	44
5 IPv6.....	69
5.1 Support for SNTP option in the DHCPv6 client.....	69
5.1.1 Configuration by LANconfig.....	69
5.1.2 Additions to the Setup menu.....	70
5.2 Support of prefix hint in the DHCPv6 client.....	70
5.2.1 Configuration by LANconfig.....	71
5.2.2 Additions to the Setup menu.....	72
5.3 Transmitting the IPv6 LAN prefix with the action table.....	72
5.4 DHCPv6 options.....	72
5.4.1 Configuration by LANconfig.....	73
5.4.2 Additions to the Setup menu.....	74
6 Virtual Private Networks - VPN.....	77
6.1 Addition to the IKEv2 encryption algorithms.....	77
6.1.1 Additions to the Setup menu.....	78
6.2 IKEv2 load balancer.....	80

6.2.1	Instances.....	82
6.2.2	Message profiles.....	83
6.2.3	Show commands via CLI.....	85
6.2.4	Trace commands.....	85
6.2.5	Additions to the Setup menu.....	85
6.3	Flexible identity comparison for PSK connections.....	93
6.4	SCEP client logging.....	95
6.4.1	Configuration by LANconfig.....	95
7	Public Spot.....	97
7.1	Independent user authentication (Smart Ticket).....	97
7.1.1	Restricting the allowed country codes when using SmartTicket via SMS.....	97
7.1.2	Additions to the Setup menu.....	98
8	Configuration.....	100
8.1	Importing files by copy & paste on the CLI.....	100
8.2	FirmSafe.....	102
8.2.1	Toggling the active firmware via console command.....	102
8.2.2	Additions to the Firmware menu.....	103
9	Voice over IP – VoIP.....	104
9.1	Transmitting phone numbers for VoIP connections.....	104
9.1.1	SIP lines.....	104
9.1.2	Additions to the Setup menu.....	105
9.2	Overlap dialing for devices with Voice Call Manager.....	106
9.2.1	Additions to the Setup menu.....	108
9.3	Fallback from an encrypted to an unencrypted VoIP connection.....	109
9.3.1	Additions to the Setup menu.....	109
9.4	Prohibit control characters on SIP lines.....	110
10	Diagnosis.....	113
10.1	SYSLOG messaging via TCP.....	113
10.1.1	Configuration by LANconfig.....	113
10.1.2	Additions to the Setup menu.....	114
10.2	IPv4/IPv6 traffic accounting.....	115
10.2.1	Additions to the Status menu.....	115
11	Interface bundling with LACP.....	116
11.1	Configuring the LACP interfaces.....	116
11.1.1	Additions to the Setup menu.....	118
12	LANCOM Content Filter.....	122
12.1	Unknown traffic via port 443.....	122
12.1.1	Additions to the Setup menu.....	123
12.2	IPv6 support.....	123
12.2.1	Configuration by LANconfig.....	125
12.2.2	Additions to the Setup menu.....	128
13	Other services.....	130
13.1	Time server for the local network.....	130

13.1.1 Configuration by LANconfig.....	130
13.1.2 Additions to the Setup menu.....	132
13.2 Simple Network Management Protocol (SNMP).....	136
13.2.1 Setting up SNMP with LANconfig.....	136
13.2.2 Additions to the Setup menu.....	137
14 Appendix.....	139
14.1 CRON syntax.....	139

1 Addendum to LCOS version 10.12

This document describes the changes and enhancements in LCOS version 10.12 since the previous version.

2 WLAN management

2.1 RADIUS

2.1.1 Availability monitoring for external RADIUS servers

As of LCOS version 10.12, you can use this feature to monitor the availability of a RADIUS server. RADIUS requests are sent at regular intervals to check whether the RADIUS service is functional.

Monitoring can be performed as follows:

- By sending status server requests (DEFAULT). These are specifically used to check the availability of RADIUS services. However, they are not supported by all RADIUS servers (a positive example is FreeRADIUS).
- By sending access requests ("dummy requests"). Only use this method if the server does not support status server requests.

You can create supervision profiles under **Setup > RADIUS > Supervision-Servers > Profiles**. These include the method used to monitor the availability test, the interval (in seconds) after which each check is performed, and the attributes to be attached to an access request (there must be at least one user name for the dummy request; status server requests do not require any additional attributes). The DEFAULT profile contains the following:

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

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

The following is an example profile for the use of access requests:

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

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

Here you see that the user name has been set as an attribute. Make sure you the user name is not known to the RADIUS server: This prevents a regular logon to the RADIUS server. The "pseudo-login" attempts by the monitoring system are taken to be failed logins.

You can now reference a profile contained in this table. This is possible for the RADIUS server used for 802.1X. The following is an example entry in the appropriate table:

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

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

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

The RADIUS server specified here is monitored using the supervision profile "DEFAULT". If an entry for "Sup.-Profile" does not match with a supervision profile, the DEFAULT profile is used automatically. If "Sup.-Profile" is empty, no monitoring is performed.

The monitored RADIUS servers and their status can be viewed in the following table:

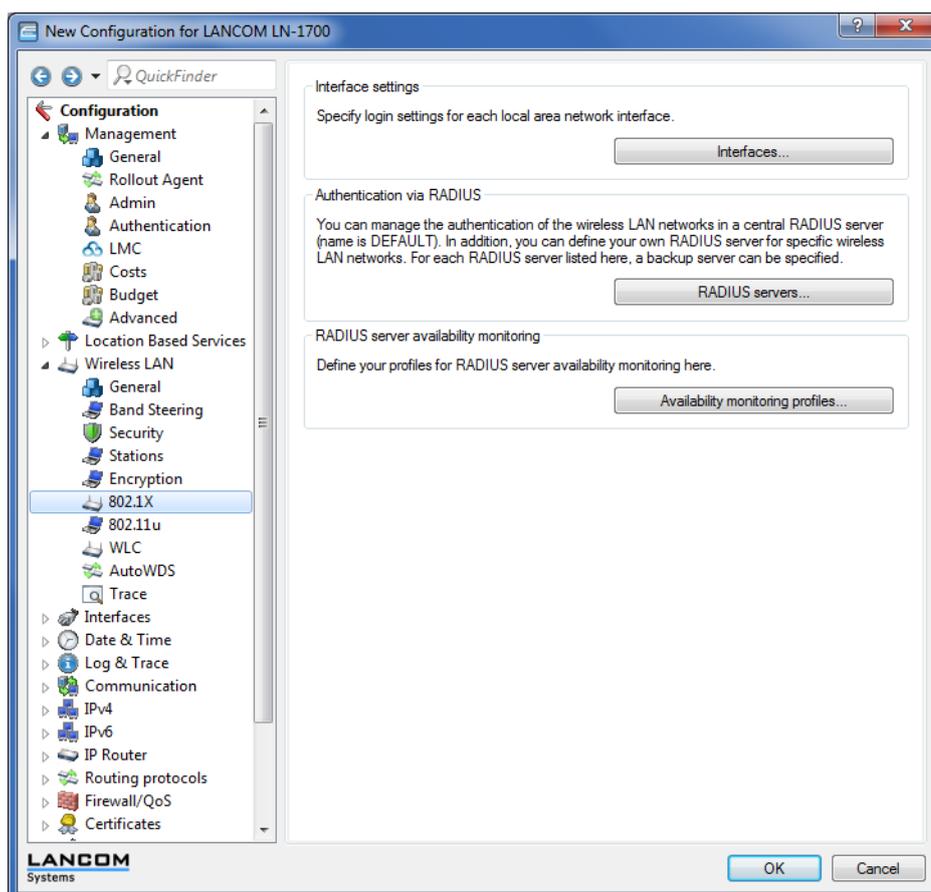
```
root@LCS_L452_Office:~/Status/TCP-IP/RADIUS-Supervision-Servers/Servers
> ls -a
[1.3.6.1.4.1.2356.11][1.9.14.1]

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

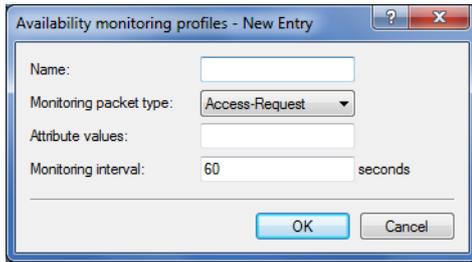
The statistic table is also available under the following path: **Status > SLA-Monitor > RADIUS > Servers.**

Availability monitoring profiles in LANconfig

Navigate to **Wireless LAN > 802.1X > RADIUS server availability monitoring.**



The table **Availability monitoring profiles** provides the following configuration options:



Name

Contains the name of the availability monitoring profile.

Monitoring packet type

Your choices are as follows:

Access request (default)

Only use this type if the server does not support status server requests.

Status server

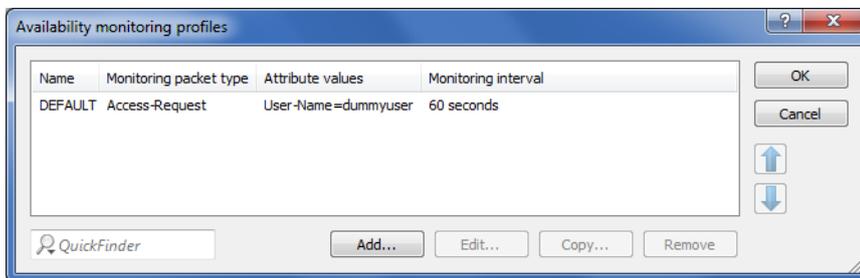
This type is specifically for the availability monitoring of RADIUS services, but it is not supported by all RADIUS servers.

Attribute values

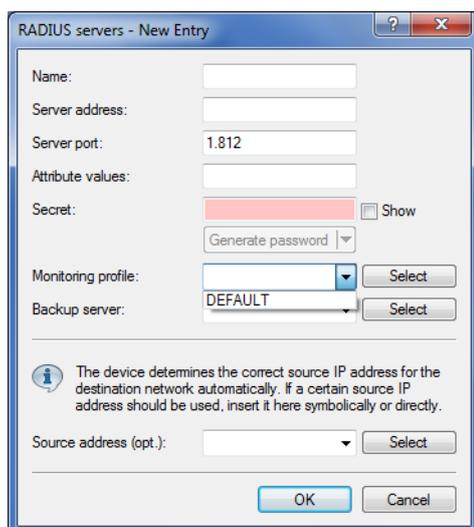
An attribute is only required for access requests. It is not required for status server requests.

Monitoring Interval

The monitoring interval in seconds (default: 60)



The new availability monitoring profile (in this case: DEFAULT) is now also available for use in the **RADIUS server** table:



Additions to the Status menu

Servers

This entry contains the status values for Servers.

SNMP ID:

1.36.2.1

Telnet path:

Status > SLA-Monitor > RADIUS

Possible values:

0

Unknown

The status of the server is not known either because no request has been sent to it or because no valid response has been received.

1

Up

The server responded to a request with a valid RADIUS response and is therefore assumed to be operational.

2

DNS error

The device cannot resolve the name of the DNS server.

3

Authenticator mismatch

The device received a response from the server, but with a faulty authentication. This indicates a shared-secret mismatch. Note that this status can only occur if, for test purposes, access requests are sent to the server immediately following this type of a mismatch. This is because status server packets contain a message authenticator attribute and are dropped silently in the event of a mismatch. Despite

this, a shared-secret mismatch does not indicate that the server is temporarily unavailable; it rather indicates a permanent mis-configuration.

4

Host unreachable

The server is not accessible via IP.

5

Port unreachable

The server is accessible via IP, but no RADIUS server is using the specified port.

6

Timeout

It is not possible to route the server's IP address.

Additions to the Setup menu

Availability monitoring

In this directory you configure the availability monitoring.

Monitoring is performed by sending status server requests or access requests.

SNMP ID:

2.25.21

Telnet path:

Setup > RADIUS

Profiles

Here you create monitoring profiles for the availability of RADIUS servers.

SNMP ID:

2.25.21.1

Telnet path:

Setup > RADIUS > Supervision-Servers

Name

Enter the name of the availability monitoring profile here.

SNMP ID:

2.25.21.1.1

Telnet path:

Setup > RADIUS > Supervision-Servers > Profiles

Possible values:

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

Default:

DEFAULT

Type

Here, you specify whether status server or access requests are sent to the RADIUS server for the purpose of availability monitoring.

SNMP ID:

2.25.21.1.2

Telnet path:

Setup > RADIUS > Supervision-Servers > Profiles

Possible values:

Access request
Status server

Default:

Access request

Attributes

If availability monitoring is performed with access requests, you can specify the attributes of the access request here by means of a comma-separated list in the format **Attribute1=value1,Attribute2=value2, etc.**. Accessibility checks by means of an access request require at least the specification of the attribute "User-Name", e.g. **User-Name=dummyuser**.



Status server requests do not require any attributes.

SNMP ID:

2.25.21.1.3

Telnet path:

Setup > RADIUS > Supervision-Servers > Profiles

Possible values:

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

Default:

empty

Request interval

Here you define the interval in seconds used by the RADIUS server to check the availability.

SNMP ID:

2.25.21.1.4

Telnet path:

Setup > RADIUS > Supervision-Servers > Profiles

Possible values:

[0–9]

Default:

60

2.2 Coordinated channel selection for Wireless ePaper

As of LCOS version 10.12, the Wireless ePaper feature offers coordinated channel selection.

This is particularly useful if you operate multiple Wireless ePaper access points at a site.

Each AP requires its own ePaper channel, so collisions or multiple assignments need to be avoided.

For this reason, ePaper APs automatically discover neighboring ePaper APs within a broadcast domain by means of a TCP-based protocol that is transmitted in a multicast group. One of these APs is automatically set as the master AP. The remaining APs become slave APs. If the master AP fails, one of the slave APs is automatically designated as the new master AP.

Each slave AP regularly sends an assessment of its current ePaper channel to the master AP. Based on the assessments from all the slaves, the master decides whether or not a slave needs to change channel.

Each ePaper AP assesses all of the ePaper channels. This takes into account the locally used WLAN channel (which the ePaper channel should not overlap) and whether the ePaper channel is a preferred channel.

 Preferred channels are: 3, 5, 8, 9 and 10.

Based on the channel assessments received, the ePaper channels are optimized as follows:

The master AP selects the best of the free channels and assigns it to the ePaper AP with the lowest ePaper AP ID (the master also assigns a channel to itself). This is performed successively for all of the ePaper APs.

 Channels are only switched if the evaluation of the competing channel is better by a certain, configurable threshold. This avoids unnecessary channel changes.

If the network contains one or more ePaper APs with a statically assigned ePaper channel, the master can still perform a coordinated channel selection. If this is enabled on an AP with a static channel, the master performing the channel allocation will consider this channel to be already assigned and will not assign it to any other AP.

The status menu of the Wireless ePaper feature has been supplemented with a peer table. This lists the APs involved in channel coordination.

The peer table contains the ePaper AP ID, the role of the AP (slave or master), the channel assessment, and the assigned ePaper channel.

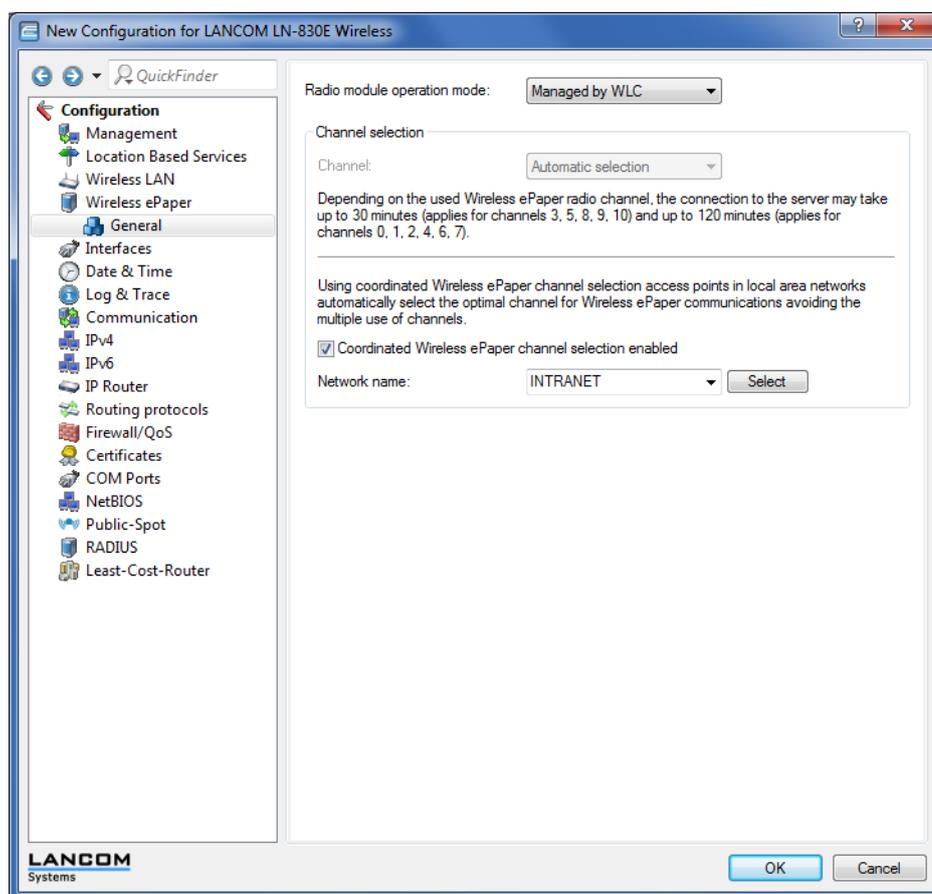
The channel assessment is shown as a list of the ePaper channels 0 to 10 followed by the assessment value. The value range is 0 to 255, a higher value being a better rating.

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

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

2.2.1 Activation and configuration in LANconfig

You activate and configure the feature under **Wireless ePaper > General**.



1. Activate the coordinated channel selection using the check box **Coordinated Wireless ePaper channel selection enabled**.

! If coordinated channel selection is not activated, the parameter **Network name** is grayed out.

2. Select the network to be used for the access points to communicate with one another from the **Network name** selection list.
3. Confirm your settings by clicking the **OK** button.

2.2.2 Additions to the Status menu

Channel coordination

This menu contains the settings for the coordinated channel assignment.

SNMP ID:

1.88.9

Telnet path:

Status > Wireless-ePaper

2.2.3 Additions to the Setup menu

Channel coordination

Prevents collisions on ePaper channels due to APs within range of each other.

SNMP ID:

2.88.4

Telnet path:

Setup > Wireless-ePaper

Operating

The coordinated channel selection is activated or deactivated here.

SNMP ID:

2.88.4.1

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

0

No

1

Yes

Default:

1

Network

Here you specify the network that the access points are to use to communicate with each other.

SNMP ID:

2.88.4.2

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**16 characters from the following character set [A-Z 0-9
@{ | } ~ ! \$ % ' () # * + - , / : ; ? [\] ^ _ . & < = >]**Announce address**

Set the announce address here.

SNMP ID:

2.88.4.3

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**

39 characters from the following character set: [0-9 A-F a-f : .]

Announce port

Set the announce port here.

SNMP ID:

2.88.4.4

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**

5 characters from the following character set: [0-9]

Announce interval

Set the announce interval here.

SNMP ID:

2.88.4.5

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination**

Possible values:

10 characters from the following character set: [0–9]

Announce timeout factor

Set the announce timeout factor here.

SNMP ID:

2.88.4.6

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

5 characters from the following character set: [0–9]

Announce timeout interval

Set the announce timeout interval here.

SNMP ID:

2.88.4.7

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

10 characters from the following character set: [0–9]

Announce master backoff interval

Set the announce master backoff interval here.

SNMP ID:

2.88.4.8

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

3 characters from the following character set: [0–9]

Coordination port

Set the coordination port here.

SNMP ID:

2.88.4.9

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**

5 characters from the following character set: [0-9]

Coordination keep-alive interval

Here you set the coordination keep-alive interval.

SNMP ID:

2.88.4.10

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**

10 characters from the following character set: [0-9]

Coordination reconnect interval

Here you set the coordination reconnect interval.

SNMP ID:

2.88.4.11

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination****Possible values:**

10 characters from the following character set: [0-9]

Assignment switch threshold

Here you set the assignment switch threshold.

SNMP ID:

2.88.4.12

Telnet path:**Setup > Wireless-ePaper > Channel-Coordination**

Possible values:

3 characters from the following character set: [0–9]

Distance weighting

Here you set the weighting of WLAN distance.



A higher value means a better weighting.

SNMP ID:

2.88.4.13

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

0 ... 255

Channel weighting

Here you set the weighting of a preferred channel.



A higher value means a better weighting.

SNMP ID:

2.88.4.14

Telnet path:

Setup > Wireless-ePaper > Channel-Coordination

Possible values:

0 ... 255

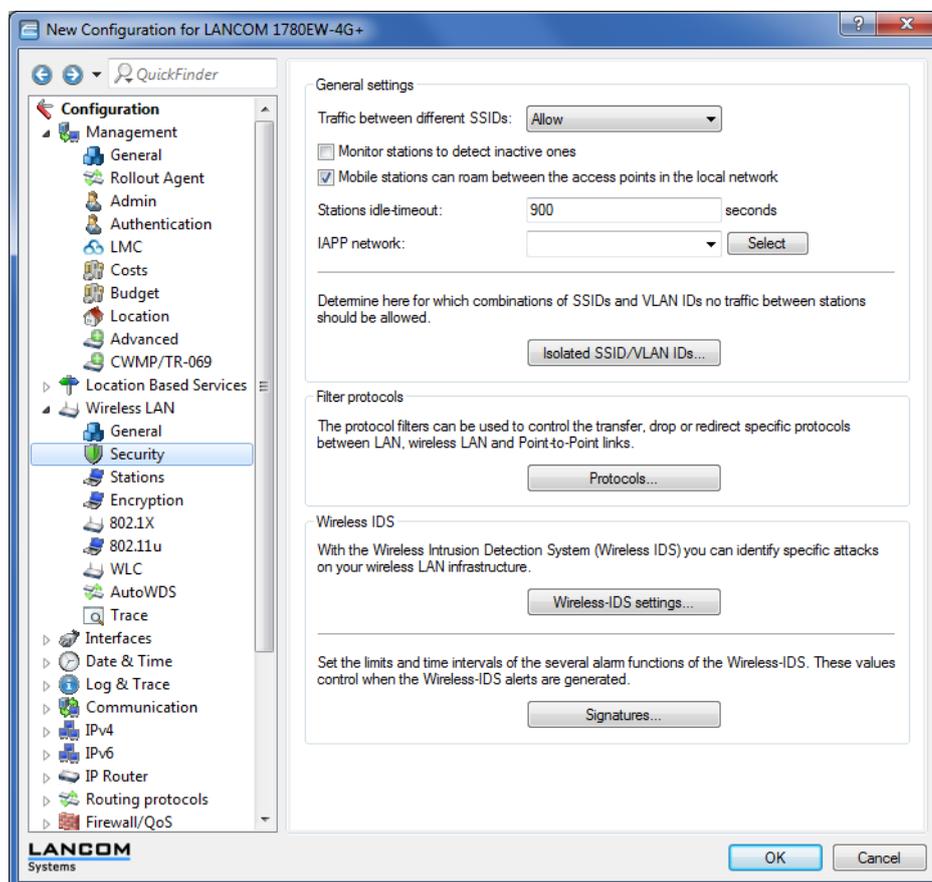
3 Wireless LAN – WLAN

3.1 Selectively allowing inter-station traffic for clients on the same VLAN

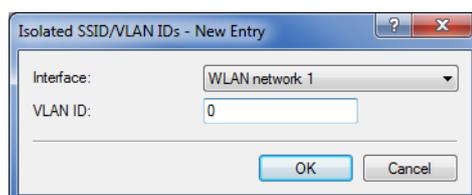
As of LCOS version 10.12 this feature allows you to map a "collective VLAN" where WLAN clients are unable to communicate with one another. Communication is only possible between WLAN client and AP (hotspot scenario). Outside of this collective VLAN, communication between the clients can be permitted. This works perfectly transparently within a common SSID where the clients are assigned to different VLANs.

3.1.1 Configuration by LANconfig

Navigate to **Wireless LAN > Security**.



Add a new entry to the menu **Isolated SSID / VLAN IDs**:



Here you specify the combinations of SSIDs and VLANs between which the traffic between clients is prohibited. This table functions as a blacklist because, generally speaking, we define just a few VLANs where the communication is forbidden, but several where it is allowed.

 This mechanism also works when the clients are associated with different APs (although care should be taken to ensure that the table configurations match). A prerequisite for this is that the APs are able to communicate via IAPP.

The table contains the following parameters:

Interface

The list of available WLAN networks.

VLAN-ID

The identification number of the VLAN.

 The menu item **Traffic between different SSIDs** must be set to **Allow** in order for this feature to manage the restrictions.

3.1.2 Additions to the Setup menu

VLAN no interstation traffic

This table contains combinations of SSIDs and VLANs for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71

Telnet path:

Setup > WLAN

Network

From the list of available SSIDs, select the network for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71.1

Telnet path:

Setup > WLAN > VLAN-No-Interstation-Traffic

VLAN-ID

Here you specify the VLAN ID for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71.2

Telnet path:**Setup > WLAN > VLAN-No-Interstation-Traffic****Possible values:**

1 ... 4094

Default:

0

3.2 Starting an environment scan at a configurable time

Your WLAN's environment can be regularly searched for rogue APs.

As of LCOS version 10.12, you can configure the times of the automatic environment scan for rogue APs.

Environment scans should be performed at times that minimize interference to normal operations.

This feature allows you to perform the scan of the configured frequency band each day at a predefined time.

In this case, scan refers to:

- > Active scanning using probe requests.
- > Passive scanning for beacons.

 It is not always possible to use active scanning, for example where a 5-GHz channel is not DFS-free. No transmissions are permitted in this case.

The configuration is performed from the command console, shown here with default values as an example:

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

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

"Hour" and "Minute" are used to set the time at which the daily environment scan is performed. These fields also permit the use of the CRON syntax. The channel list can be used to limit the channels to be scanned (as a comma-separated list). If this list is left empty, all of the channels of the frequency band operating on the module are scanned.

During the scan, the WLAN module spends about three seconds on each channel. The next channel is then scanned. Once all of the configured channels have been scanned, the module returns to normal operating mode.

 During the scan the module is not capable of regular WLAN operations, in contrast, for example, to the background scan. However, only one of the two modules can perform an environment scan at any one time, and the other module operates normally.

In addition to the time-controlled activation of the environment scan, it can also be activated permanently. For this purpose, the WLAN module can be switched to the operating mode "Scanner" (see operation mode 7):

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

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

3 Wireless LAN – WLAN

```

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

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

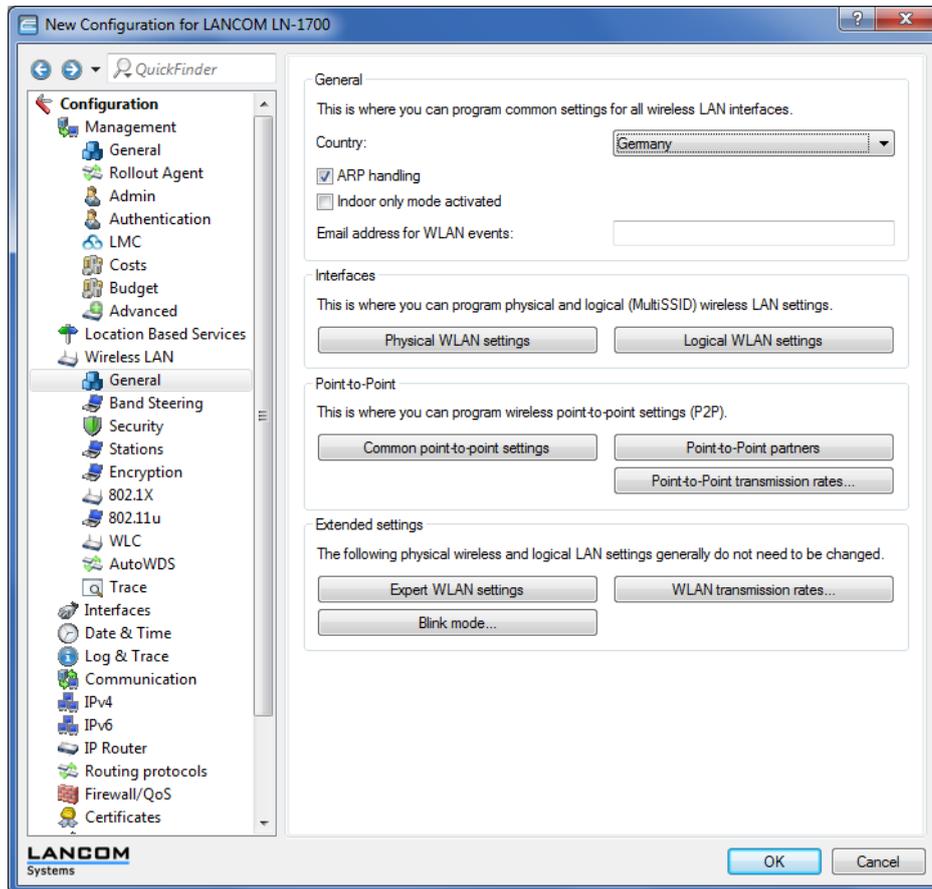
This performs the environment scan as described above: After scanning the configured channels, the scan does not terminate but it starts again from the beginning.

This operating mode allows the use of an AP as a full-time "scanner" AP.

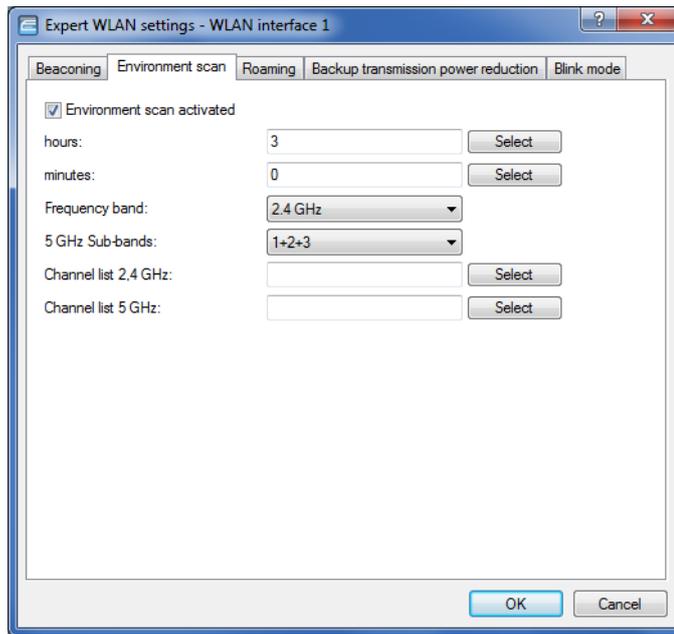
The result of the environment scan can be found in the table **Status > WLAN > Environment-Scan-Results**.

3.2.1 Configuration by LANconfig

Navigate to **Wireless LAN > General > Extended settings**.



The parameters for the environment scan are set in the table **Expert WLAN settings** on the tab **Environment scan**.



Environment scan activated

Activates/deactivates the environment scan.



The following parameters are grayed out if the environment scan is disabled.

Hours

Contains the hour value of the time for the environment scan.

Minutes

Contains the minute value of the time for the environment scan.

Frequency band

Contains the frequency bands for the environment scan.

Possible values:

2.4 GHz

Scans the 2.4-GHz frequency band.

5 GHz

Scans the 5-GHz frequency band.

2.4/5 GHz

Scans the 2.4-GHz and 5-GHz frequency bands.

5-GHz subbands

Contains the subbands of the 5-GHz frequency band.

Possible values:

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

Channel list 2.4 GHz

Specifies the 2.4-GHz channels for the environment scan.

 If you make no entries here, the environmental scan is performed for all channels of the 2.4-GHz frequency band.

Possible values (multiple selection allowed):

1 to 13

In steps of 1.

Channel list 5GHz

Specifies the 5-GHz channels for the environment scan.

 If you make no entries here, the environmental scan is performed for all channels of the 5-GHz frequency band.

Possible values (multiple selection allowed):

36 to 64

In steps of 4.

100 to 140

In steps of 4.

3.2.2 Additions to the Setup menu

Starting an environment scan at a configurable time

This table is used to specify the daily time when the frequency band of the corresponding interface is scanned for rogue APs. It is also possible to use the *CRON syntax* for this. The search relies on active scanning with probe requests as well as passive scanning for beacons.

 It is not always possible to use active scanning, for example where a 5-GHz channel is not DFS-free.

SNMP ID:

2.23.20.27

Telnet path:

Setup > Interfaces > WLAN

Ifc

This table contains the available WLAN interfaces.

SNMP ID:

2.23.20.27.1

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

1

WLAN-1

2

WLAN-2

Yes

Enables/disables the environment scan.

SNMP ID:

2.23.20.27.2

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

0

Not active

1

Active

Default:

0

Hours

Set the hours value for the time of the environment scan here.

SNMP ID:

2.23.20.27.6

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

0 ... 23

Default:

3

Minutes

Set the minutes value for the time of the environment scan here.

SNMP ID:

2.23.20.27.7

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

0 ... 59

Default:

0

Frequency band

Here you set the radio band for which your WLAN module performs an environment scan.

SNMP ID:

2.23.20.27.8

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

2.4 GHz

Scans the 2.4-GHz frequency band.

5 GHz

Scans the 5-GHz frequency band.

2.4/5 GHz

Scans the 2.4-GHz and 5-GHz frequency bands.

Default:

2.4 GHz

Subbands-5GHz

Here you configure the subbands of your 5-GHz frequency band.

SNMP ID:

2.23.20.27.9

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

1+2+3

1+2

1+3

2+3

1

2

3

Default:

1+2+3

Channel-List-2.4 GHz

Here you can limit the 2.4-GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 2.4-GHz frequency band.

SNMP ID:

2.23.20.27.10

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

empty

The environment scan is performed for all channels in the 2.4-GHz frequency band.

1

The environment scan is performed for channel 1 in the 2.4-GHz frequency band.

2

The environment scan is performed for channel 2 in the 2.4-GHz frequency band.

3

The environment scan is performed for channel 3 in the 2.4-GHz frequency band.

4

The environment scan is performed for channel 4 in the 2.4-GHz frequency band.

5

The environment scan is performed for channel 5 in the 2.4-GHz frequency band.

- 6**
The environment scan is performed for channel 6 in the 2.4-GHz frequency band.
- 7**
The environment scan is performed for channel 7 in the 2.4-GHz frequency band.
- 8**
The environment scan is performed for channel 8 in the 2.4-GHz frequency band.
- 9**
The environment scan is performed for channel 9 in the 2.4-GHz frequency band.
- 10**
The environment scan is performed for channel 10 in the 2.4-GHz frequency band.
- 11**
The environment scan is performed for channel 11 in the 2.4-GHz frequency band.
- 12**
The environment scan is performed for channel 12 in the 2.4-GHz frequency band.
- 13**
The environment scan is performed for channel 13 in the 2.4-GHz frequency band.

Channel-List-5 GHz

Here you can limit the 5-GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 5-GHz frequency band.

SNMP ID:

2.23.20.27.11

Telnet path:

Setup > Interfaces > WLAN > Environment-Scan

Possible values:

empty

The environment scan is performed for all channels in the 5-GHz frequency band.

- 36**
The environment scan is performed for channel 36 in the 5-GHz frequency band.
- 40**
The environment scan is performed for channel 40 in the 5-GHz frequency band.
- 44**
The environment scan is performed for channel 44 in the 5-GHz frequency band.
- 48**
The environment scan is performed for channel 48 in the 5-GHz frequency band.
- 52**
The environment scan is performed for channel 52 in the 5-GHz frequency band.
- 56**
The environment scan is performed for channel 56 in the 5-GHz frequency band.
- 60**
The environment scan is performed for channel 60 in the 5-GHz frequency band.

- 64** The environment scan is performed for channel 64 in the 5-GHz frequency band.
- 100** The environment scan is performed for channel 100 in the 5-GHz frequency band.
- 104** The environment scan is performed for channel 104 in the 5-GHz frequency band.
- 108** The environment scan is performed for channel 108 in the 5-GHz frequency band.
- 112** The environment scan is performed for channel 112 in the 5-GHz frequency band.
- 116** The environment scan is performed for channel 116 in the 5-GHz frequency band.
- 120** The environment scan is performed for channel 120 in the 5-GHz frequency band.
- 124** The environment scan is performed for channel 124 in the 5-GHz frequency band.
- 128** The environment scan is performed for channel 128 in the 5-GHz frequency band.
- 132** The environment scan is performed for channel 132 in the 5-GHz frequency band.
- 136** The environment scan is performed for channel 136 in the 5-GHz frequency band.
- 140** The environment scan is performed for channel 140 in the 5-GHz frequency band.

3.3 Converting data streams from multicast into unicast

As of LCOS version 10.12, you can convert multicast data streams to unicast data streams.

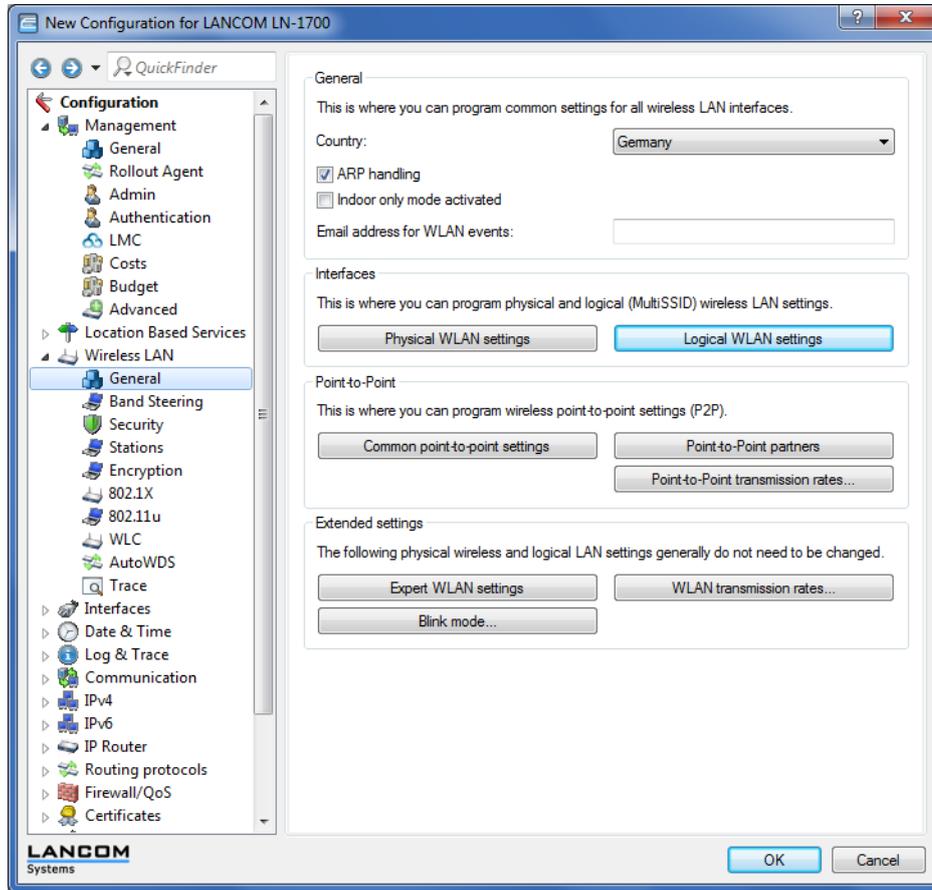
The ability to automatically convert multicast to unicast data streams allows multiple WLAN clients to smoothly stream high-resolution video applications. For applications such as IPTV services, you benefit from better performance and a marked improvement in quality.

After activation of the feature, multicast data streams intended for transmission over WLAN interfaces are converted on the MAC layer or WLAN layer into individual unicast data streams for each client. Although the packets are identical for each client, the fact that they are now part of a unicast means that they can be transmitted at the highest possible data rate supported by the respective client. Even though the packets are now duplicated, in most scenarios the much faster transmission means that significantly less airtime is consumed, which benefits the other transmissions.

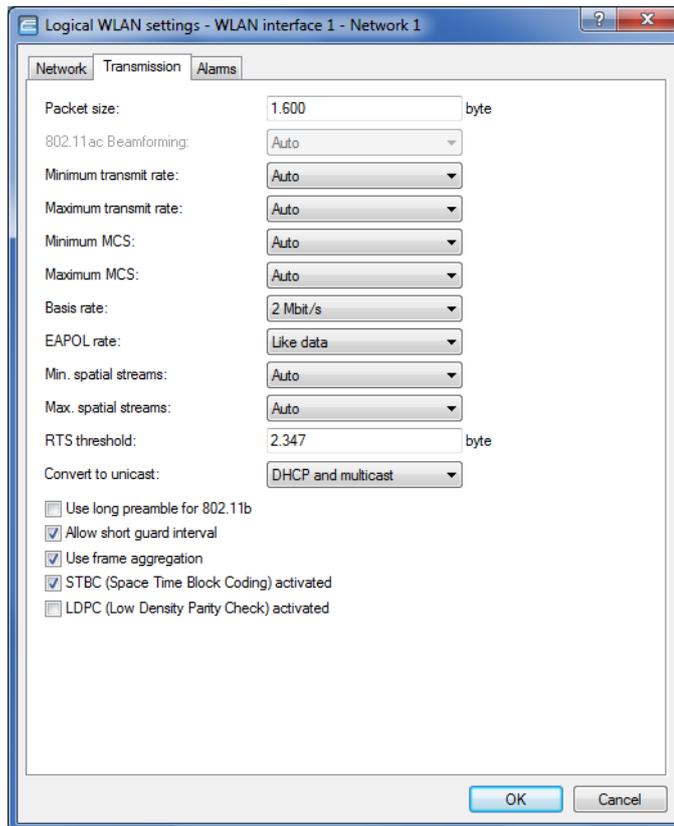
 In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

3.3.1 Configuration by LANconfig

The new feature is to be found under **Wireless LAN > General > Interfaces > Logical WLAN settings**



after selecting a WLAN interface on the **Transmission** tab.



Convert to unicast

You have the following options for converting data streams to unicast:

None

No data streams are converted to unicast.

DHCP

Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

Multicast

After activation of the feature, multicast data streams intended for transmission over WLAN interfaces are converted on the MAC layer or WLAN layer into individual unicast data streams for each client.

DHCP and multicast

Converts DHCP and multicast data streams to unicast.

3.3.2 The CLI 'show' command

Using the command `show igmp-snooping` you can see which clients have "subscribed" to which multicast groups. If the feature is activated, a conversion is performed for the members listed here. Here's an example:

```
> show igmp-snooping
```

```
Group          | VLAN | Ports
```

```

=====
224.0.0.251      |      1 | WLAN-1

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

```

3.3.3 Additions to the Setup menu

Convert-to-Unicast

This parameter is used to specify which type of data packets sent in a WLAN as a broadcast are automatically converted into unicast by the device.

SNMP ID:

2.23.20.2.25

Telnet path:

Setup > Interfaces > WLAN > Transmission

Possible values:

0

None

1

DHCP: Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

2

Multicast: In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

3

DHCP and multicast conversion

Default:

1

4 Routing and WAN connections

4.1 OSPF

As of version 10.12, LCOS features OSPF.

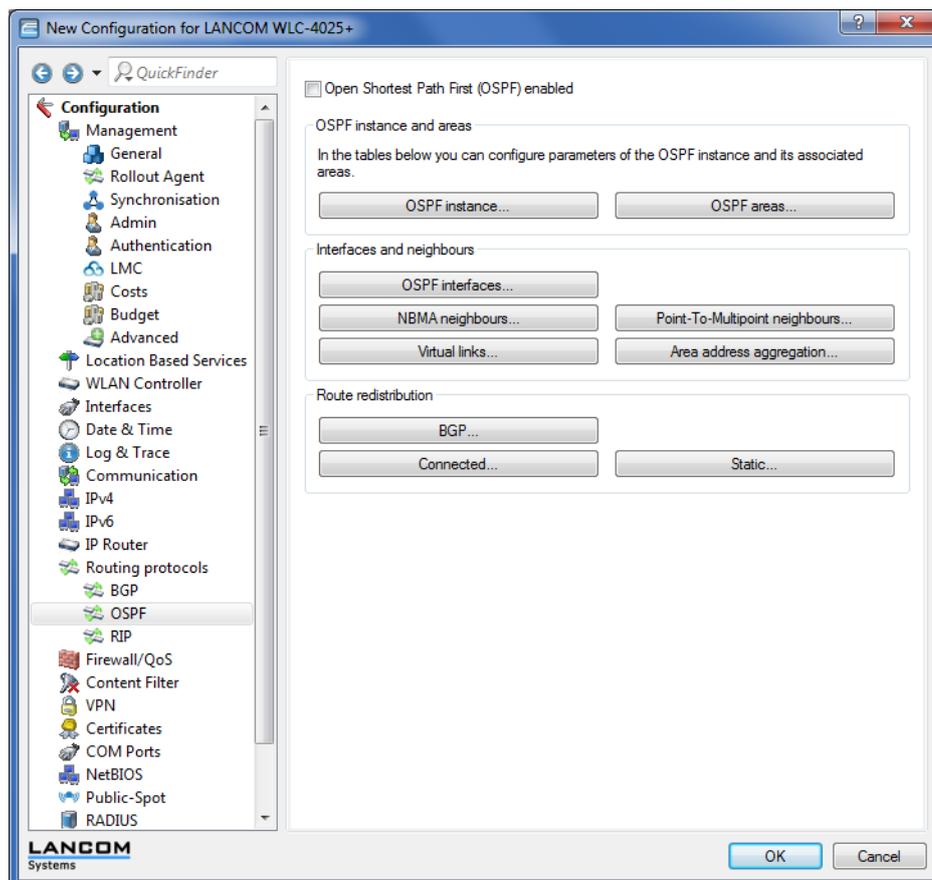
Open Shortest Path First (OSPF) is a link-state routing protocol as per RFC 2328. It belongs to the category **Interior Gateway Protocols (IGP)**. This involves routers regularly exchanging link-status information via link-state advertisements (LSA). The routers use multicast to automatically discover one another on the local network. OSPF is generally used for the exchange of internal routing information in large networks (LANs).

Each router has an identical copy of the database (link state database, LSDB), which routers use to determine the best routes (Shortest Path First, SPF) using the Dijkstra algorithm.

In contrast, BGP is one of the **Exterior Gateway Protocols (EGP)** and is typically used to route between autonomous systems or within VPNs.

4.1.1 Setting up OSPF with LANconfig

In order to configure OSPF with LANconfig, navigate to the **Routing protocols > OSPF** menu.



Open Shortest Path First (OSPF) enabled

To activate the OSPF function, set a check mark for **Open Shortest Path First (OSPF) enabled**.

OSPF instance

The table **OSPF instance** defines the OSPF instances on this device. It is possible for a device to operate multiple OSPF instances in parallel. Each instance corresponds to an autonomous system or an OSPF domain.

OSPF areas

The table **OSPF areas** is used to define the parameters of the OSPF areas.

OSPF interfaces

This table specifies the interfaces on which OSPF is to operate.

NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.



The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. If no default router is selected, multicast is used for communications instead.

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at area borders that transition from non-backbone areas to the backbone area. The corresponding subnet is advertised as a summary LSA.

BGP

Routes learned dynamically from BGP sources or protocols can be distributed by OSPF.

Connected

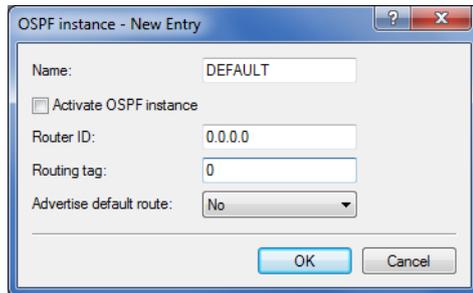
Connected routes, i.e. routes that the operating system automatically enters into the routing table, can be redistributed by OSPF.

Static

Static routes, i.e. routes that the user manually enters into the routing table, can be redistributed by OSPF.

OSPF instance

You configure the OSPF instance of the device under **OSPF instance**.



Name

Contains the name of the OSPF instance.

Activate OSPF instance

Activates or deactivates this OSPF instance.

Router ID

Contains the 32-bit router ID (represented as an IPv4 address) of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

Routing tag

Contains the routing tag assigned to this instance.

Advertise default route

Specifies whether this router should advertise or propagate the default route in this instance.

Possible values:

No (Default)

The router does not advertise a default route.

Yes

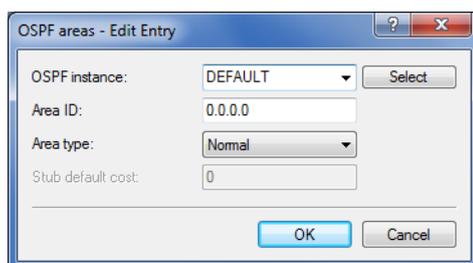
The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

OSPF areas

The parameters for the OSPF area are configured under **OSPF areas ...**.



OSPF instance

Contains the name of the OSPF instance.

Area ID

The area ID (displayed as an IPv4 address) identifies the area.

 If this instance is to be the backbone area, the value to be used is 0.0.0.0.

Area type

Specifies the type of the area.

Possible values:

Normal (default)

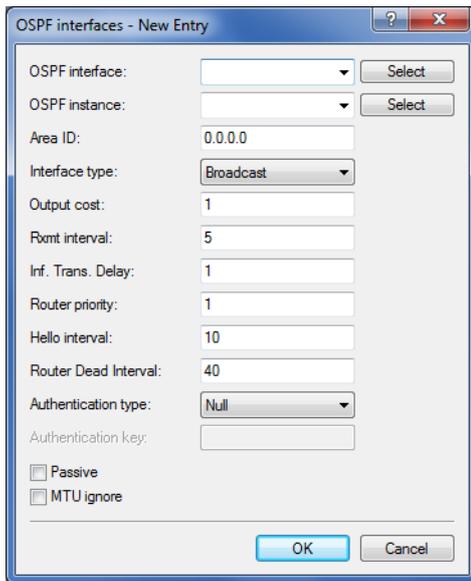
Stub

Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

OSPF interfaces

Defines the interfaces on which OSPF should be operated.

**OSPF interface**

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

Port type

Defines the interface type.

Possible values:

Broadcast

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

Non-Broadcast Multi-Access (NBMA)

Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication; the neighbors are configured manually.

Output cost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

 The value must always be greater than zero.

Retransmit interval

Contains the number of seconds between retransmissions.

Transmit delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

Router priority

Defines the priority of this router on this interface when set as the designated router (DR). The router with the highest priority is set as the default router.

 The value 0 prevents the router from becoming default router on this interface.

Hello interval

Contains the interval in seconds in which the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

 This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

Null**Simple password****Cryptographic MD5****Authentication key**

Contains the authentication key for this network.

! In this case the authentication type **Null** may not be selected.

Passive

Defines whether OSPF should work actively or passively on this interface.

Possible values:

Yes

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

No (Default)**MTU ignore**

Disables the MTU value check in database description packets.

! This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. Initially, a default router is selected for this purpose.

! The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

OSPF instance

Contains the name of the OSPF instance.

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

Polling interval

Contains the interval in which Hello messages are sent to this router.

! The value zero disables the transmission of Hello messages.

Eligible as default router

Specifies whether the local device itself is selectable as default router.

Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. No default router is selected and multicast is used for communications.

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

Polling interval

Contains the interval in which Hello messages are sent to this router.



The value zero disables the transmission of Hello messages.

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

OSPF instance

Contains the name of the OSPF instance.

Transit area ID

Contains the area ID, defined as an IPv4 address.

Router ID

Contains the router ID of the router at the remote end of the virtual link as an IPv4 address.

Retransmit interval

Contains the number of seconds between retransmissions.

Hello interval

Specifies the interval in seconds that the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

! This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

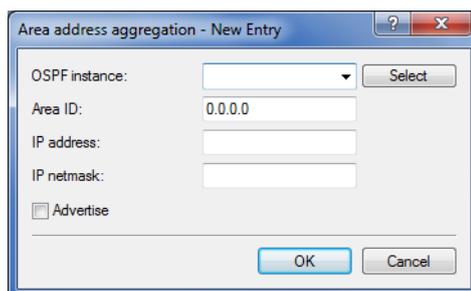
Null**Simple password****Cryptographic MD5****Authentication key**

Contains the authentication key for this network.

! In this case the authentication type **Null** may not be selected.

Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at area borders that transition from non-backbone areas to the backbone area. The corresponding subnet is advertised as a summary LSA.

**OSPF instance**

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

! If this instance is to be the backbone area, the value to be used is 0.0.0.0.

IP address

Contains the IPv4 address.

IP netmask

Contains the IPv4 subnet mask.

Advertise

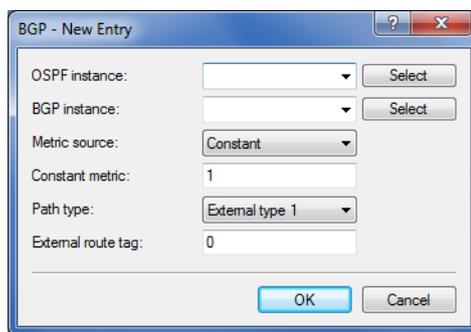
Enables or disables the advertisement of this address aggregation.

Route redistribution

Routes can be redistributed from other route sources or protocols by means of OSPF. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by OSPF.

BGP

The distribution of routes learned dynamically from the Border Gateway Protocol is configured under **BGP**.

**OSPF instance**

Contains the name of the OSPF instance.

BGP instance

Contains the name of the BGP instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The "Local preference" value of the BGP prefix is used or imported.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

! In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

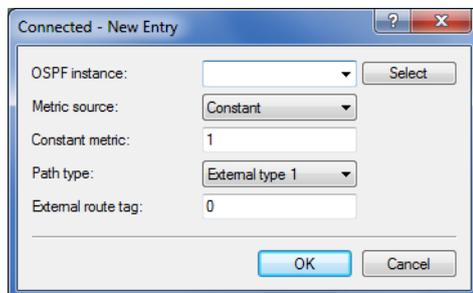
External route tag

Specifies which external route tag the routes are imported with.

! The value is not processed by OSPF itself.

Connected

The redistribution of routes that are automatically set by the operating system is configured under **Static**.



OSPF instance

Contains the name of the OSPF instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

! In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

External route tag

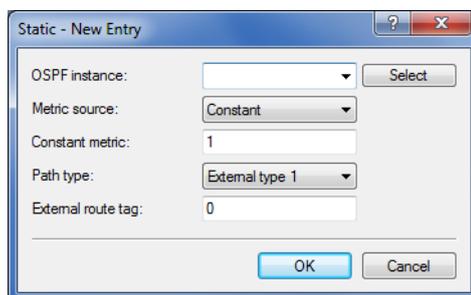
Specifies which external route tag the routes are imported with.



The value is not processed by OSPF itself.

Static

The redistribution of static routes, i.e. routes that the user manually enters into the routing table, is configured under **Static**.

**OSPF instance**

Contains the name of the OSPF instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.



In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

External route tag

Specifies which external route tag the routes are imported with.



The value is not processed by OSPF itself.

4.1.2 Show commands via CLI

The the available show commands are listed in the following:

> **show ospf-config**

Displays a summary of the configured OSPF instances.

> **show ospf-database**

Displays the OSPF database.

> **show ospf-graph**

Displays the OSPF areas as a graphical representation in Graphviz format.

> **show ospf-neighbor**

Displays information about OSPF neighbors.

> **show ospf-rib**

Displays information about the OSPF Routing Information Base.

4.1.3 Additions to the Setup menu

OSPF

This directory enables you to configure the device for the Open Shortest Path First protocol.

SNMP ID:

2.93.3.

Telnet path:

Setup > Routing-Protocols

OSPF instance

This table is used to configure the OSPF instances.

SNMP ID:

2.93.3.1

Telnet path:

Setup > Routing-Protocols > OSPF

Name

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.1.1

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Instance

Possible values:

Characters from the following character set [A-Z a-z 0-9 @{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

Activate OSPF instance

Activates or deactivates this OSPF instance

SNMP ID:

2.93.3.1.2

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Instance

Possible values:

0
Disabled
1
Activated

Default:

0

Router ID

The 32-bit router ID of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

SNMP ID:

2.93.3.1.3

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Instance

Possible values:

IPv4 address [0-9 .]

Default:

0.0.0.0

Routing tag

Contains the routing tag assigned to this instance.

SNMP ID:

2.93.3.1.4

Telnet path:**Setup > Routing-Protocols > OSPF > OSPF-Instance****Possible values:**

0 ... 65535

Advertise default route

Specifies whether this router should advertise or propagate the default route in this instance.

SNMP ID:

2.93.3.1.5

Telnet path:**Setup > Routing-Protocols > OSPF > OSPF-Instance****Possible values:****No**

The router does not advertise a default route.

Yes

The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

Default:

No

OSPF areas

This table is used to configure the OSPF areas.

SNMP ID:

2.93.3.2

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.2.1

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Areas

Possible values:

Characters from the following character set [A-Z a-z 0-9
@{ }~!\$%'()+- , / : ; ? [\] ^ _ . & < = >]

Area ID

The area ID (displayed as an IPv4 address) identifies the area.

SNMP ID:

2.93.3.2.2

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Areas

Possible values:

IPv4 address [0-9.]

Special values:

0.0.0.0

Designates this instance as the backbone area.

Area type

This parameter describes the type of the area.

SNMP ID:

2.93.3.2.3

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Areas

Possible values:

Normal
Stub

Default:

Normal

Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

SNMP ID:

2.93.3.2.4

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Areas

Possible values:

0 ... 4294967295

Area address aggregation

This table is used to configure the area address aggregation.

SNMP ID:

2.93.3.3

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.3.1

Telnet path:

Setup > Routing-Protocols > OSPF > Area-Address-Aggregation

Possible values:

Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

Area ID

Contains the ID of the area.

SNMP ID:

2.93.3.3.2

Telnet path:

Setup > Routing-Protocols > OSPF > Area-Address-Aggregation

Possible values:

IPv4 address [0–9 .]

Default:

0.0.0.0

IP address

This parameter contains the IPv4 address.

SNMP ID:

2.93.3.3.3

Telnet path:

Setup > Routing-Protocols > OSPF > Area-Address-Aggregation

Possible values:

IPv4 address [0–9 .]

Default:

0.0.0.0

IP netmask

This parameter contains the IPv4 subnet mask.

SNMP ID:

2.93.3.3.4

Telnet path:

Setup > Routing-Protocols > OSPF > Area-Address-Aggregation

Possible values:

IPv4 netmask [0–9 .]

Advertise

Enables or disables the advertisement of this address aggregation.

SNMP ID:

2.93.3.3.5

Telnet path:

Setup > Routing-Protocols > OSPF > Area-Address-Aggregation

Possible values:**No**

Advertising disabled

Yes

Advertising enabled

Default:

No

OSPF interfaces

Specifies the interfaces on which OSPF is operated.

SNMP ID:

2.93.3.4

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.4.1

Telnet path:

Setup > Routing-Protocols > OSPF > OSPF-Interfaces

Possible values:

Characters from the following character set: [a-z A-Z 0-9 .]

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.4.2

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]**Area ID**

Contains the ID of the area.

SNMP ID:

2.93.3.4.3

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

IPv4 address [0-9.]

Default:

0.0.0.0

Interface type

Contains the interface type.

SNMP ID:

2.93.3.4.4

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:****Broadcast**

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

Non-Broadcast Multi- Access (NBMA)

Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication. All neighbors must be configured manually.

Default:

Broadcast

Output cost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

SNMP ID:

2.93.3.4.5

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 4294967295

Retransmit interval

Contains the number of seconds between retransmissions.

SNMP ID:

2.93.3.4.6

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 4294967295

Transmit delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

SNMP ID:

2.93.3.4.7

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 4294967295

Router priority

The priority of this router on this interface when it is set as default router (DR). The router with the highest priority is set as the default router.

SNMP ID:

2.93.3.4.8

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 255

Special values:**0**

The value 0 prevents the router from becoming default router on this interface.

Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

SNMP ID:

2.93.3.4.9

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 4294967295

Router Dead Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.



This value must be greater than the Hello interval.

SNMP ID:

2.93.3.4.10

Telnet path:**Setup > Routing-Protocols > OSPF > Interfaces****Possible values:**

0 ... 4294967295

Authentication type

Authentication method used for this interface.

SNMP ID:

2.93.3.4.11

Telnet path:

Setup > Routing-Protocols > OSPF > Interfaces

Possible values:

Null
Simple password
Cryptographic MD5

Default:

Null

Authentication key

Authentication key for this network in the case that the authentication type **Null** is used.

SNMP ID:

2.93.3.4.12

Telnet path:

Setup > Routing-Protocols > OSPF > Interfaces

Possible values:

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

Passive

Defines whether OSPF works actively or passively on this interface.

SNMP ID:

2.93.3.4.13

Telnet path:

Setup > Routing-Protocols > OSPF > Interfaces

Possible values:**No****Yes**

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

Default:

No

MTU ignore

Disables the MTU value check in database description packets. This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

SNMP ID:

2.93.3.4.14

Telnet path:**Possible values:****No****Yes****Default:**

No

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

SNMP ID:

2.93.3.5

Telnet path:**Setup > Routing-Protocols > OSPF****OSPF instance**

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.5.1

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]**Transit area ID**

Defines the area ID of the transit area.

SNMP ID:

2.93.3.5.2

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**

IPv4 address [0-9.]

Default:

0.0.0.0

Router ID

Defines the router ID of the router at the remote end of the virtual link.

SNMP ID:

2.93.3.5.3

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**

IPv4 address [0-9.]

Default:

0.0.0.0

Retransmit interval

Contains the number of seconds between retransmissions.

SNMP ID:

2.93.3.5.4

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**

0 ... 4294967295

Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

SNMP ID:

2.93.3.5.5

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**

0 ... 4294967295

Router Dead Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.



This value must be greater than the Hello interval.

SNMP ID:

2.93.3.5.6

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**

0 ... 4294967295

Authentication type

Authentication method used for this interface.

SNMP ID:

2.93.3.5.7

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:****Null**
Simple password
Cryptographic MD5**Default:**

Null

Authentication keyAuthentication key for this network in the case that the authentication type **Null** is used.**SNMP ID:**

2.93.3.5.8

Telnet path:**Setup > Routing-Protocols > OSPF > Virtual-Links****Possible values:**16 characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () # * + - , / : ; ? [\] ^ _ . & < = >]**NBMA neighbors**The neighbors of your non-broadcast multi-access network are configured in the **NBMA neighbors** menu.

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.



The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

SNMP ID:

2.93.3.6

Telnet path:**Setup > Routing-Protocols > OSPF****OSPF instance**

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.6.1

Telnet path:**Setup > Routing-Protocols > OSPF > NBMA-Neighbors****Possible values:**Characters from the following character set [A-Z a-z 0-9
@{ } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]**OSPF interface**

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.6.2

Telnet path:**Setup > Routing-Protocols > OSPF > NBMA-Neighbors****Possible values:**

Characters from the following character set: [a-z A-Z 0-9 .]

IP address

Contains the IPv4 address of the neighbor router at the remote end.

SNMP ID:

2.93.3.6.3

Telnet path:**Setup > Routing-Protocols > OSPF > NBMA-Neighbors****Possible values:**

IPv4 address [0-9 .]

Default:

0.0.0.0

Request interval

Defines the interval in which Hello messages are sent to this router.

SNMP ID:

2.93.3.6.4

Telnet path:

Setup > Routing-Protocols > OSPF > NBMA-Neighbors

Possible values:

0 ... 4294967295

Special values:

0

Disables the transmission of Hello messages.

Eligible as default router

Specifies whether the local device itself is selectable as default router.

SNMP ID:

2.93.3.6.5

Telnet path:

Setup > Routing-Protocols > OSPF > NBMA-Neighbors

Possible values:

No
Yes

Default:

No

Point-to-multipoint neighbors

This table is used to configure your point-to-multipoint neighbors.

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network.



If no default router is selected, multicast is used for communications instead.

SNMP ID:

2.93.3.7

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.7.1

Telnet path:**Setup > Routing-Protocols > OSPF > Point-to-MultiPoint-Neighbors****Possible values:**

16 characters from the following character set [A-Z a-z 0-9 @{ } ~ ! \$ % ' () # * + - , / : ; ? [\] ^ _ . & < = >]

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.7.2

Telnet path:**Setup > Routing-Protocols > OSPF > Point-to-MultiPoint-Neighbors****Possible values:**

Characters from the following character set: [a-z A-Z 0-9 .]

IP address

Contains the IPv4 address of the neighbor router at the remote end.

SNMP ID:

2.93.3.7.3

Telnet path:**Setup > Routing-Protocols > OSPF > Point-to-MultiPoint-Neighbors****Possible values:**

IPv4 address [0-9 .]

Default:

0.0.0.0

Request interval

Defines the interval in which Hello messages are sent to this router.

SNMP ID:

2.93.3.7.4

Telnet path:

Setup > Routing-Protocols > OSPF > Point-to-MultiPoint-Neighbors

Possible values:

0 ... 4294967295

Special values:

0

Disables the transmission of Hello messages.

BGP

in the **BGP** menu you configure the redistribution of routes that were learned dynamically from the Border Gateway Protocol.

SNMP ID:

2.93.3.8

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.8.1

Telnet path:

Setup > Routing-Protocols > OSPF > BGP

Possible values:

Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

BGP instance

Contains the name of the BGP instance.

SNMP ID:

2.93.3.8.2

Telnet path:

Routing-Protocols > OSPF > BGP

Possible values:

Characters from the following character set [A-Z a-z 0-9
@{|}~!\$%'()+- , / : ; ? [\] ^ _ . & < = >]

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.8.3

Telnet path:

Routing-Protocols > OSPF > BGP

Possible values:**Constant**

Uses a user-defined constant metric.

Protocol

Uses the "local preference" value of the BGP prefix.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.

 The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.8.4

Telnet path:

Routing-Protocols > OSPF > BGP

Possible values:

0 ... 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.8.5

Telnet path:**Routing-Protocols > OSPF > BGP****Possible values:****External type 1**

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.



The value is not processed by OSPF itself.

SNMP ID:

2.93.3.8.6

Telnet path:**Routing-Protocols > OSPF > BGP****Possible values:**

0 ... 4294967295

Connected

Routes that are automatically entered into the routing table by the operating system are configured under **Connected**.

SNMP ID:

2.93.3.9

Telnet path:**Setup > Routing-Protocols > OSPF****OSPF instance**

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.9.1

Telnet path:**Setup > Routing-Protocols > OSPF > Connected****Possible values:**

Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.9.2

Telnet path:**Setup > Routing-Protocols > OSPF > Connected****Possible values:****Constant**

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.



The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.9.3

Telnet path:**Setup > Routing-Protocols > OSPF > Connected****Possible values:**

0 ... 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.9.4

Telnet path:

Setup > Routing-Protocols > OSPF > Connected

Possible values:**External type 1**

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.



The value is not processed by OSPF itself.

SNMP ID:

2.93.3.9.5

Telnet path:

Setup > Routing-Protocols > OSPF > Connected

Possible values:

0 ... 4294967295

Static

Routes that the user manually enters into the routing table are configured in the menu **Static**.

SNMP ID:

2.93.3.10

Telnet path:

Setup > Routing-Protocols > OSPF

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.10.1

Telnet path:

Setup > Routing-Protocols > OSPF > Static

Possible values:

Characters from the following character set [A-Z a-z 0-9 @{ }~!\$%'()+- , / : ; ? [\] ^ _ . & < = >]

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.10.2

Telnet path:

Setup > Routing-Protocols > OSPF > Static

Possible values:**Constant**

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.

 The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.10.3

Telnet path:

Setup > Routing-Protocols > OSPF > Static

Possible values:

0 ... 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.10.4

Telnet path:**Setup > Routing-Protocols > OSPF > Static****Possible values:****External type 1**

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.



The value is not processed by OSPF itself.

SNMP ID:

2.93.3.10.5

Telnet path:**Setup > Routing-Protocols > OSPF > Static****Possible values:**

0 ... 4294967295

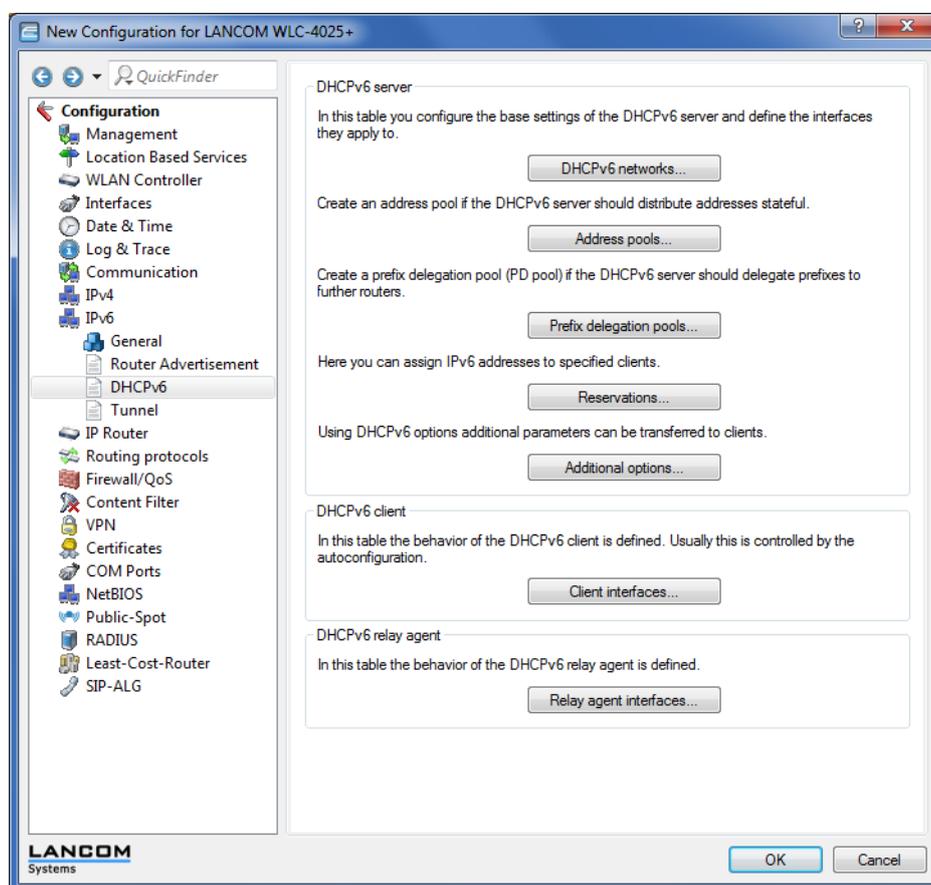
5 IPv6

5.1 Support for SNTP option in the DHCPv6 client

From LCOS version 10.12, the DHCPv6 client is able to request a list of SNTP (Simple Network Time Protocol) servers from the DHCPv6 server.

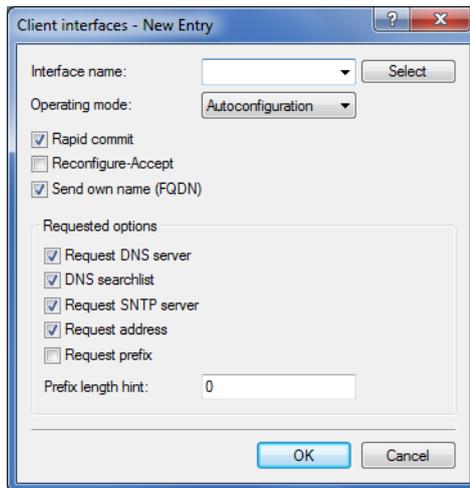
5.1.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.
2. Navigate to **IPv6 > DHCPv6 > DHCPv6 server**.



3. Click the button **Client interfaces**.

- Click the button **Add** to create a new entry or **Edit** to modify an existing entry.



- Activate **Request SNTP server** in order to enable the new SNTP feature.

5.1.2 Additions to the Setup menu

Request SNTP

Specify whether the DHCPv6 client requests a list of SNTP (Simple Network Time Protocol) servers from the DHCPv6 server.

 This requires regular synchronization with a timeserver.

SNMP ID:

2.70.3.2.1.10

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List

Possible values:

0
No
1
Yes

Default:

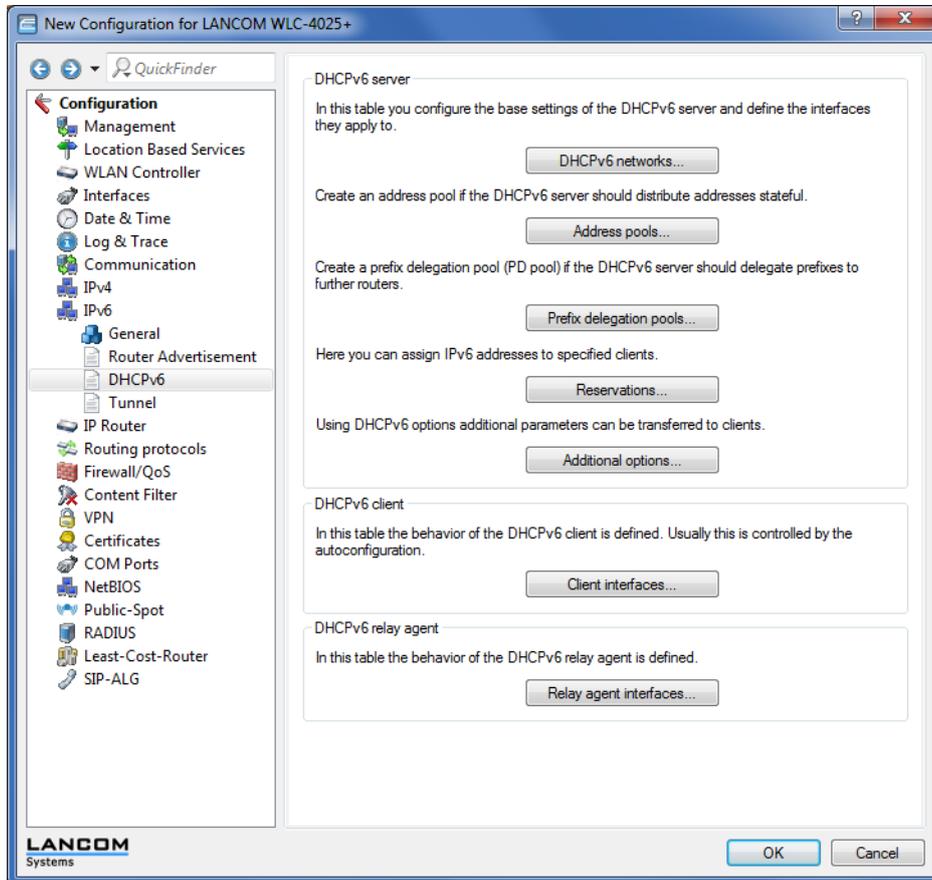
0

5.2 Support of prefix hint in the DHCPv6 client

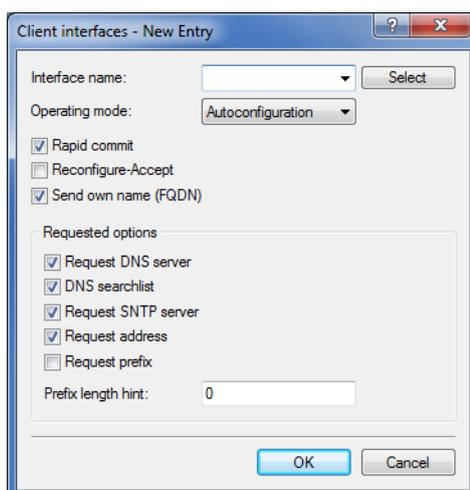
As of LCOS version 10.12, the DHCPv6 client can request the DHCPv6 server for the necessary prefix length, e.g. 56 or 48 bits. The server can then assign the prefix to the client with the required length.

5.2.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.
2. Navigate to **IPv6 > DHCPv6 > DHCPv6 server**.



3. Click the button **Client interfaces**.
4. Click the button **Add** to create a new entry or **Edit** to modify an existing entry.



5. Enter the required prefix length into the input field **Prefix length hint**.

! In order to send the desired prefix length to the DHCPv6 server, you must first enable Request prefix. Enter a three-digit number.

5.2.2 Additions to the Setup menu

PD hint

Here you specify whether the DHCPv6 client requests a desired prefix length from the DHCPv6 server.

SNMP ID:

2.70.3.2.1.11

Telnet path:

Setup > IPv6 > DHCPv6 > Client > Interface-List

Possible values:

Three characters from the following character set: [0-9]

5.3 Transmitting the IPv6 LAN prefix with the action table

The action table offers two new variables as of LCOS version 10.12.

A number of dynamic DNS providers, such as feste-ip.net and dynv6.com, are able to form fully-fledged Global Unicast Addresses (GUAs), which are accessible from the Internet, by combining the IPv6 LAN prefix transmitted by the router and the host identifiers of the LAN clients that are known to the provider. All the provider has to do is to append the host identifier to the transmitted LAN prefix. This GUA is then available from the provider as a AAAA record in the DNS. This allows you to make your IPv6-enabled LAN devices available at a fixed host name from anywhere in the world, even if the IPv6 prefix changes after a forced re-connection.



In order for the LAN clients to be accessible from the outside, the IPv6 firewall of the LANCOM router needs to be configured with the appropriate exceptions. By default, no connections are permitted from the outside to the LAN.

Table 1: The following variables are available for use in the action table:

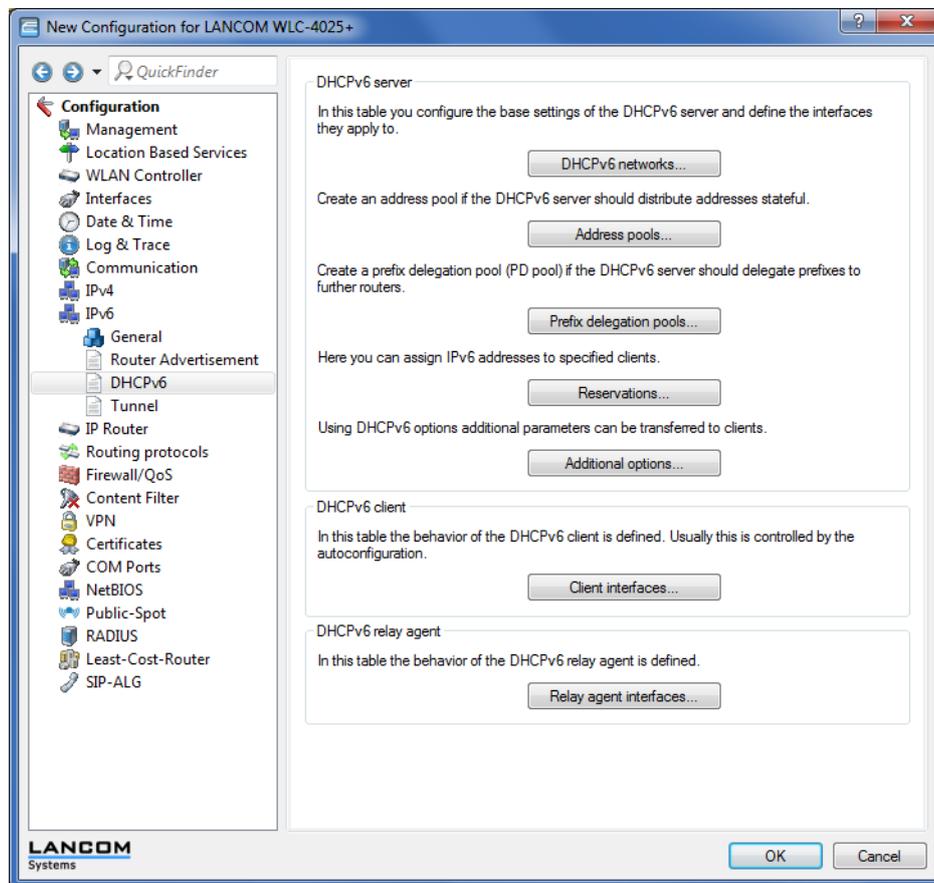
Variable	Meaning
%x	The current IPv6 LAN prefix as a string in the format "fd00:0:0:1::/64"
%y	The current IPv6 LAN address of the device as a string in the format "fd00::1:2a0:57ff:fa1b:9d7b"

5.4 DHCPv6 options

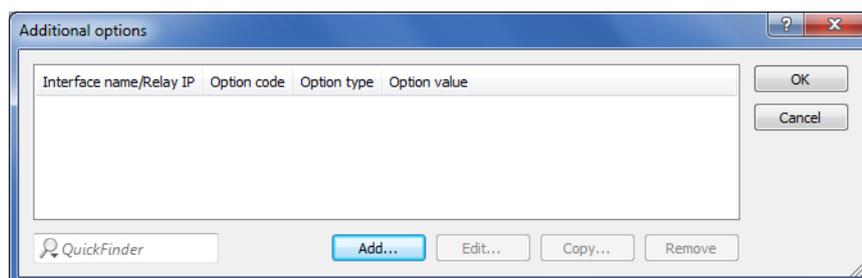
As of LCOS version 10.12, the DHCPv6 server is able to assign DHCPv6 options to its DHCPv6 clients.

5.4.1 Configuration by LANconfig

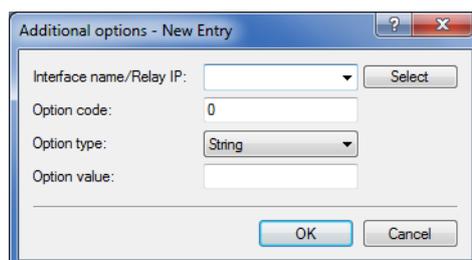
1. Navigate to the configuration menu **IPv6 > DHCPv6 > DHCPv6 server**.



2. Click the button **Additional options**.



3. Click on **Edit** or **Add** as necessary.



4. From the selection list **Interface name/Relay IP**, select the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option.

 Note: In order for this option to be delivered to clients, the request sent by a client must also contain the corresponding option code.

5. Enter the code of the DHCPv6 option into the **Option code** input box.
6. Use the selection list **Option type** to set the type of the DHCPv6 option.

 A number of types are available here:

- > **String**: Accepts the characters as a string.
- > All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.
- > **Integer types** are decimal, octal with a leading 0, and hexadecimal with a leading 0x; capitalization is ignored. The value range for Integer8 is from -128 to 127; for Integer16 from -32768 to 32767; and for Integer32 from -2147483648 to 2147483647. A leading + or - sign is generally allowed.
- > **IPv6Address** accepts IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses (e.g., ::ffff:1.2.3.4).
- > **Domain-List** accepts all strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain always ends with the empty label 0.
- > **Hexdump** expects each block to have hex numbers only, without a leading 0x. It fills each block with a leading 0 for an even length and ends with the block **bigendian**.

7. The input field **Option value** is for the content of the DHCPv6 option, formatted according to the option type.
8. To accept the configuration, click the button **OK**.

5.4.2 Additions to the Setup menu

Additional options

This is the **Additional options** table for the DHCP server.

 In order for this option to be delivered to clients, the request sent by a client must contain the corresponding option code.

SNMP ID:

2.70.3.1.8

Telnet path:

Setup > IPv6 > DHCPv6 > Server

Interface-Name-or-Relay

Here you choose the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option

SNMP ID:

2.70.3.1.8.1

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Additional-Options

Possible values:

Characters from the following character set:

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

Option code

Enter the code of your DHCPv6 option here.

SNMP ID:

2.70.3.1.8.2

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Additional-Options

Possible values:

0 ... 65535

Default:

0

Option type

Select the type of your DHCPv6 option here.

SNMP ID:

2.70.3.1.8.3

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Additional-Options

Possible values:**String**

The characters are accepted as a string. Please note: All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.

Integer8

An 8-bit integer from -128 to 127 optionally decimal, octal with prefix '0', or hexadecimal with prefix '0x'.

Integer16

A 16-bit integer from -32768 to 32767.

Integer32

A 32-bit integer from -2147483648 to 2147483647.

IPv6 address

IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses, such as ::ffff:1.2.3.4.

Domain list

All strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain always ends with the empty label 0.

Hexdump

Expects each block to have hex numbers only, without a leading 0x. Each block is filled with a leading 0 for an even length. The block is taken as **bigendian**.

Option value

Enter the contents of your DHCPv6 option here. The content must be formatted according to the selected option type.

SNMP ID:

2.70.3.1.8.4

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Additional-Options

Possible values:

Depending on the option type, characters from:

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

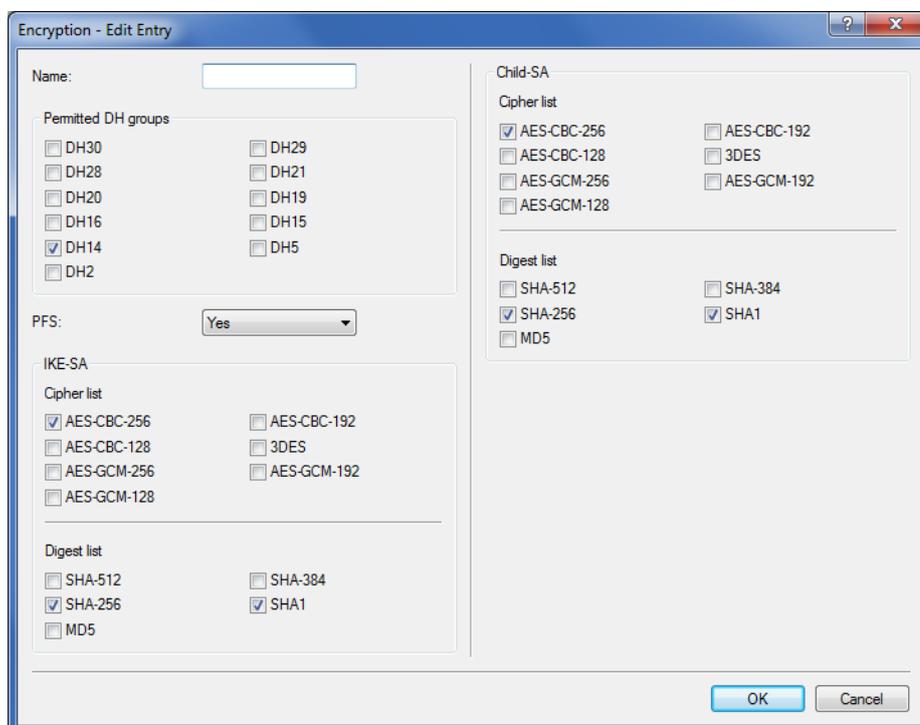
6 Virtual Private Networks - VPN

6.1 Addition to the IKEv2 encryption algorithms

As of LCOS version 10.12, an additional encryption algorithm is supported: GCM (Galois/Counter Mode).

This algorithm is particularly efficient and provides a noticeable increase in performance.

Also, new groups are available for the Diffie-Hellmann key exchange, namely DH-19 to DH-21 as per RFC5903 as well as DH-28 to DH-30 as per RFC 6954.



The new groups for the Diffie-Hellmann key exchange:

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

Variants of the newly added Galois/Counter Mode encryption algorithm:

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

6.1.1 Additions to the Setup menu

DH-Groups

Contains the selection of Diffie-Hellman groups.

SNMP ID:

2.19.36.2.2

Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

DH30

(as of LCOS version 10.12)

DH29

(as of LCOS version 10.12)

DH28

(as of LCOS version 10.12)

DH21

(as of LCOS version 10.12)

DH20

(as of LCOS version 10.12)

DH19

(as of LCOS version 10.12)

DH16

DH15

DH14

DH5

DH2

Default:

DH14

IKE-SA cipher list

Specifies which encryption algorithms are enabled. As of version 10.12, LCOS also supports AES-GCM (Galois/Counter Mode).

SNMP ID:

2.19.36.2.4

Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(as of LCOS version 10.12)
AES-GCM-192
(as of LCOS version 10.12)
AES-GCM-128
(as of LCOS version 10.12)

Default:

AES-CBC-256

AES-GCM-256

Child-SA cipher list

Specifies which encryption algorithms are enabled in the Child-SA. As of version 10.12, LCOS also supports AES-GCM (Galois/Counter Mode).

SNMP ID:

2.19.36.2.6

Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(as of LCOS version 10.12)
AES-GCM-192
(as of LCOS version 10.12)
AES-GCM-128
(as of LCOS version 10.12)

Default:

AES-CBC-256

AES-GCM-256

6.2 IKEv2 load balancer

LCOS version 10.12 saw the introduction of the IKEv2 load balancer. This allows the operation of any number of VPN nodes while balancing the number of incoming VPN connections according to their load.

The IKEv2 load balancer allows the distribution of incoming IKEv2 connections to other gateways depending on the current load or number of VPN tunnels. The IKEv2 redirect mechanism is used to achieve this.

Larger-scale VPN scenarios generally operate with redundant VPN gateways. Often, the gateways are not used evenly, and some gateways are reserved for backup events. The result is a non-uniform resource load across the installation.

With multiple VPN gateways in operation, all of them need to be configured on all of the clients. Particularly when a new VPN gateway is installed, it has to be subsequently configured on all of the clients. With the redirect mechanism (RFC 5685), IKEv2 offers an enhancement that enables a VPN gateway to redirect a client to another gateway.

The IKEv2 redirect mechanism in combination with VRRP provides a highly available IKEv2 load balancer that is suitable for enterprise scenarios.

In the first step, a VRRP group is activated on all participating VPN gateways. The virtual VRRP IP address is at the same time the master IP address of the IKEv2 load balancer cluster. The VPN gateways now exchange information about their load and their availability by means of regular status messages via multicast. If the master goes down, another VPN gateway is automatically set as the master.

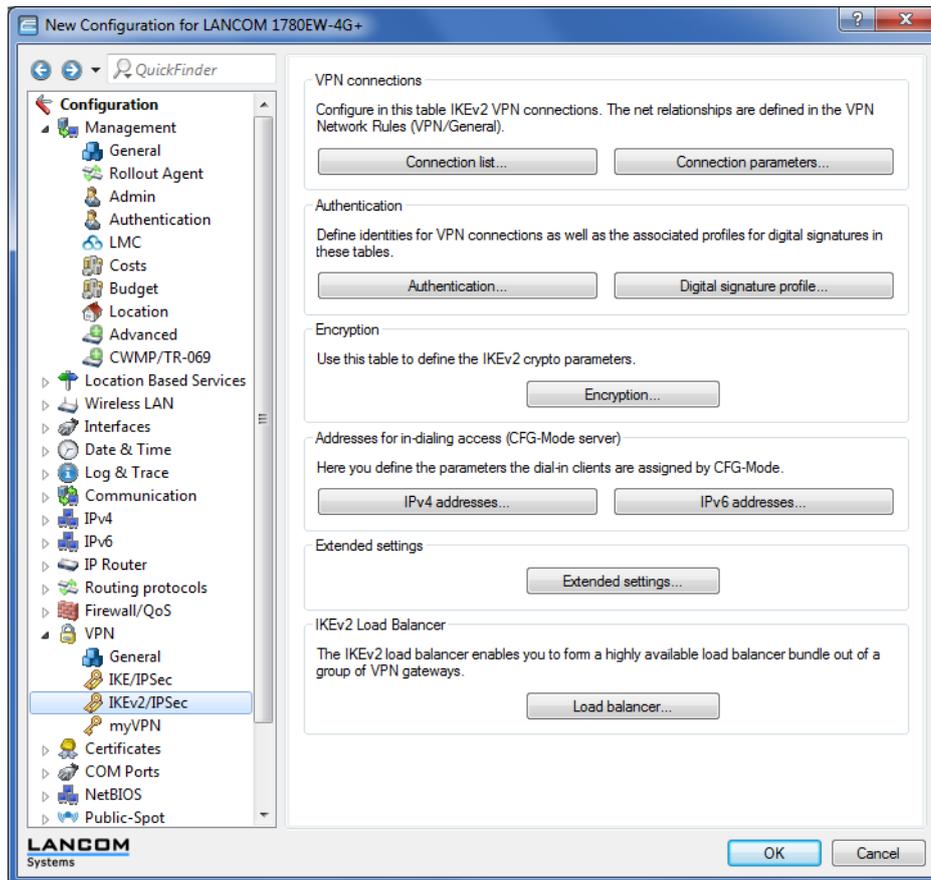
The only information the clients need is the master IP address. If a client establishes a VPN connection to this IP address, the master gateway checks the load of the VPN gateways and redirects the client to the gateway with the least load. The master gateway sends a redirect either in the IKE_SA_INIT response or in the IKE Auth phase. The redirect depends on the availability of free VPN tunnels of the participating gateways. The VPN client is directed to the VPN gateway with the lowest number of active tunnels.

The virtual gateway address is only used for the initial contact before the subsequent redirect. The client then establishes the actual VPN tunnel to a different gateway address.

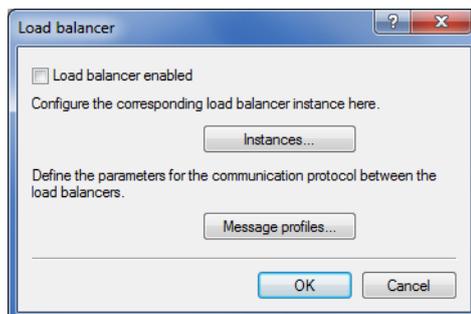
The following limiting conditions must be observed:

- > VRRP is required for the automatic selection of the master gateway.
- > The VPN gateways involved must have a common layer-2 connection for the VRRP and the exchange of status messages via multicast.
- > VRRP is currently supported on LAN interfaces only.
- > An upstream router (redundant, if necessary) is required for WAN access.
- > The client must support IKEv2 gateway redirect as per RFC 5685 (currently applies to LANCOM routers and the LANCOM Advanced VPN Client on Windows).

In **LANconfig** you configure the IKEv2 load balancer under **VPN > IKEv2/IPSec > IKEv2 load balancer**



in the menu **Load balancer**,



Load balancer enabled

activates the IKEv2 load balancer.

6.2.1 Instances

Load balancer instances are configured in the **Instances** table.

VRRP-ID

VRRP-ID (router ID) to be used for this IKEv2 load balancer instance. VRRP must be activated on this device and configured for this VRRP ID.

Possible values:

0 to 255

Default: 1

Local IPv4 redirect target

IPv4 address or FQDN on which the device is to receive VPN tunnels. A VPN client is forwarded to this address by the master in the load-balancer cluster.

 This is not the virtual VRRP-IP address.

Message profile

Message profile to use for this instance. The message profile contains the parameters for the status log used by the device to communicate its status information to the load balancer cluster.

Default: DEFAULT.

Redirection mode

Specifies at which phase of the IKEv2 negotiation the VPN gateway redirects clients to another gateway.

 This parameter only takes effect if the device is VRRP master.

Possible values:

IKEv2-Init (default)

The redirect message is sent in the IKE_SA_INIT response from the VPN gateway.

IKEv2-Auth

The redirect message is sent in the IKE_AUTH phase after the client has identified itself to the VPN gateway.

Redirection destinations

Specifies the destination to which the VPN client is redirected.

 The parameter only takes effect if the device is VRRP master.

Possible values:

Local or remote

Clients are redirected to the device's own IP address and also to other remote gateways in the cluster.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed between all gateways except for the master gateway.



This can be used to configure scenarios in which the load balancer master only distributes the clients, but does not terminate any VPN tunnels itself.

Comment

Enter a descriptive comment for this entry.

6.2.2 Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.

Name

Unique name for this profile

Interface

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

Possible values:

Entries from the IPv4 networks table**IP address**

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

Default: 239.255.22.11

Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

Default: 1987

Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

Possible values:

0 to 65535

Default: 500

Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.



The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

Possible values:

0 to 65535

Default: 3000

Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

Possible values:

1 to 9

Default: 5

0

Disables the replay detection.

Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

Possible values:

0 to 255

Default: 15

Secret

Shared secret for the load balancer communication log.



The secret must be the same on all of the VPN gateways in a cluster.

Possible values:

Up to 32 random characters

Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None (default)

AES-128-GCM

AES-192-GCM

AES-256-GCM

HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None

96 bits (default)

128 bits

Comment

Enter a descriptive comment for this entry.

6.2.3 Show commands via CLI

`show vlb-status`: Displays the status of the individual gateways in the cluster.

6.2.4 Trace commands

The available trace commands are listed in the following:

- > VLB-Status
- > VLB-Packet

6.2.5 Additions to the Setup menu

IKEv2 load balancer

Configures the IKEv2 load balancer.

SNMP ID:

2.19.50

Telnet path:

Setup > VPN

Operating

Activates/deactivates the IKEv2 load balancer.

SNMP ID:

2.19.50.1

Telnet path:**Setup > VPN > IKEv2 Load Balancer****Possible values:****Yes**

Activates the IKEv2 load balancer.

No

Deactivates the IKEv2 load balancer.

Default:

No

InstancesLoad balancer instances are configured in the **Instances** table.**SNMP ID:**

2.19.50.2

Telnet path:**Setup > VPN > IKEv2 Load Balancer****VRRP-ID**

VRRP-ID (router ID) to be used for this IKEv2 load balancer instance. VRRP must be activated on this device and configured for this VRRP ID.

SNMP ID:

2.19.50.2.1

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Possible values:**

0 ... 255

Default:

1

Local IPv4 redirect target

IPv4 address or FQDN on which the device is to receive VPN tunnels. A VPN client is forwarded to this address by the master in the load-balancer cluster.

 This is not the virtual VRRP-IP address.

SNMP ID:

2.19.50.2.2

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Message profile**

Message profile to use for this instance. The message profile contains the parameters for the status log used by the device to communicate its status information to the load balancer cluster.

SNMP ID:

2.19.50.2.4

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Possible values:**

Characters from the following character set [A-Z a-z 0-9
@{|}~!\$%'()+-./:;?[\]^_.<=>]

Default:

DEFAULT

Redirection mode

Specifies at which phase of the IKEv2 negotiation the VPN gateway redirects clients to another gateway.

 This parameter only takes effect if the device is VRRP master.

SNMP ID:

2.19.50.2.5

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Possible values:****IKEv2-Init**

The redirect message is sent in the IKE_SA_INIT response from the VPN gateway.

IKEv2-Auth

The redirect message is sent in the IKE_AUTH phase after the client has identified itself to the VPN gateway.

Default:

IKEv2-Init

Redirection destinations

Specifies the destination to which the VPN client is redirected.

 The parameter only takes effect if the device is VRRP master.

 This can be used to configure scenarios in which the load balancer master only distributes the clients, but does not terminate any VPN tunnels itself.

SNMP ID:

2.19.50.2.6

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Possible values:****Local or remote**

Clients are redirected to the device's own IP address and also to other remote gateways in the cluster.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed between all gateways except for the master gateway.

Comment

Contains a comment about this instance.

SNMP ID:

2.19.50.2.7

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Instances****Possible values:**

Characters from the following character set [A-Z a-z 0-9 @ { | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.

SNMP ID:

2.19.50.3

Telnet path:**Setup > VPN > IKEv2 Load Balancer****Name**

Unique name for this profile

SNMP ID:

2.19.50.3.1

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Message-Profiles****Possible values:**Characters from the following character set [A-Z a-z 0-9
@{ } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]**Interface**

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

SNMP ID:

2.19.50.3.2

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Message-Profiles****Possible values:****Entries from the IPv4 networks table****IP address**

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

SNMP ID:

2.19.50.3.3

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Message-Profiles****Possible values:**

IPv4 address [0-9.]

Default:

239.255.22.11

Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

SNMP ID:

2.19.50.3.4

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Message-Profiles****Possible values:**

0 ... 65535

Default:

1987

Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

SNMP ID:

2.19.50.3.5

Telnet path:**Setup > VPN > IKEv2 Load Balancer > Message-Profiles****Possible values:**

0 ... 65535

Default:

500

Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.



The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

SNMP ID:

2.19.50.3.6

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

0 ... 65535

Default:

3000

Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

SNMP ID:

2.19.50.3.7

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

0 ... 9

Default:

5

Special values:

0

Disables the replay detection.

Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

SNMP ID:

2.19.50.3.8

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

0 ... 255

Default:

15

Key

Shared secret for the load balancer communication log.

 The secret must be the same on all of the VPN gateways in a cluster.

SNMP ID:

2.19.50.3.9

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

32 characters from the following character set [A-Z a-z 0-9 @{|}~!\$%'()+-, /: ;? [\] ^ _ . & < = >]

Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

SNMP ID:

2.19.50.3.10

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

None
AES-128-GCM
AES-192-GCM
AES-256-GCM

Default:

None

HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

SNMP ID:

2.19.50.3.11

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Message-Profiles

Possible values:

None
96 bits
128 bits

Default:

96 bits

Comment

Contains a comment about this message profile.

SNMP ID:

2.19.50.3.12

Telnet path:

Setup > VPN > IKEv2 Load Balancer > Instances

Possible values:

Characters from the following character set [A-Z a-z 0-9
@{ | } ~ ! \$ % ' () + - , / : ; ? [\] ^ _ . & < = >]

6.3 Flexible identity comparison for PSK connections

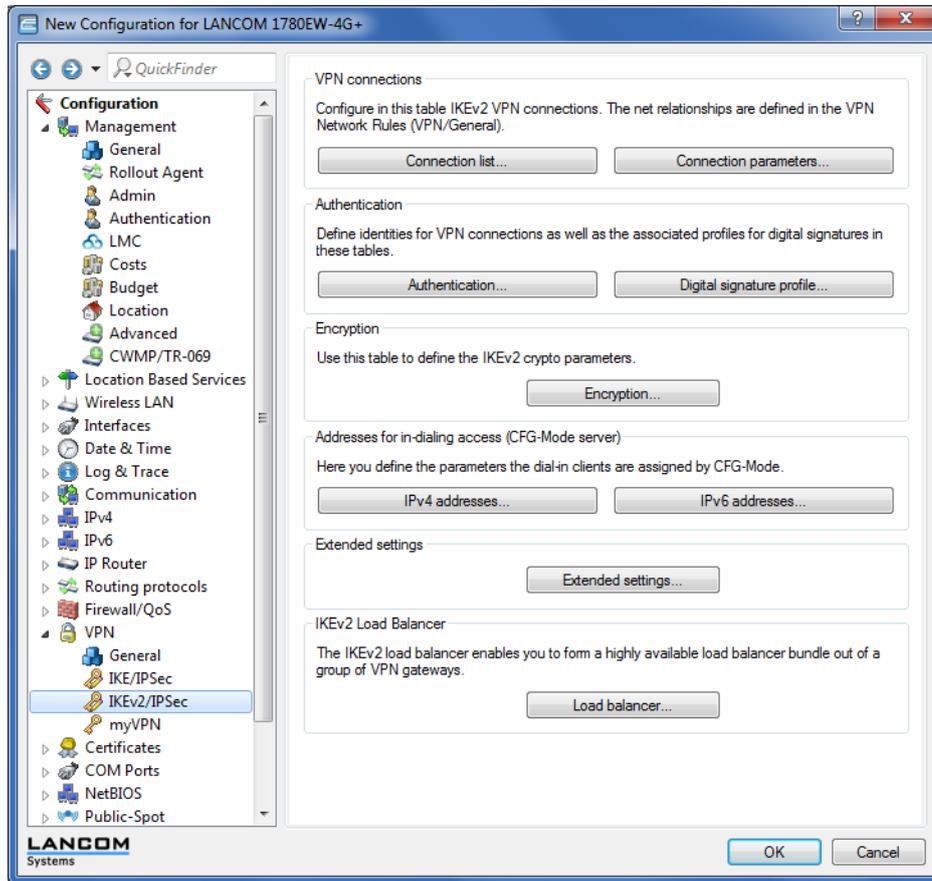
With LCOS version 10.12 the flexible identity comparison now includes PSK connections (IKEv2). Until now, identity comparison was only possible for certificate-based VPN connections (distinguished name).

 Support of "wildcard globbing" is now available for IKEv2 identities. Here '?' stands for exactly one character and '*' for any number characters, including zero.

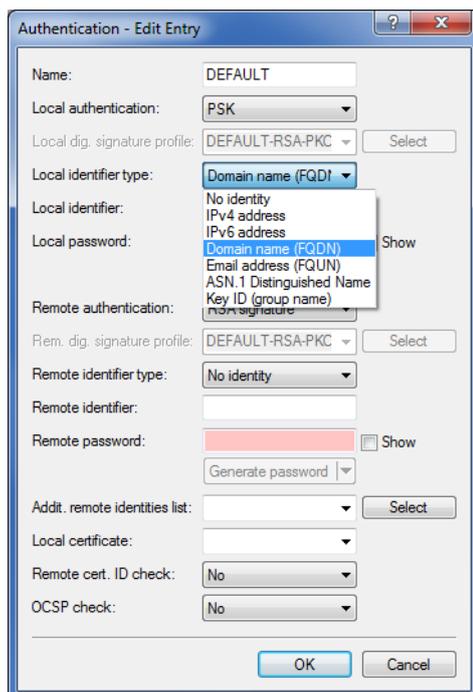
This feature makes it easier to configure your VPN, since in principle all you need for inbound IKEv2 connections is a single entry.

 The prerequisite is that all inbound connections use a particular syntax and that flexible comparison is enabled.

Flexible identity comparison is configured in **LANconfig** under **VPN > IKEv2/IPSec > Authentication** and clicking the **Authentication** button.



Flexible identity comparison for PSK connections supports the two identity types **FQUN** and **FQDN**.



ⓘ Please note that all parameters are case-sensitive.

On the command line, you can access the parameters with the path **Setup > VPN > IKEv2 > Auth > Parameter**.

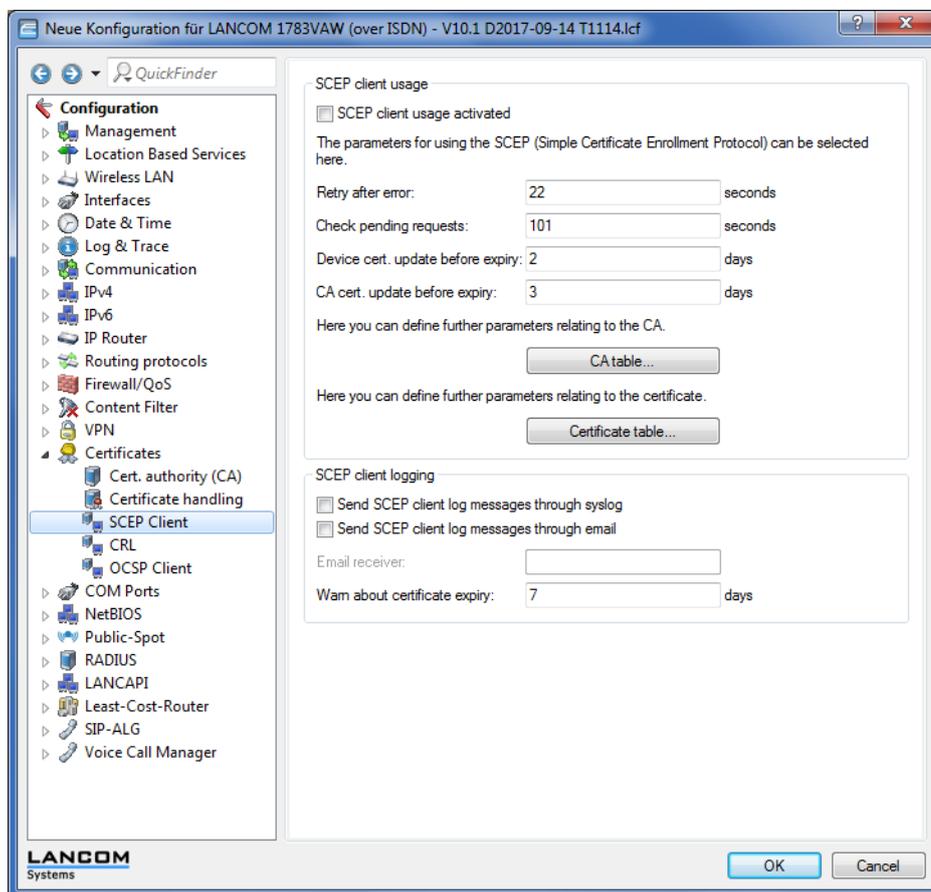
6.4 SCEP client logging

As of LCOS version 10.12 you have the option to send an e-mail or SYSLOG message informing you that the certificate has expired after an unsuccessful request for certificate renewal.

You can also issue a warning message in advance. In this way you can ensure that there is enough time to update the certificate before it expires.

6.4.1 Configuration by LANconfig

You configure the new feature under **Certificates > SCEP client > SCEP client logging**.



The new parameters:

Send SCEP client log messages through syslog

Enables/disables log message transmission via SYSLOG.

Send SCEP client log messages through email

Enables/disables log message transmission via e-mail.

 This requires that you enter an e-mail address in the corresponding input box.

Email receiver

E-mail address to receive the log message.

 To make an entry, you first have to activate the option **Send SCEP client log messages through email**.

Warn about certificate expiry

Time interval in days before certificate expiry.

7 Public Spot

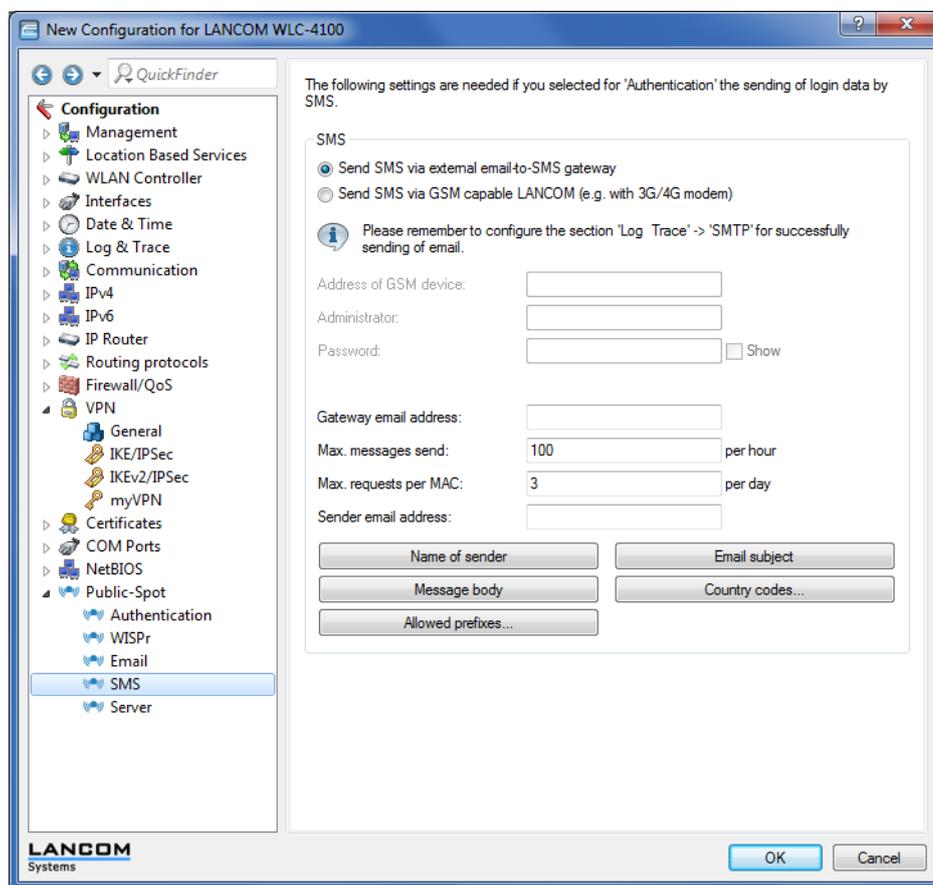
7.1 Independent user authentication (Smart Ticket)

7.1.1 Restricting the allowed country codes when using SmartTicket via SMS

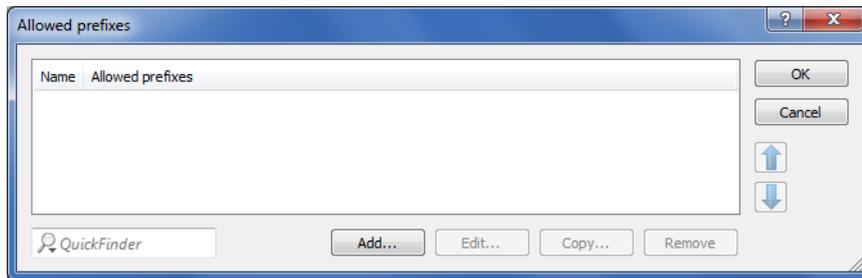
As of LCOS version 10.12 you have the option to restrict the permitted area codes for each country.

Restricting the permitted area codes prevents SMS messages from being sent to expensive premium or service call numbers.

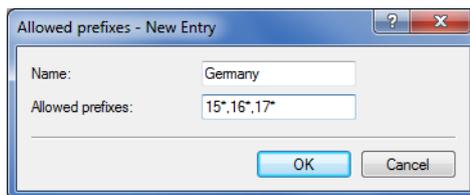
This avoids unnecessarily high costs when operating authorization by SMS.



1. Click the button **Allowed prefixes**.



2. Click **Add**.



3. Enter the name for the country into the **Name** input box.
4. You can limit the transmission of SMS text messages to certain area codes for each country by entering the permissible codes followed by a '*' into a comma-separated list. An example for German mobile phone providers: 15* , 16* , 17*.

 If you do not make an entry for a country in this table, all country codes will be allowed. Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

7.1.2 Additions to the Setup menu

Restricting the allowed country codes when using SmartTicket via SMS

In this table you specify the permitted country codes for the option SmartTicket via SMS. Each country requires an entry in the Allowed-Country-Codes table.

SNMP ID:

2.24.41.2.26

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > e-mail2Sms-Authentication

Country name

This is where you enter the name of the allowed country (e.g., Germany or DE) for which access to certain area dialing codes is to be restricted.

 Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

SNMP ID:

2.24.41.2.26.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > e-mail2Sms-Authentication > Allowed-Prefixes

Possible values:

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

Default:

Germany

8 Configuration

8.1 Importing files by copy & paste on the CLI

From LCOS version 10.12, your device supports the loading of files into file slots from the console and also by means of a script.

This offers the convenience of using a script to roll-out files together with the configuration or, for example, to import SSH keys and VPN certificates.



- > The file format must be of type text or ASCII; binary formats are not supported.
- > In the case of certificates, the file format must be PEM-encoded (ASCII/Base64). DER-encoded certificates are not supported.

Syntax of the CLI command **importfile**:

```
importfile -a <application> [-p <passphrase>] [-n] [-h <hash> -f <fingerprint>] [-c] [-r]
```

Required parameters:

-a <application>

<application> specifies the storage location and thus the usage for the entered data. For a complete list of the storage locations on your device, enter **importfile -?**.

Optional parameters:

-n

-n starts the non-interactive mode. There are no prompts or other outputs on the CLI. The non-interactive mode is intended for use with scripts.

-p <passphrase>

<passphrase> is the password required to decrypt an entered private key.

-h <hash>

The hash algorithm used to determine the fingerprint of the root CA certificate.

-f <fingerprint>

The fingerprint of the root CA certificate, created with **-h**. The fingerprint can be entered either with or without colons.

-c

Only CA certificates are uploaded.

-r

Uploaded CA certificates replace any existing ones.



CTRL+Z cancels any active input.

Example:

In this example, user input is shown in **bold** and prompts for the user are shown in *italic*. Certificates and other long, multi-line outputs are abbreviated with [...] for legibility. At the end of the example you will find explanations for the individual steps.

```
root@test:/
  importfile -a VPN2 -p lancom -h SHA512 -f
4F:A7:5E:C9:D4:77:CE:D3:06:4C:79:93:D8:FA:3A:8E:7B:FE:19:61:E2:0C:37:4F:BB:7A:E6:46:36:04:46:EE:F6:DA:97:15:6B:EB:
2D:8F:B6:66:E6:7C:54:1E:B4:02:79:54:D6:DF:1E:9B:27:7C:9C:EA:B8:CB:1B:6D:90:1C
```

The input can be aborted by pressing CTRL+Z.

Please enter the PEM-encoded (Base64) device certificate, the end of the input will be detected automatically:

```
importfile>-----BEGIN CERTIFICATE-----
importfile>MIID9DCCAtwCCQDgaoWRcmWaLjANBgkqhkiG9w0BAQ0FADAKMQswcQYDVQQG[...]
importfile>[...]s7pM510L0d0=
importfile>-----END CERTIFICATE-----
```

Importing device certificate:

```
Version: 1 (0x0)
Serial Number:
  e0:6a:85:91:0a:65:9a:2e
Signature Algorithm: sha512WithRSAEncryption
Issuer: CN=OCSP-TEST-CA,C=DE
Validity
  Not Before: Jul  4 12:34:07 2017 GMT
  Not After : Oct  5 12:34:07 2024 GMT
Subject: CN=TEST,O=Internet Widgits Pty Ltd,ST=Some-State,C=DE
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  Public-Key: (4096 bit)
  Modulus:
    00:bb:93:f6:b9:9a:41:b2:3e:30:2b:09:7f:d1:f9:
    49:54:5a:82:c9:17:10:1f:79:6d:ab:55:df:b8[...]
    [...]2f:0c:8a:69:7b:a9:82:32:f3:ca:9c:02:20:14:
    bd:8b:0d
  Exponent: 65537 (0x10001)
Signature Algorithm: sha512WithRSAEncryption
  06:5b:a4:1a:a2:69:c1:bf:6f:b1:d2:6c:b0:21:e1:10:43:[...]
  [...]50:e6:a3:1d:f3:15:b7:87:8c:65:2f:25:f6:b3:ba:4c:e6:
  5d:0b:d1:dd
```

The input can be aborted by pressing CTRL+Z.

Please enter the PEM-encoded (Base64) device private key, the end the input will be detected automatically:

```
importfile>-----BEGIN RSA PRIVATE KEY-----
importfile>Proc-Type: 4,ENCRYPTED
importfile>DEK-Info: AES-128-CBC,8FB95ED0568DA9AE17D7573BC294ACD8
importfile>[...]5Cuf2p798Obhw3isAe04XRwmdLno8ZcPDyB33ZKPjmhUzB0WsdzGdSSq5iYjD
importfile>-----END RSA PRIVATE KEY-----
```

The private key was read successfully.

The private key matches the device certificate.

The input can be aborted by pressing CTRL+Z.

Please enter the chain of PEM-encoded (Base64) CA certificates.

The input is closed with "endcachain":

```
importfile>-----BEGIN CERTIFICATE-----
importfile>MIIDGzCCAgOgAwIBAgIJAMlNxBFGQqpOMA0GCSqGSIB3DQEBDQUAMCQxCzAJB[...]
importfile>[...]EUDI9giYt9tnAT8hJfLkkyN/PHSiP+e+vopjSpKuyg==
importfile>-----END CERTIFICATE-----
importfile>endcachain
```

Importing CA certificate:

```
Version: 3 (0x2)
Serial Number:
  c9:4d:c4:11:46:42:aa:68
Signature Algorithm: sha512WithRSAEncryption
Issuer: CN=OCSP-TEST-CA,C=DE
```

```

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

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

```

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

1. The `importfile` command is called for the storage location `VPN2`, so we are dealing with a certificate for use in the VPN. The password for the private key is `lancom` and the root CA certificate can be checked with `SHA512` and the specified fingerprint.
2. In the following, the user is prompted to enter the certificate.
3. After entering the certificate, it is then imported.
4. In the following, the user is prompted to enter the private key.
5. Following the input, the key is checked.
6. In the following, the user is prompted to enter the CA certificate chain. The end of the input is not detected automatically. After the last certificate, the end is determined by entering `endcachain`. Type this command on a new line, because all of the input on a line containing the string **endcachain** is discarded.
7. Following these entries, the CA certificates are imported and the process is completed.

8.2 FirmSafe

8.2.1 Toggling the active firmware via console command

As of `LCOS` version 10.12, the current firmware can be switched over to the alternative firmware with a CLI command. The previously inactive firmware is set to "active" and the previously active firmware is set to "inactive". After entering the command, the device automatically executes a restart without further confirmation.

Under `/ Firmware`, enter the command `do switch-firmware`.

 The restart is performed automatically.

8.2.2 Additions to the Firmware menu

Switch firmware

This command line is used to switch the active firmware into the inactive state. Correspondingly, the alternative, non-active firmware is switched to the active state.



The device restarts automatically and immediately starts using the alternative firmware. By switching again, you restore the initial state.

SNMP ID:

3.8

Telnet path:

Firmware

Possible values:

do Switch-Firmware

Switch the firmware and restart the device

9 Voice over IP – VoIP

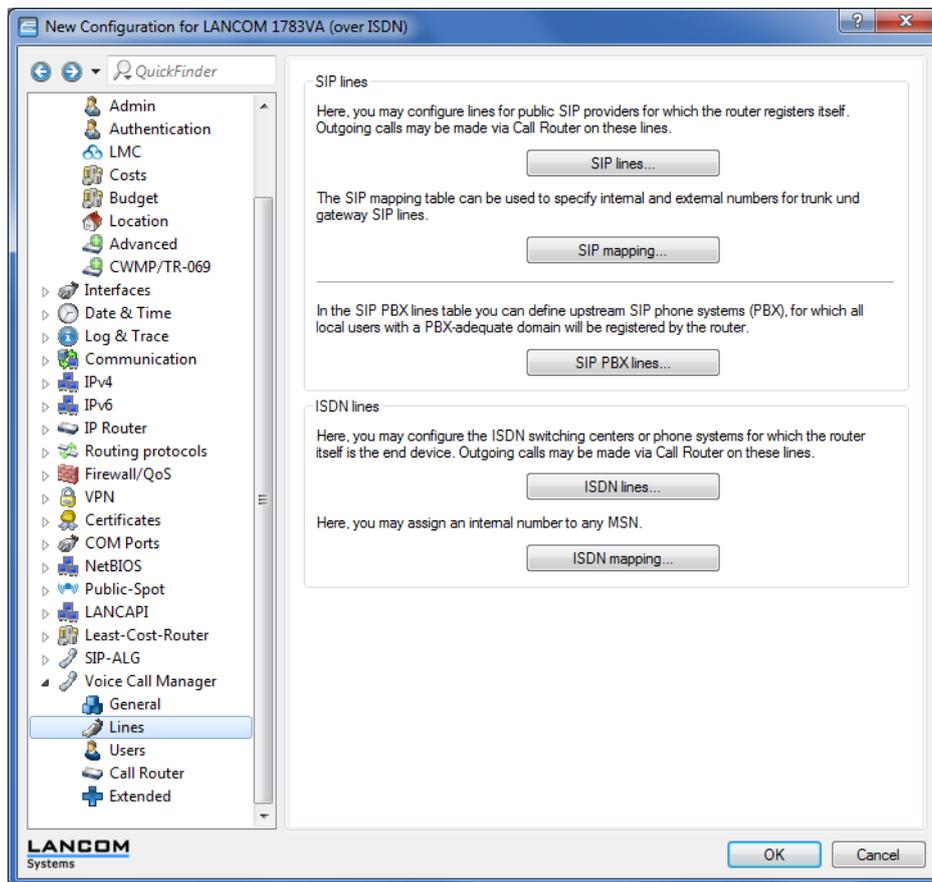
9.1 Transmitting phone numbers for VoIP connections

9.1.1 SIP lines

The SIP protocol has various options for transmitting a line's number and identifier to the SIP trunk provider. It may be necessary to adjust the transmission of the information to the VoIP provider.

As of LCOS version 10.12, the "SIP-ID transmission" switch allows you to configure the structure of the SIP packet and specify the field used for SIP ID transmission.

In **LANconfig** you configure the new feature under **Voice Call Manager > Lines > SIP lines**



under **SIP lines** on the tab **Advanced**:

Possible values with the new feature:

- > P-Preferred Identity (DEFAULT)
- > FROM

9.1.2 Additions to the Setup menu

User-Id-Field

Specifies the field used to transmit the SIP ID.

! In order for the P-Preferred-Identity-Field to be transferred at all, then under **Calling line identification restriction (CLIR)** you need to click on "Trusted area activated" and set the **Transmission method** to "RFC3325".

SNMP ID:

2.33.4.1.1.39

Telnet path:

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

Possible values:**P-Preferred Identity**

The SIP ID of the connection is transmitted in the P-Preferred-Identity field.

The source identifier transmitted to the called number is entered into the FROM field of the SIP packet.

FROM

The SIP ID of the connection is transmitted in the FROM field.

The source identifier transmitted to the called number is entered into the P-Preferred-Identity field of the SIP packet.

Default:

P-Preferred Identity

9.2 Overlap dialing for devices with Voice Call Manager

As of LCOS version 10.12, overlap dialing significantly reduces the waiting time between the number being dialed and the call being established.

With overlap dialing disabled, your LANCOM device uses an overlap timer. The factory setting for this is 6 seconds. If the timer expires without you dialing any further numbers, the number entered so far is considered to be complete and the call is established.

With overlap dialing enabled on the line, the portions of the dialed number are already sent to the All-IP provider.

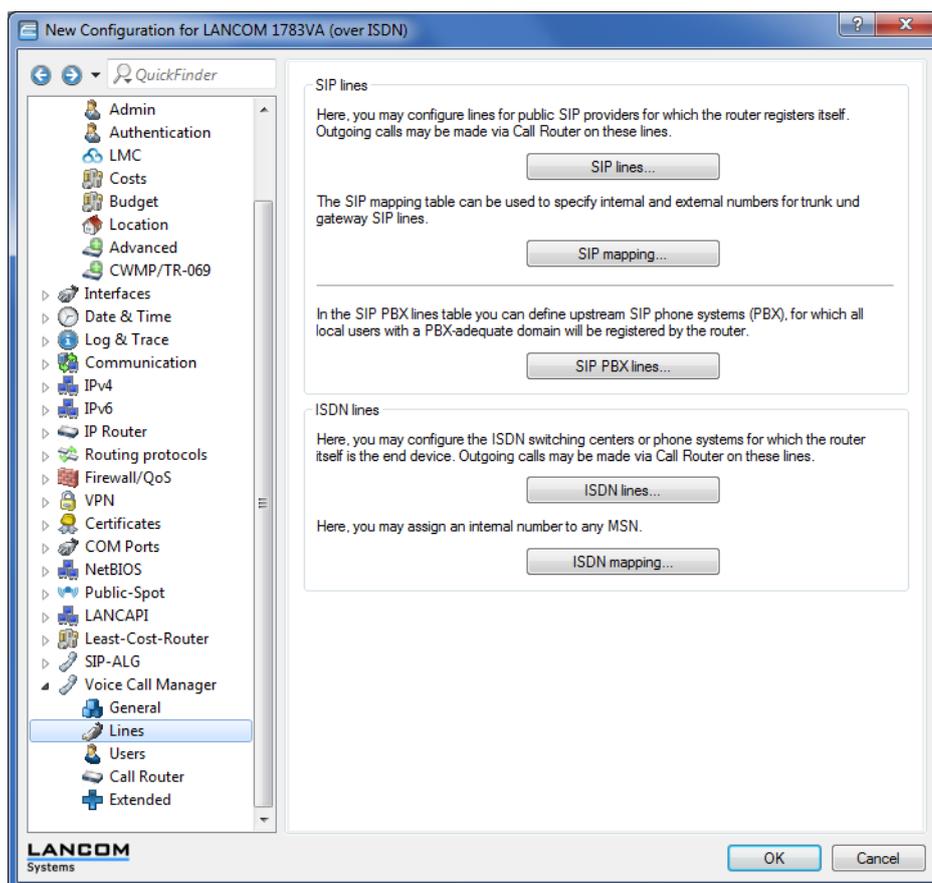
If the All-IP provider responds with "484 number incomplete", the Voice Call Manager collects any additional dialed digits and sends them to the exchange again.

In this way, calls are established as quickly as possible without the 6-second delay, as you are accustomed to from your ISDN connection.

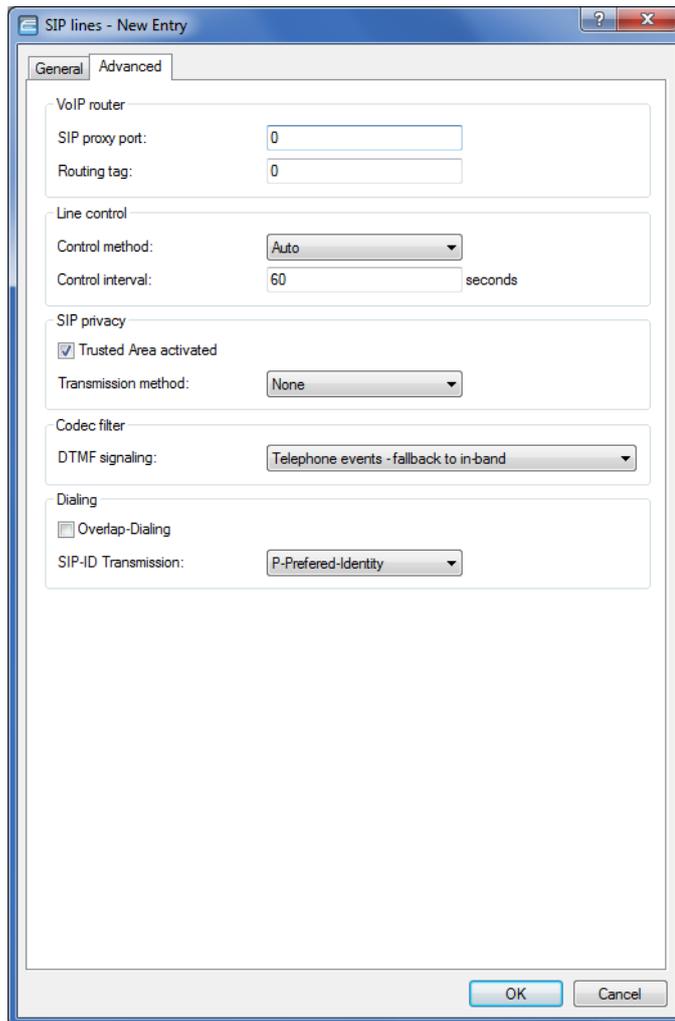


However, since this functionality is not supported by all SIP providers, overlap dialing has to be configured for each individual SIP line.

In **LANconfig** you configure the new feature under **Voice Call Manager > Lines > SIP lines**



under **SIP lines** on the tab **Advanced**:



The screenshot shows a dialog box titled "SIP lines - New Entry" with two tabs: "General" and "Advanced". The "Advanced" tab is selected. The dialog is divided into several sections:

- VoIP router:** SIP proxy port: 0, Routing tag: 0.
- Line control:** Control method: Auto (dropdown), Control interval: 60 seconds.
- SIP privacy:** Trusted Area activated (checked checkbox), Transmission method: None (dropdown).
- Codec filter:** DTMF signaling: Telephone events - fallback to in-band (dropdown).
- Dialing:** Overlap-Dialing (unchecked checkbox), SIP-ID Transmission: P-Preferred-Identity (dropdown).

At the bottom right, there are "OK" and "Cancel" buttons.

The possible values of the **Overlap dialing** feature:

Disabled

Disables overlap dialing (default).

Enabled

Enables overlap dialing.

9.2.1 Additions to the Setup menu

Overlap dialing

This is where you enable or disable overlap dialing.

SNMP ID:

2.33.4.1.1.36

Telnet path:

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

Possible values:

- 0
Deactivated
- 1
Activated

Default:

0

9.3 Fallback from an encrypted to an unencrypted VoIP connection

As of LCOS version 10.12 devices with the Voice Call Manager have a mechanism to fallback from an encrypted to an unencrypted VoIP connection.

Not all VoIP providers support encrypted VoIP connections on all connections. If sites need to be configured uniformly, this fallback mechanism can be useful. If an encrypted connection becomes available at a later time, the LANCOM router will use this automatically.

9.3.1 Additions to the Setup menu

Fallback

Configures the fallback mechanism for the SIP provider line.

SNMP ID:

2.33.4.1.1.38

Telnet path:**Setup > Voice-Call-Manager > Lines > SIP-Provider > Line****Possible values:****No**

No fallback to an unencrypted connection is performed. If it is not possible to establish an encrypted connection to the VoIP provider, the line remains unregistered.

UDP

As a rule, encrypted SIP connections are made with the TCP protocol and unencrypted connections are made with the UDP protocol. This setting switches directly to an unencrypted UDP connection if the encrypted TCP connection cannot be established.

Complete

If an encrypted TCP connection with the configured TLS version cannot be established, then attempts are made to establish an unencrypted TCP connection, and finally a UDP connection in order to register the VoIP line.



This setting provides the best compatibility, but may lead to a longer registration time.

Default:

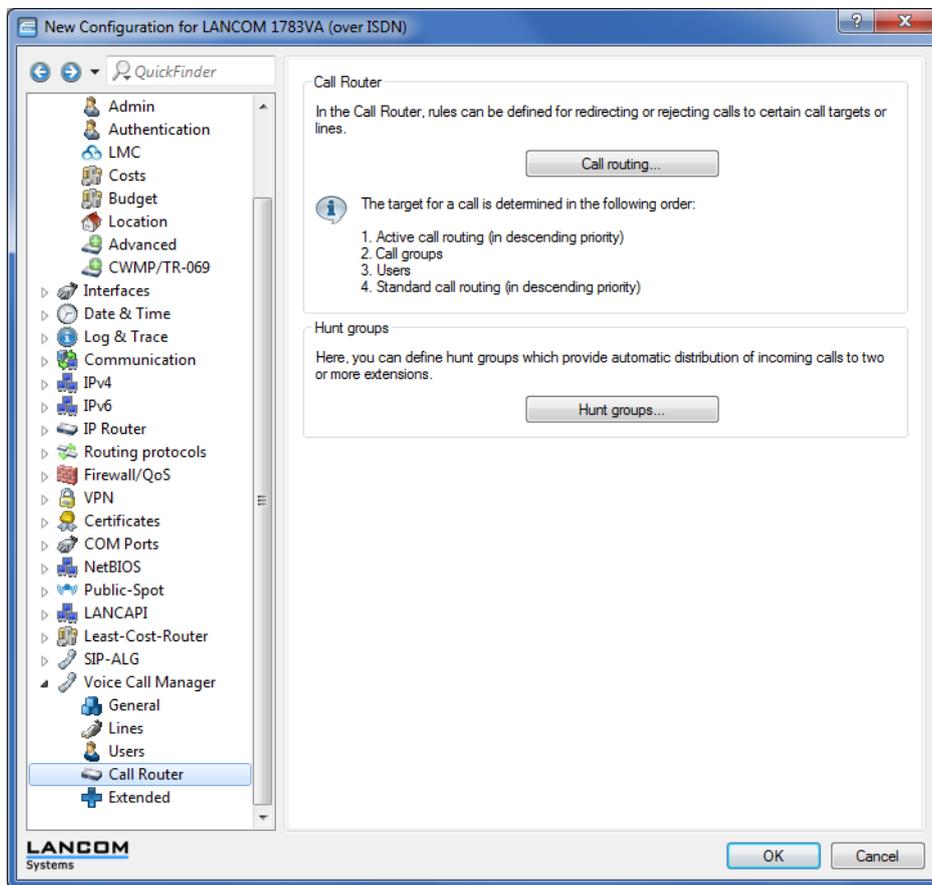
No

9.4 Prohibit control characters on SIP lines

As of LCOS version 10.12, you have the option of preventing the use of control codes. Control codes can, for example, be used to configure call forwarding. You can prevent this for any particular lines or persons.

Here's an example:

1. Start LANconfig and open the configuration dialog for your device.
2. Navigate to **Voice Call Manager > Call Router**.



3. Click the button **Call routing**.

4. Add a new call route.

Call routing - New Entry

Entry active / default line: Active

Priority: 0

Called number:

Comment:

Mapping

Calling number:

Destination number:

Destination line: Select

If the line is not available, you can define additional destinations here.

2. dest. number:

2. dest. line: Select

3. dest. number:

3. dest. line: Select

Filters

In addition to the called number you can define further filters for this entry:

Called domain: Select

Calling number:

Calling domain: Select

Source line: Select

OK Cancel

5. Under **Called number**: enter ##.
6. Under **Destination number**: enter #.
7. For the **Destination line** select REJECT.

8. Enter a **Comment**; e.g. "No numbers beginning with #".

Call routing - New Entry

Entry active / default line: Active

Priority: 0

Called number: ##

Comment: umbers beginning with #

Mapping

Calling number:

Destination number: #

Destination line: REJECT Select

If the line is not available, you can define additional destinations here.

2. dest. number:

2. dest. line: Select

3. dest. number:

3. dest. line: Select

Filters

In addition to the called number you can define further filters for this entry:

Called domain: Select

Calling number:

Calling domain: Select

Source line: Select

OK Cancel

9. Confirm your settings by clicking the **OK** button.

10 Diagnosis

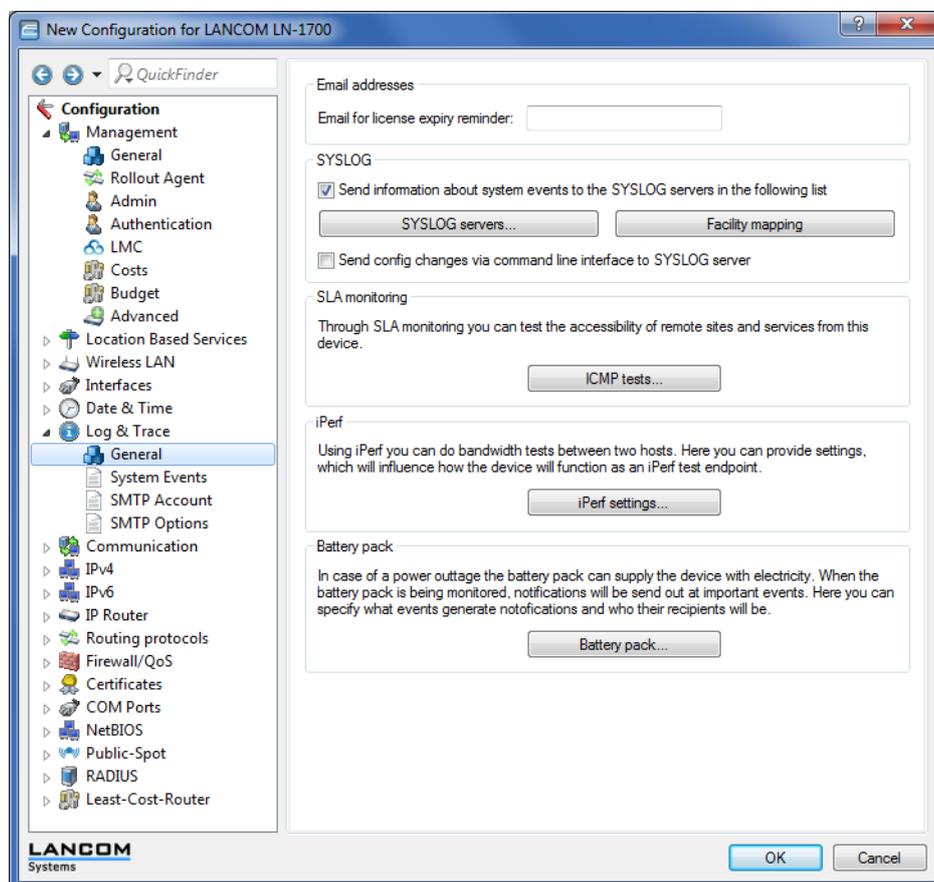
10.1 SYSLOG messaging via TCP

As of LCOS version 10.12, the SYSLOG client can also send messages to a SYSLOG server via TCP.

During TCP transmission, every data packet is checked to see that it arrived at the destination address completely and unmodified.

10.1.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.



- Change to the dialog **Log & Trace > General** and open the table **SYSLOG servers**.

- Set the **Port** input field to 514.
- From the selection list **Protocol** select TCP.

10.1.2 Additions to the Setup menu

Port

This entry contains the port used for SYSLOG.

SNMP ID:

2.22.2.8

Telnet path:

Setup > SYSLOG > Server

Possible values:

514

TCP/UDP

Default:

514

Protocol

This entry contains the protocol used for SYSLOG.

SNMP ID:

2.22.2.9

Telnet path:**Setup > SYSLOG > Server****Possible values:**

TCP
UDP

Default:

UDP

10.2 IPv4/IPv6 traffic accounting

As of LCOS version 10.12, layer-7 application detection captures IPv4 and IPv6 traffic separately.

There is no need to switch on this feature separately. With layer-7 application detection is active, both IPv4 and IPv6 applications are automatically resolved separately.

Layer-7 application detection logs details about the traffic transmitted over the relevant interface.

This is presented in the following status table:

```

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

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

```

The inbound (RX) and the outbound (TX) traffic are listed separately for IPv4 and IPv6 in kBytes.

10.2.1 Additions to the Status menu

Total traffic per protocol

This table presents inbound and outbound IPv4 / IPv6 traffic in kBytes.

SNMP ID:

1.95.8

Telnet path:**Status > Layer-7-App-Detection****Possible values:**

0 ... 4294967295

11 Interface bundling with LACP

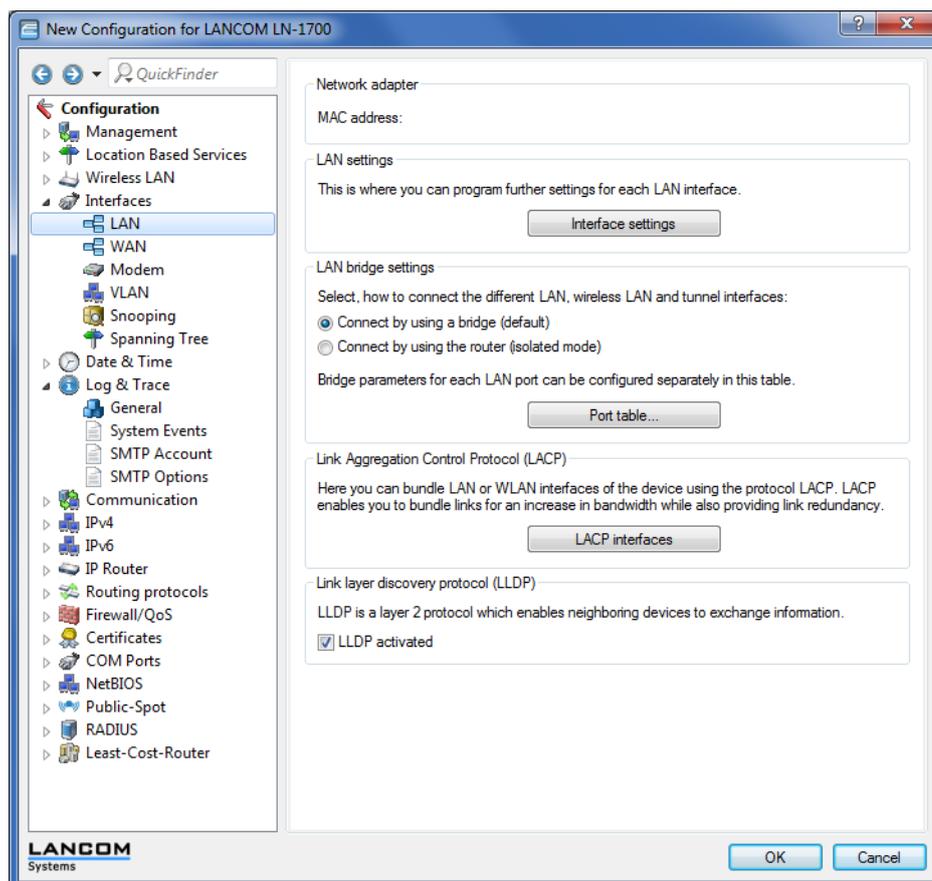
Significant improvements in terms of failover reliability and performance come with LCOS version 10.12 and the new support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle Ethernet ports into a virtual link. Physical Ethernet connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

! For example, 11ac Wave 2 (4x4 MIMO) achieves a data throughput greater than 1 Gbps net per AP.

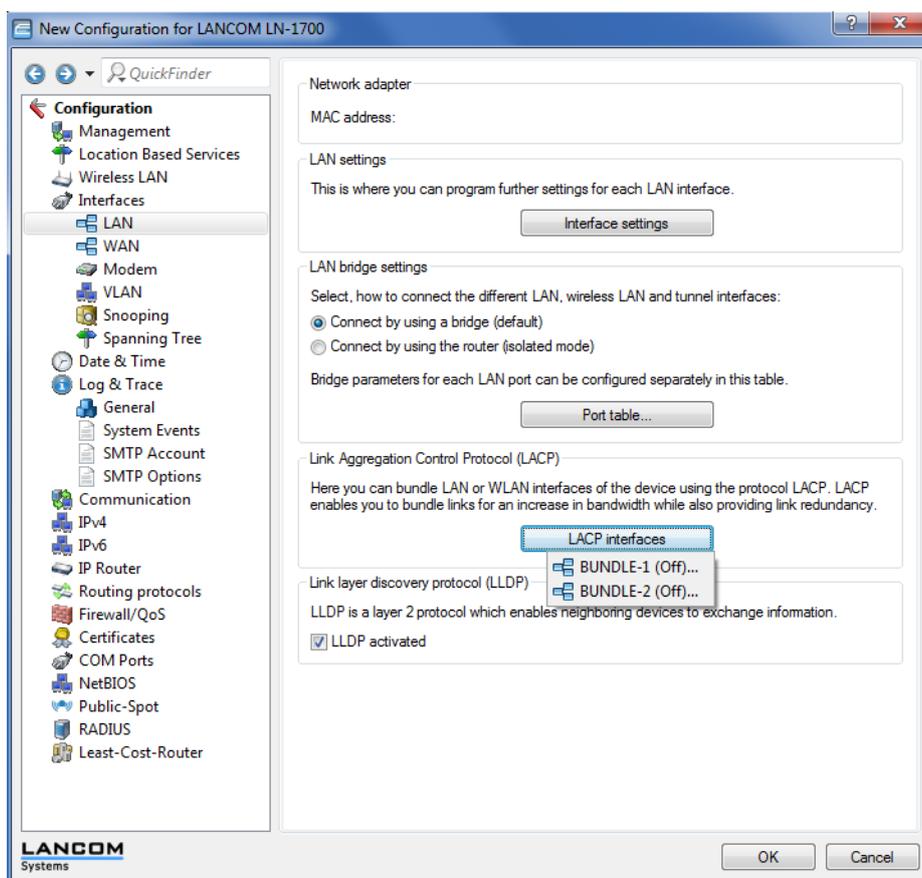
Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

11.1 Configuring the LACP interfaces

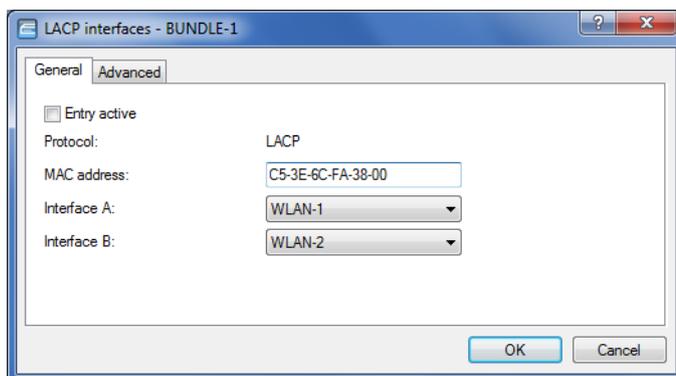
In LANconfig, you configure LACP interfaces under **Interfaces > LAN** in the section **Link Aggregation Control Protocol (LACP)**.



1. Click the button **LACP interfaces** to access the list of available bundles.



2. Choose a bundle.



3. Enter the MAC address of the device into the input field **MAC address**.

ⓘ The MAC address is used to identify the LACP partner within the LAG. If this is left empty or set to 0, the LAN MAC address of the device is set automatically. The MAC address does not necessarily have to belong to an interface of the bundle. In case of a configuration reset, the system-wide MAC address is entered here as the default.

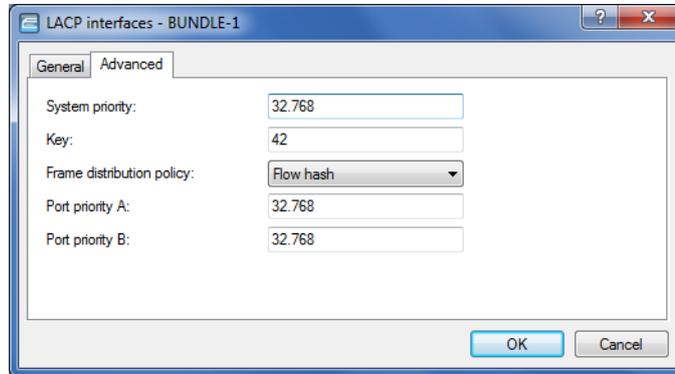
4. Select the first interface from the selection menu **Interface A**.
5. Select the second interface from the selection menu **Interface B**.
6. Activate the bundle by checking the checkbox **Entry active**.

ⓘ The remaining steps are optional.

The default settings are suitable for most common applications.

Further customizations to the configuration should only be performed by an experienced network technician.

7. Further configuration options are available on the **Advanced** tab.



8. In the **System priority** input field, enter a multiple of 4,096. The default value is 32,768.
 9. Enter a value for the **Key**.

! The key is a number from 1 to 54 and is used to identify the bundle.

10. Select an entry from the drop-down menu **Frame distribution policy**. The default setting for most scenarios is Flow hash.
 11. In the **Port priority A** input field, enter a multiple of 4,096. The default value is 32,768.
 12. In the **Port priority B** input field, enter a multiple of 4,096. The default value is 32,768.

11.1.1 Additions to the Setup menu

LACP

This menu is used to configure the Link Aggregation Control Protocol (LACP).

SNMP ID:

2.4.13.12

Telnet path:

Setup > LAN > Interface-Bundling

Interfaces

Select an interface bundle here.

SNMP ID:

2.4.13.12.1

Telnet path:

Setup > LAN > Interface-Bundling > LACP

Possible values:**BUNDLE-1**

Interface bundle 1

BUNDLE-2

Interface bundle 2

Interface

Use this menu to access the advanced features.

SNMP ID:

2.4.13.12.1.1

Telnet path:**Setup > LAN > Interface-Bundling > LACP > Interfaces****Possible values:****General**

Contains previously known features of the interface bundling.

Advanced

Contains new features of the interface bundling.

Default:

General

System-Priority

Set the system priority here.

SNMP ID:

2.4.13.12.1.2

Telnet path:**Setup > LAN > Interface-Bundling > LACP > Interfaces****Possible values:**

Multiples of 4096 [0-9]

Default:

32768

Key

Here, you assign a number as an identifier for the bundle.

SNMP ID:

2.4.13.12.1.3

Telnet path:

Setup > LAN > Interface-Bundling > LACP > Interfaces

Possible values:

1 ... 54

Default:

42

Frame distribution policy

Outbound packets from the transmitting end are distributed to the individual interfaces within the link aggregation group (LAG) according to the frame distribution policy.

SNMP ID:

2.4.13.12.1.4

Telnet path:

Setup > LAN > Interface-Bundling > LACP > Interfaces

Possible values:**VLAN**

Outbound packets are distributed to the individual links of the LAG according to their VLAN tags.

Flow hash

For outbound packets, a flow hash is formed from the IP addresses and the TCP/UDP ports. The flow hash determines how the packets are distributed to the individual links of the LAG.

Source MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address.

Destination MAC

Outbound packets are distributed to the individual links of the LAG according to their destination MAC address.

Source-dest. MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address and destination MAC address.

Default:

Flow hash

Port priority A

Here you set the status values for port priority A.

SNMP ID:

2.4.13.12.1.5

Telnet path:

Setup > LAN > Interface-Bundling > LACP > Interfaces

Possible values:

Multiples of 4096 [0–9]

Default:

32768

Port priority B

Here you set the status values for port priority A.

SNMP ID:

2.4.13.12.1.6

Telnet path:

Setup > LAN > Interface-Bundling > LACP > Interfaces

Possible values:

Multiples of 4096 [0–9]

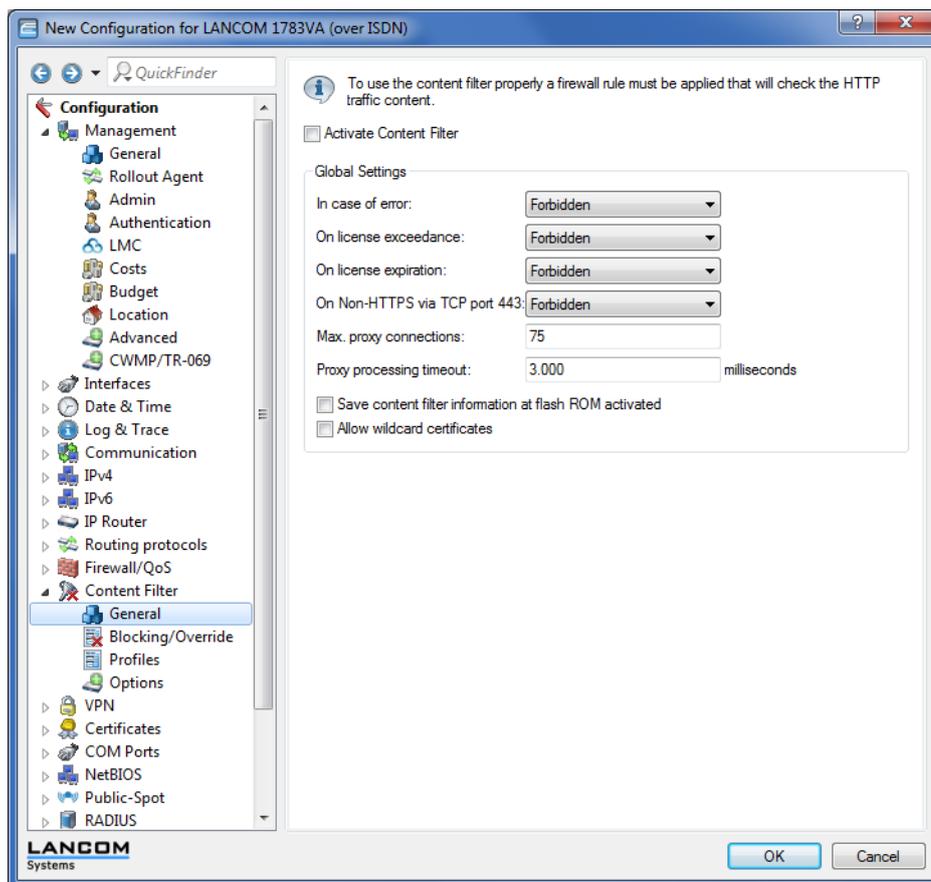
Default:

32768

12 LANCOM Content Filter

12.1 Unknown traffic via port 443

As of LCOS version 10.12 you can allow non-HTTPS connections over port 443. A new selection window was implemented in **LANconfig** for this purpose:



For non-HTTPS traffic over port 443

Forbidden

Prevents non-HTTPS traffic over port 443

Allowed

Permits non-HTTPS traffic over port 443

By default the TCP port 443 is reserved exclusively for HTTPS connections.

Some applications that do not use HTTPS still use TCP port 443. In this case, you can also open TCP port 443 for non-HTTPS connections.

 If you permit non-HTTPS connections over port 443, the traffic is not further classified and is open for any connection. By default, non-HTTPS connections over port 443 are not permitted.

12.1.1 Additions to the Setup menu

Unknown 443 traffic

Here, you can permit non-HTTPS communication via TCP port 443.

SNMP ID:

2.41.2.2.30

Telnet path:

Setup > UTM > Content-Filter > Global-Settings

Possible values:

0
Deny
1
Allow

Default:

0

12.2 IPv6 support

As of LCOS version 10.12 the content filter supports IPv6 as well as IPv4.

IPv6 data traffic is checked and filtered exactly like IPv4 traffic. Like IPv4, the configuration takes place in the firewall. In the IPv6 firewall, you can define actions that forward data traffic to the content filter for checking:

```
root@Router_PP:/Setup/IPv6/Firewall/Actions/CONTENT-FILTER-BASIC
> ls -a
[1.3.6.1.4.1.2356.11][2.70.5.7.1][column][20.67.79.78.84.69.78.84.45.70.73.76.84.69.82.45.66.65.83.73.67]
[ 1] Name           INFO:    CONTENT-FILTER-BASIC
[ 2] Limit           VALUE:   0
[ 3] Unit            VALUE:   packets
[ 4] Time            VALUE:   absolute
[ 5] Context         VALUE:   session
[ 6] Flags           VALUE:   none
[ 7] Action          VALUE:   check
[10] Content-Filter  VALUE:   CF-BASIC-PROFILE
[11] DiffServ        VALUE:   No
[12] DSCP-value      VALUE:   0
[13] Conditions     VALUE:
[14] Trigger-actions VALUE:
```

The action **check** is important in the context of the content-filter profile specified under **Content-Filter**. The profile is created as usual in the content-filter configuration.

By default, the following action objects are already created in the IPv6 firewall:

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

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

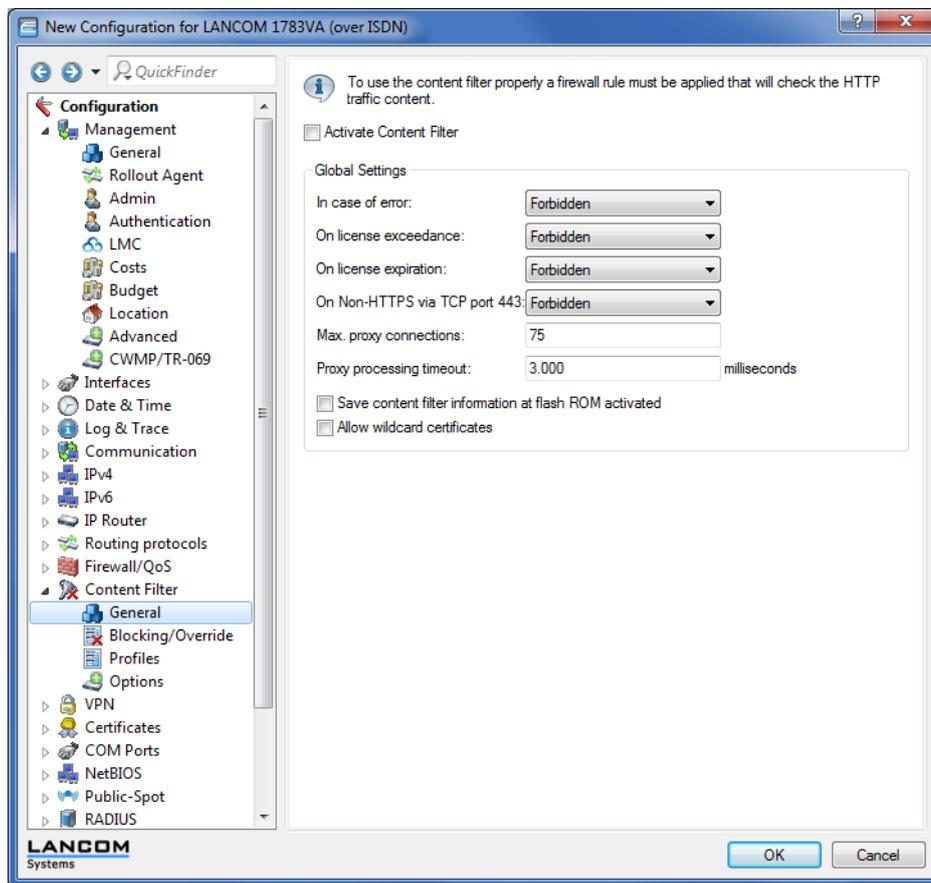
In the Forwarding-Rules table, the following rule is stored by default. It is disabled and can be activated by the user:

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

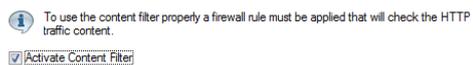
[1.3.6.1.4.1.2356.11][2.70.5.2]
Name          Action          Services Source-Stations Destination-Stations Flags
Comment
[1]           [5]            [7]    [8]           [9]           [2]
[10]
CONTENT-FILTER CONTENT-FILTER-BASIC ANY    ANYHOST      ANYHOST      deactivated
pass web traffic to...
...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

12.2.1 Configuration by LANconfig

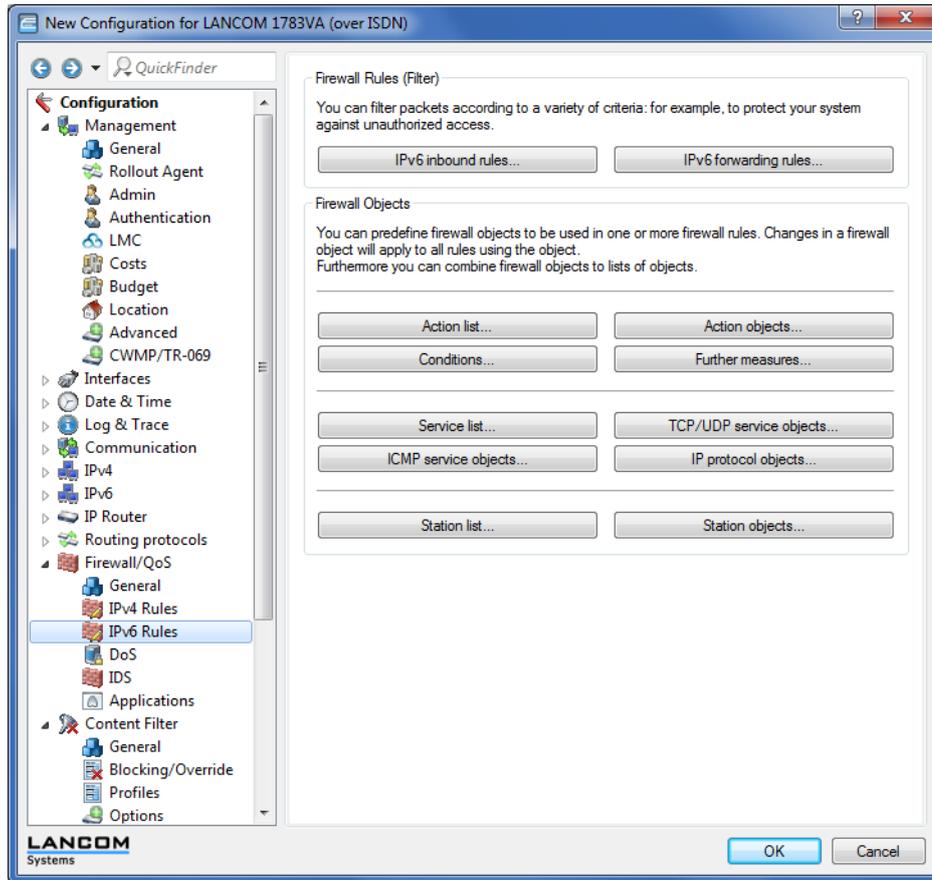
Navigate to **Content-Filter > General**



and enable the Content Filter using the drop-down box **Activate Content Filter**.

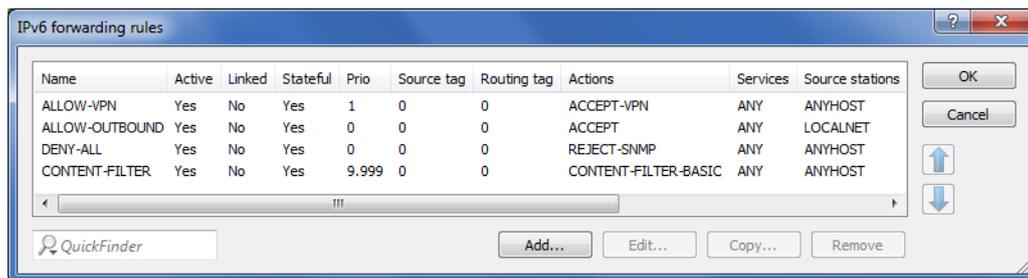


Now navigate to **Firewall/QoS > IPv6 rules**.

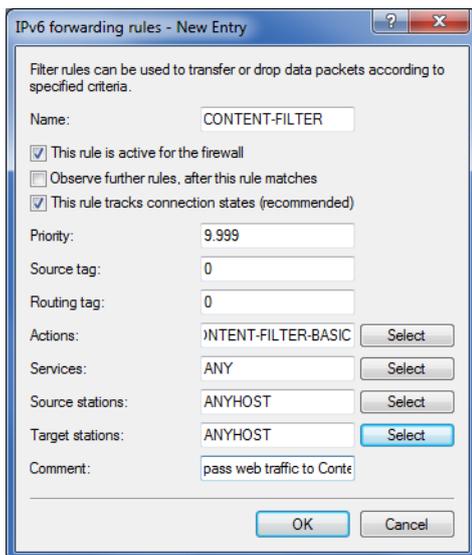


IPv6 forwarding rules

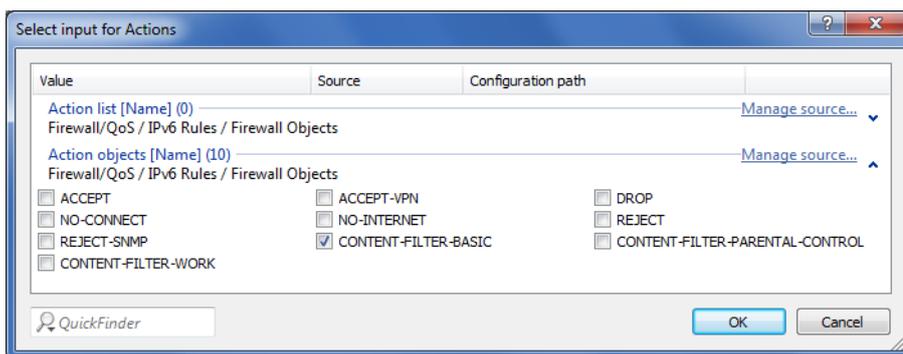
Forwarding rules are specified under **Firewall/QoS > IPv6 rules > Firewall rules (filter)** in the menu **IPv6 forwarding rules**:



By default the profile **CONTENT-FILTER** is created with the following settings:

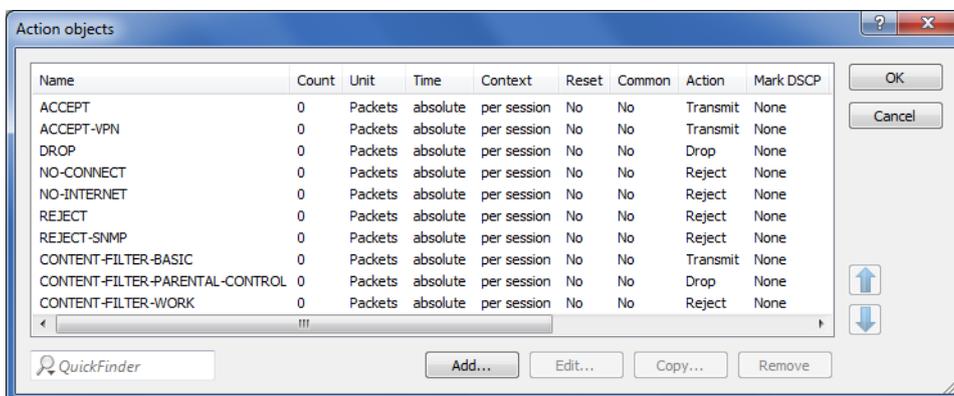


In the **Actions** selection list, you see the default content-filter profiles **CONTENT-FILTER-BASIC**, **CONTENT-FILTER-PARENTAL-CONTROL** and **CONTENT-FILTER-WORK**:



IPv6 action objects

You define the required firewall objects under **Firewall/QoS > IPv6 rules > Firewall objects** in the menu **Action objects**:



By default, the content filter profiles **CONTENT-FILTER-BASIC**, **CONTENT-FILTER-PARENTAL CONTROL** and **CONTENT FILTER WORK** have already been created as action objects.

If you edit one of these three entries, the field **Packet action** presents your content-filter profile options:

The screenshot shows a dialog box titled "Action objects - Edit Entry". The "Name" field contains "INTENT-FILTER-BASIC". Below the name is a descriptive text: "Configure in this action object trigger, packet actions and properties to be used once or more in the rule table." The dialog is divided into three main sections: "Trigger", "Packet action", and "Properties".

- Trigger:**
 - Count: 0
 - Unit: Packets
 - Time: absolute
 - Context: per session
 - Reset counter:
 - Common counter:
- Packet action:**
 - Action: Check via proxy
 - Mark with DiffServ-CP: Transmit, Drop, Reject
 - DiffServ-CP value: Check via proxy
- Properties:**
 - Conditions: [dropdown] [Select]
 - Further measures: [dropdown] [Select]

At the bottom of the dialog are "OK" and "Cancel" buttons.

Options:

Check via proxy (default)

The proxy decides whether the packet is transmitted or not.

Transmit

The packet is transmitted normally.

Drop

The packet is dropped silently.

Reject

The packet is rejected and the recipient is sent a corresponding message via ICMPv6.

12.2.2 Additions to the Setup menu

Content-Filter

Defines the content filter profile.

SNMP ID:

2.70.5.7.10

Telnet path:

Setup > IPv6 > Firewall > Actions

Possible values:

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

Default:

CF-BASIC-PROFILE

Default:

CF-PARENTAL-CONTROL-PROFILE

Default:

CF-WORK-PROFILE

13 Other services

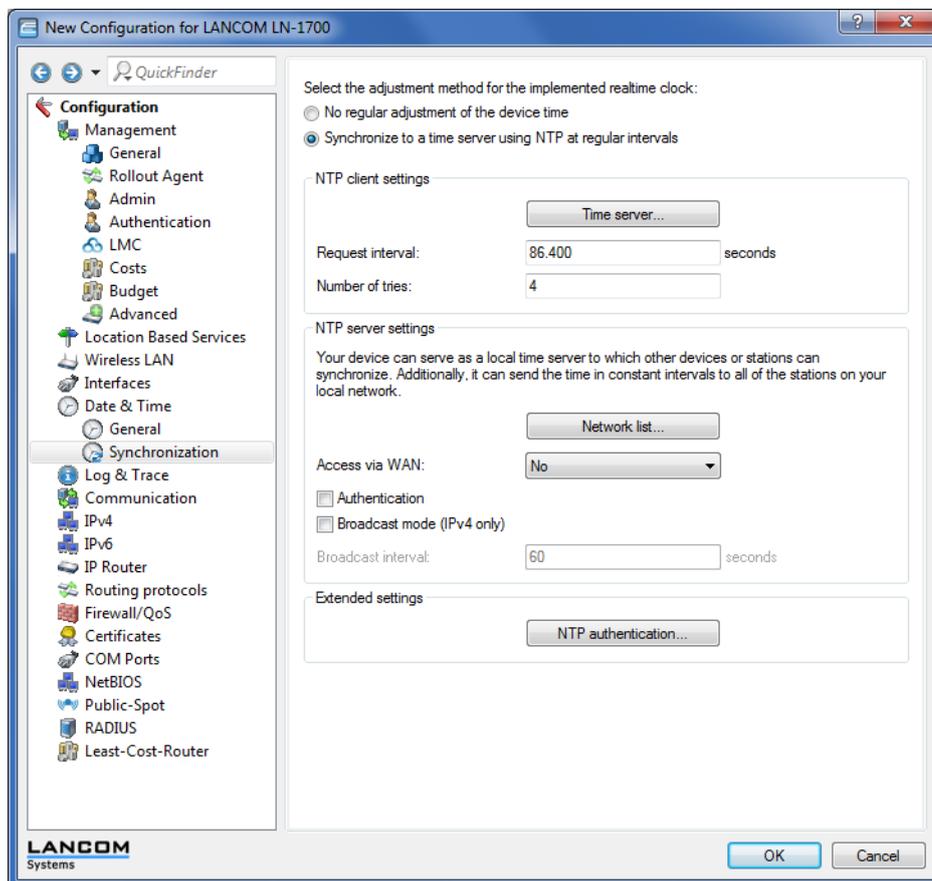
13.1 Time server for the local network

Additional features are available as of LCOS version 10.12:

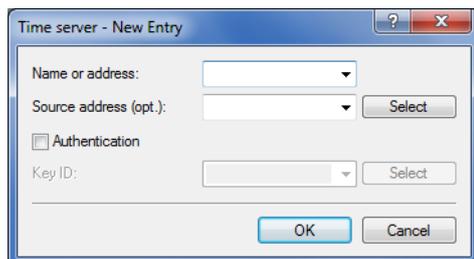
- > The NTP server can be activated for each ARF network.
- > NTP servers and NTP clients support MD5 authentication.
- > Access to the NTP server from the WAN can be enabled or disabled.

13.1.1 Configuration by LANconfig

You configure the new features under **Date & Time > Synchronization**.



In the section **NTP client settings**, the **Time server** menu contains two additional parameters.



Authentication

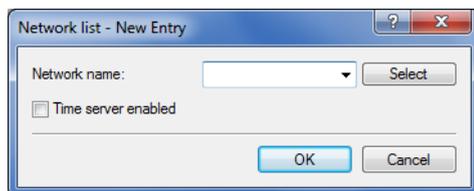
Enables or disables MD5 authentication by the client.

Key-ID

Identifies the key used by the client for MD5 authentication.

New in the section **NTP server settings**:

You can configure the list of networks to which your device forwards the current time under **Network list**.



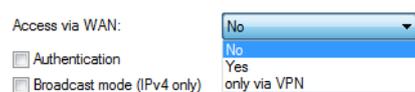
Network name

Specifies the name of the network.

Time server enabled

Determines whether the time server function of your device is activated for the selected network.

WAN access is configured with the selection list **Access via WAN**.



Options:

No

Access to the NTP server from the WAN is disabled.

Yes

Access from the WAN to the NTP server is possible via unmasked connections, but is in principle not possible with WAN masked connections.

Only via VPN

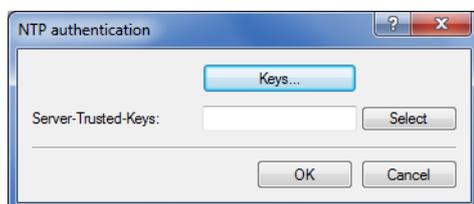
VPN access to the NTP server is enabled.

MD5 authentication support is enabled with **Authentication**.

New section **Extended settings**:

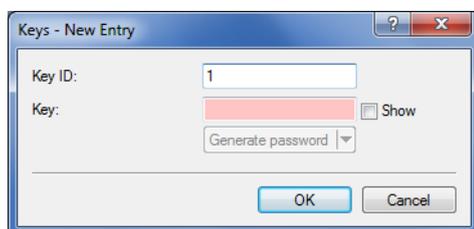


Configure the list of server trusted keys under **NTP authentication**.



The available keys are listed under **Server trusted keys** and are set with the **Select** button.

Keys are edited or added under **Keys**.



13.1.2 Additions to the Setup menu

Authentication

Enables or disables MD5 authentication for the client.

SNMP ID:

2.26.11.3

Telnet path:

Setup > NTP > RQ-Address

Possible values:

No

Disabled

Yes

Enabled

Default:

No

Key-ID

Identifies the key ID used for the client for MD5 authentication.

SNMP ID:

2.26.11.4

Telnet path:**Setup > NTP > RQ-Address****Possible values:**

1 ... 65535

Authentication

Enables or disables MD5 authentication for the server.

SNMP ID:

2.26.13

Telnet path:**Setup > NTP****Possible values:****No**

Disabled

Yes

Enabled

Default:

No

Key

Configures the table **Authentication-Keys**.

SNMP ID:

2.26.14

Telnet path:**Setup > NTP****Key-ID**

Identifies the key ID used for the server for MD5 authentication.

SNMP ID:

2.26.14.1

Telnet path:**Setup > NTP > Authentication-Keys****Possible values:**

1 ... 65535

Key

This entry contains the value of the key.

SNMP ID:

2.26.14.2

Telnet path:**Setup > NTP > Authentication-Keys****Possible values:**

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

Server-Trusted-Keys

Contains the list of trusted keys (comma-separated list of key numbers).

SNMP ID:

2.26.15

Telnet path:**Setup > NTP****Possible values:**

Max. 63 characters from [0-9,]

Network list

This list contains the networks that your device uses as a time server.

SNMP ID:

2.26.16

Telnet path:**Setup > NTP**

Network name

Defines the name of the network on which the NTP server is to be activated.

SNMP ID:

2.26.16.1

Telnet path:

Setup > NTP > Networklist

Possible values:

Entries from Setup/TCP-IP/Networklist: Characters from

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

Server-Operating

Defines whether the NTP server is enabled on the selected network.

SNMP ID:

2.26.16.2

Telnet path:

Setup > NTP > Networklist

Possible values:**No**

Disabled

Yes

Enabled

Default:

No

Server-WAN-Access

Configures WAN access to your device.

SNMP ID:

2.26.17

Telnet path:

Setup > NTP

Possible values:**No**

Disables access to the NTP server from the WAN.

Yes

Access from the WAN to the NTP server is possible via unmasked connections, but is in principle not possible with masked connections.

VPN

VPN access to the NTP server is enabled.

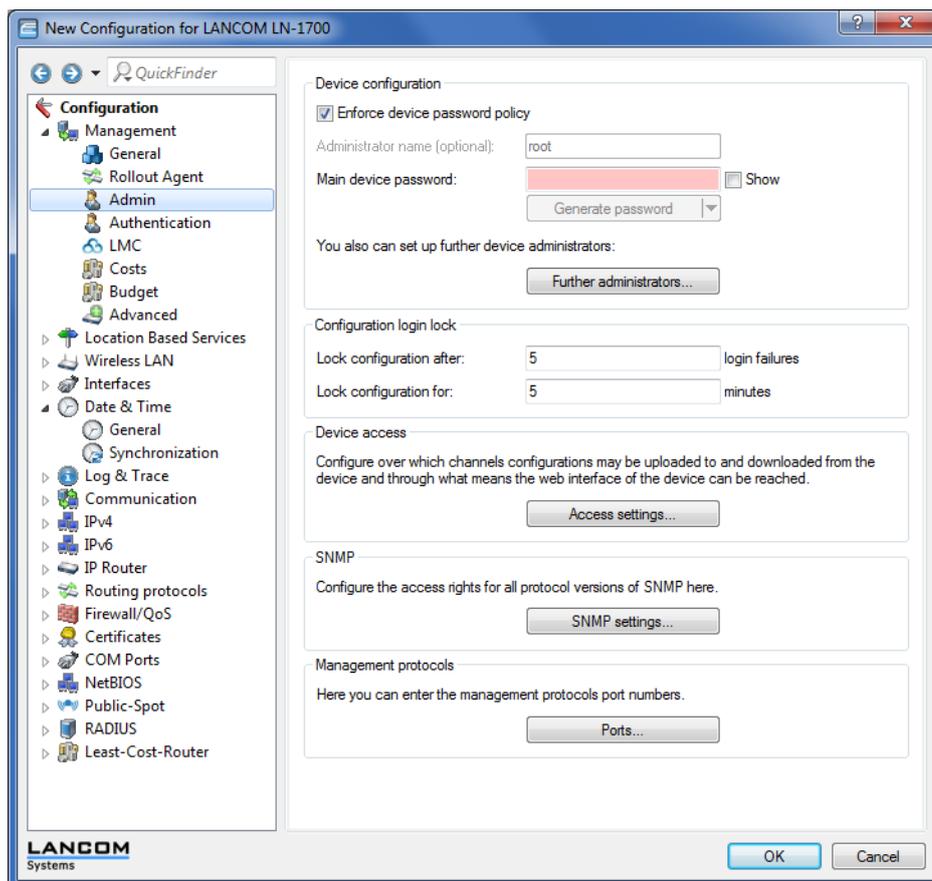
13.2 Simple Network Management Protocol (SNMP)

As of LCOS version 10.12, SNMPv3 users can make use of additional authentication algorithms.

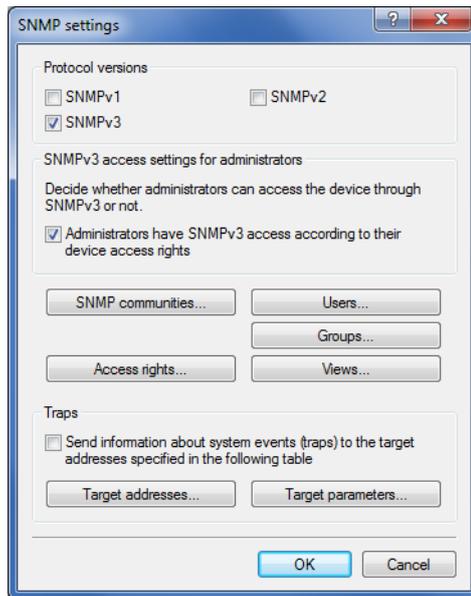
This means a further improvement to security.

13.2.1 Setting up SNMP with LANconfig

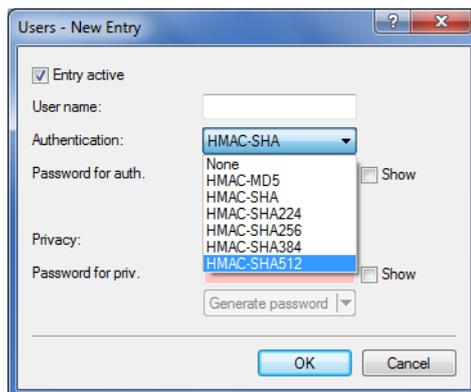
You configure the new features under **Management > Admin > SNMP**



in the menu **SNMP settings**.



The **Users** menu contains the **Authentication** selection list.



The new authentication algorithms:

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

13.2.2 Additions to the Setup menu

Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

As of LCOS version 10.12, you can use hash algorithms with a hash length of 224 bits and more.

SNMP ID:

2.9.32.5

Telnet path:

Setup > SNMP > Users

Possible values:**None**

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

Default:

HMAC-SHA

14 Appendix

14.1 CRON syntax

A CRON job consists of six fields:

```
minute    hour    day of month    month    day of week    command
```

The asterisk '*' serves as a placeholder for all permitted characters.

Here are some examples of performing regular restarts with the use of CRON:

Every day at 13:30h:

```
30        13        *        *        *        restart
```

Every day 30 minutes past each hour:

```
30        *        *        *        *        restart
```

Every 30 minutes every day:

```
* / 30    *        *        *        *        restart
```

Every Saturday at 20:15h:

```
15        20        *        *        6        restart
```

 Sundays is selected either with '0' or '7'.

At 00:00h on the first day of the month

```
0         0         1         *        *        restart
```