SECURE. **NETWORKS.**

LCOS 10.20

Addendum

01/2019

LANCOM
Systems

Contents

1 Addendum to LCOS version 10.20

This document describes the changes and enhancements in LCOS version 10.20 since the previous version.

2 Configuration

2.1 Configuration software

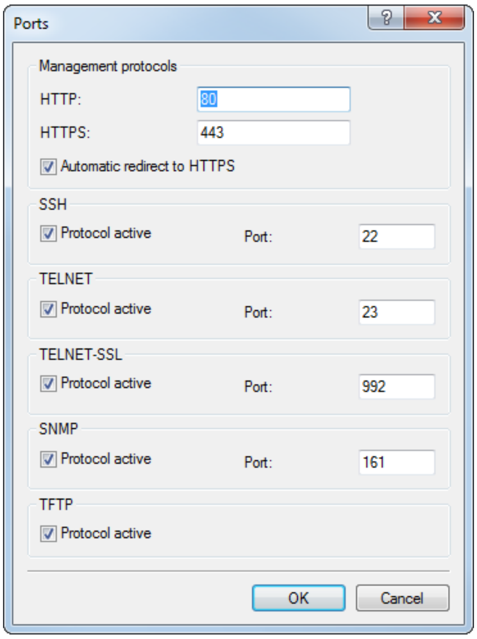
2.1.1 Automatic redirection of WEBconfig access to HTTPS

From LCOS version 10.20, unencrypted connection requests received by WEBconfig are automatically switched to encrypted HTTPS connections.

This improves the security when the user wishes to configure the LANCOM device via WEBconfig and enters the IP address or name into the browser address bar. The browser would normally establish an unencrypted HTTP connection.

The usual way to establish an encrypted HTTPS connection is to explicitly enter the prefix `https://` into the browser. This change makes it easier to enter the address and, at the same time, confidential data such as the login password or the configuration itself are secured by the encrypted connection.

This feature is always switched on in new configurations. Existing configurations will not be changed automatically. In these cases you can enable the function under **Management** > **Admin** > **Management protocols** > **Ports** > **Automatic redirect to HTTPS**.



Ports

Management protocols

HTTP: 80

HTTPS: 443

☑ Automatic redirect to HTTPS

SSH

☑ Protocol active Port: 22

TELNET

☑ Protocol active Port: 23

TELNET-SSL

☑ Protocol active Port: 992

SNMP

☑ Protocol active Port: 161

TFTP

☑ Protocol active

Additions to the Setup menu

Automatic-Redirect-to-HTTPS

This switch determines whether the WEBconfig login dialog receiving an unencrypted connection request automatically switches to an encrypted HTTPS connection. This is always switched on in new configurations. Existing configurations will not be changed.

SNMP ID:

2.21.24

Telnet path:

Setup > **HTTP**

Possible values:

No

WEBconfig does not automatically switch to an encrypted connection upon receiving an unencrypted connection request.

Yes

WEBconfig automatically switches to an encrypted connection upon receiving an unencrypted connection request.

Default:

Yes

2.1.2 Commands for the CLI

As of LCOS version 10.20 your device supports the new commands or options as follows.

Table 1: Overview of new commands available at the command line

Command	Description
`find <term>`	Looks for the search <term> and outputs all menu items containing it.
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) is a command-line tool specified in RFC 6835 to query LISP mappings on a map resolver. Possible arguments are: › `-i <instance>`: Name of the LISP instance used for the destination query › `-m <server>`: LISP map server used for the destination query › `-id <num>`: LISP Instance ID [0-16777215] used for the destination query › `destination-eid`: Requested destination EID › `-retries <num>`: LISP retries to the map server [0-10] › `-rtg-tag <num>`: Routing tag used › `-source-eid <num>`: Source EID used Example: `lig -i LISP-INST 172.16.200.1`
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	The readscript command generates a text dump of all commands and parameters required to configure the device in its current state. The following option switch is new: › `-o`: Replaces the passwords with a "*" to obfuscate them in the text output. **Access rights**: Supervisor-Read
`show admin-distance`	Shows the administrative (routing) distance of all internal applications or routing protocols. **Access rights**: Supervisor-Read, Local-Admin-Read
`show ip-addresses`	Displays all IPv4 and IPv6 addresses for the device for the LAN and WAN interfaces, along with advanced status information. **Access rights**: Supervisor-Read, Local-Admin-Read

Command	Description
`show ipv4-addresses`	Displays all IPv4 addresses for the device for the LAN and WAN interfaces, along with advanced status information. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp instance`	Displays status information about all configured LISP instances. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp instance [instance]`	Displays status information about the LISP instance named [instance]. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache`	Displays status information about the map cache entries available for all instances. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache [instance]`	Displays status information about the map cache entries for the instance named [instance]. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp registrations`	Displays status information about the EIDs/RLOCs of all instances registered with the map server. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp registrations [instance]`	Displays status information about the EIDs/RLOCs of the instance named [instance] registered with the map server. **Access rights**: Supervisor-Read, Local-Admin-Read
`show VLAN`	Other LCOS modules can at runtime instruct the VLAN module to add further VLANs and VLAN memberships to the static configuration. This is used by CAPWAP or WLAN/802.1X, for example. The `show` command now displays this with the new option `VLAN`. **Access rights**: Supervisor-Read, Local-Admin-Read
`ssldefaults [-y]`	This command resets the SSL / TLS settings in all submenus of the current configuration to the default values after a security prompt. In LCOS, each module comes with its own submenu for SSL / TLS settings. This provides a way to reset all settings in these various submenus to the current secure default settings. The parameter `-y` ensures that the security prompt is automatically answered so that the command can be used non-interactively in scripts.

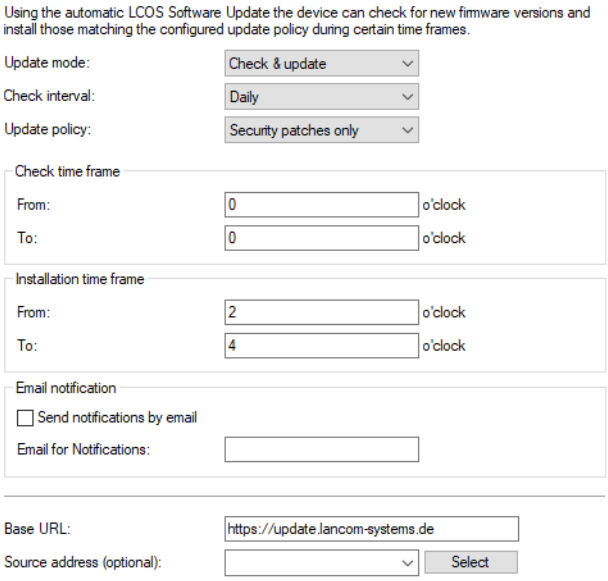
2.2 LANCOM Auto Updater

The LANCOM Auto Updater allows the automatic updating of on-site LANCOM devices without further user intervention. LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

2.2.1 Configuring the Auto Updater

The configuration for the LANCOM Auto Updater in LANconfig is located under **Management** > **Software update**.



Using the automatic LCOS Software Update the device can check for new firmware versions and install those matching the configured update policy during certain time frames.

Update mode: Check & update
Check interval: Daily
Update policy: Security patches only

Check time frame
From: 0 o'clock
To: 0 o'clock

Installation time frame
From: 2 o'clock
To: 4 o'clock

Email notification
□ Send notifications by email
Email for Notifications:

Base URL: https://update.lancom-systems.de
Source address (optional):

Update mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security patches only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest version w/o release

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 Rel.

Check time frame

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

Installation time frame

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Send notifications by e-mail

This setting determines whether the LANCOM Auto Updater sends e-mail notifications to the specified e-mail address. Administrators can use the e-mail notifications to receive information about events relating to the automatic firmware update by the Auto Updater. An e-mail is sent after the following events:

- An update was found (in the update mode “Check” only)
- An update was found and a time for automatic installation was scheduled (the in update mode “Check & Update”)
- An update has been successfully installed (including successful access check)
- An update was not successful and a fallback to the previously installed firmware was performed
- Error messages from the Auto Updater (e.g. update server could not be reached)

ⓘ Notification is only given for automatically executed actions. If actions are started manually, e.g. an update check via LANmonitor or WEBconfig, then there is no e-mail notification.

E-mail address

Here you enter the e-mail address to be used when e-mail alerts are enabled.

Base URL

Specifies the URL of the server that provides the latest firmware versions.

Source address

A routing tag can be set automatically by specifying a loopback address.

2.2.2 Additions to the Setup menu

Automatic-Firmware-Update

The LANCOM Auto Updater allows on-site LANCOM devices to be updated automatically without further user intervention (unattended). LANCOM Devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

SNMP ID:

2.107

Telnet path:

Setup

Mode

Set the operating mode of the LANCOM Auto Updater.

SNMP ID:

2.107.1

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Manual

The Auto Updater only checks for new updates when prompted by the user.

Users can manually use the Auto Updater to initiate the latest available update.

Check

The Auto Updater regularly checks the LANCOM update server for new updates. The availability of a new update is signaled to the user in the LCOS menu tree and via syslog. Users can manually use the Auto Updater to initiate the latest available update.

Check and update

The Auto Updater regularly checks the LANCOM update server for new updates. The update server uses the version policy to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater. The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Default:

Check and update

Check firmware now

This command triggers the device to check the LANCOM update server for new firmware.

SNMP ID:

2.107.2

Telnet path:

Setup > **Automatic-Firmware-Update**

Update firmware now

This command triggers the device to download and install the latest firmware from the LANCOM update server.

SNMP ID:

2.107.3

Telnet path:

Setup > **Automatic-Firmware-Update**

Cancel current action

This command triggers the device to abort any current actions by the Auto Updater. This applies to manually started and scheduled actions.

SNMP ID:

2.107.4

Telnet path:

Setup > **Automatic-Firmware-Update**

Reset updater config

This command resets the boot-persistent configuration files that are created by the Auto Updater. This includes the local blacklist of firmware versions that failed an automatic update.

SNMP ID:

2.107.5

Telnet path:

Setup > **Automatic-Firmware-Update**

Base URL

Specifies the URL of the server that provides the latest firmware versions.

SNMP ID:

2.107.6

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default:

https://update.lancom-systems.de

Check interval

After booting, the Auto Updater sets a random time period within a day or a week for the check to be performed. The update itself is performed in the next time period between 02:00 - 04:00 (default).

SNMP ID:

2.107.7

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Daily
Weekly

Default:

Daily

Version policy

Set the version policy of the LANCOM Auto Updater. This controls which firmware versions are offered to update a device.

SNMP ID:

2.107.8

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Latest

Always the newest version, irrespective of the release version. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security updates only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest without REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 Rel.

Default:

Security updates only

Loopback-Addr.

A routing tag can be set automatically by specifying a loopback address.

SNMP ID:

2.107.9

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

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

Default:

empty

Check time begin

The hour of the day at the start of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.10

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

Check time end

The hour of the day at the end of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.11

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 2 characters from `[0-9]`

Default:

0

Install time begin

The hour of the day at the start of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.12

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 2 characters from `[0-9]`

Default:

2

Install time end

The hour of the day at the end of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.13

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 2 characters from `[0-9]`

Default:

4

E-mail notification

This setting determines whether the LANCOM Auto Updater e-mail notifications are sent to the e-mail address specified in 2.107.15 . Administrators can use the e-mail notifications to receive information about events relating to the automatic firmware update by the Auto Updater. An e-mail is sent after the following events:

- An update was found (in the update mode "Check" only)
- An update was found and a time for automatic installation was scheduled (the in update mode "Check & Update")
- An update has been successfully installed (including successful access check)
- An update was not successful and a fallback to the previously installed firmware was performed
- Error messages from the Auto Updater (e.g. update server could not be reached)

ⓘ Notification is only given for automatically executed actions. If actions are started manually, e.g. an update check via LANmonitor or WEBconfig, then there is no e-mail notification.

SNMP ID:

2.107.14

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

No

The Auto Updater does not send notifications.

Yes

The Auto Updater sends notifications.

Default:

No

E-mail address

Here you can enter the e-mail address to be used by the LANCOM Auto Updater when e-mail alerts are enabled under 2.107.14 .

SNMP ID:

2.107.15

Telnet path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 63 characters from `` [A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.` ``

Default:

empty

2.3 Managing rights for different administrators

2.3.1 Improved protection of the device configuration against unwanted changes

From LCOS version 10.20, access to the table **Configuration** > **Management** > **Admin** > **Further administrators** is only possible for the root administrator. This is no longer possible for other administrators configured in this table, even if their ‘Access rights’ are configured as “All”.

On the CLI, this change means that the table is no longer visible to other administrators. Reading out the file with “readscript” is also no longer possible. If another administrator tries to access the table with a script, the corresponding script lines are not executed and a “Script Error” is issued.

The cron table works with the user configured for it, meaning that if the commands “loadconfig/loadscript” are executed via the cron table, they will only be able to read the configuration completely if they are run with the root administrator.

The table is still displayed in LANconfig, but it is shown as empty if accessed by another administrator. Changes are not written back to the device.

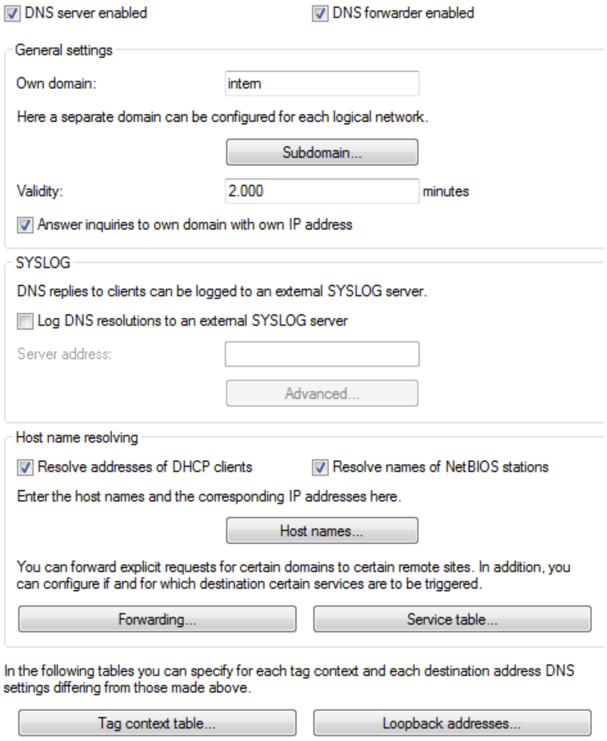
SNMP access (read/write) to this table has been deprecated as a part of this feature.

3 Routing and WAN connections

3.1 Advanced Routing and Forwarding (ARF)

3.1.1 Routing tags for DNS forwarding

With DNS forwarding, it is possible to set up multiple forwarding definitions (especially general wildcard definitions with "*") that are independent of one another by marking them with unique routing tags. Depending on the routing context of the requesting client, the router considers only those forwarding entries that are correspondingly tagged and any general entries that are marked with "0".



☑ DNS server enabled ☑ DNS forwarder enabled

General settings

Own domain: intern

Here a separate domain can be configured for each logical network.

Validity: 2.000 minutes

☑ Answer inquiries to own domain with own IP address

SYSLOG

DNS replies to clients can be logged to an external SYSLOG server.

☐ Log DNS resolutions to an external SYSLOG server

Server address:

Host name resolving

☑ Resolve addresses of DHCP clients ☑ Resolve names of NetBIOS stations

Enter the host names and the corresponding IP addresses here.

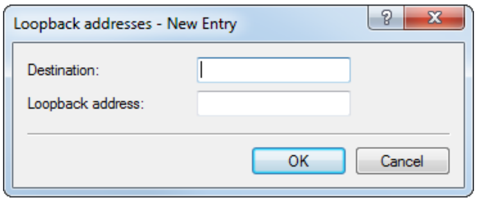
You can forward explicit requests for certain domains to certain remote sites. In addition, you can configure if and for which destination certain services are to be triggered.

In the following tables you can specify for each tag context and each destination address DNS settings differing from those made above.

From LCOS version 10.20, each destination for DNS forwarding can be given a specific loopback address.

Loopback addresses

LANconfig allows loopback addresses to be specified for every remote site under **IPv4** > **DNS** > **Loopback addresses**. Consequently, there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one remote site and loopback address. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.



The following options are possible for each loopback address:

Destination

The remote site for a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an "@". The remote site must also be in the DNS Destinations table.

Source address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

Additions to the Setup menu

Loopback-Addresses

This table allows you to store loopback addresses for each remote site. This means that there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one remote site and loopback address. The remote site must also be in the DNS Destinations table. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.

SNMP ID:

2.17.17

Telnet path:

Setup > **DNS**

Destination

The remote site as part of a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an @. The remote site must also be in the DNS Destinations table.

SNMP ID:

2.17.17.1

Telnet path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Loopback address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

SNMP ID:

2.17.17.2

Telnet path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

3.2 Locator / ID Separation Protocol (LISP)

As of version 10.20, LCOS features LISP.

The Locator/ID Separation Protocol (LISP) as per RFC 6830 is a new routing architecture that splits an IP address into two entities: The routing locator (RLOC) and the endpoint identifier (EID). The goal is to achieve a highly scalable routing architecture with integrated routing, tunneling and overlay protocols.

Conventional routing protocols such as RIP, OSPF or BGP work according to the “push principle” and proactively distribute their best routes to their neighbors. This architecture is of limited scalability, as the ever larger BGP tables and routing tables increasingly become a challenge.

LISP works according to the “pull principle” and works much like the Domain Name System (DNS). LISP routers register their networks, referred to as endpoint identifiers (EIDs), at a central instance called a map server or map resolver. Along with the EID, they also register their global (WAN) address, called the routing locator (RLOC). This keeps the information about the location (locator) separate from the identity (ID).

If a router wants to transfer data to a remote LISP network, first the LISP map resolver is queried for the mappings between the requested EID prefix and the routing locator. In the next step, a data tunnel is established between the two LISP routers.

LISP currently does not provide encryption of the data tunnel and, when used in insecure networks such as the Internet, it is typically combined with VPN. Application scenarios for LISP are multi-VPNs.

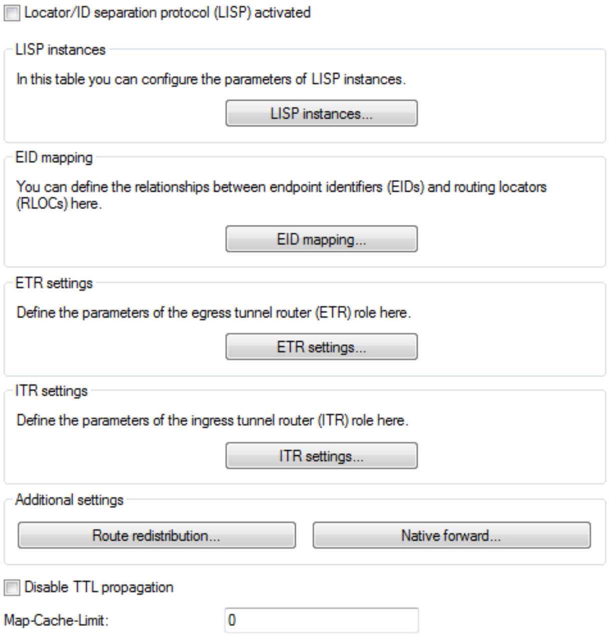
LCOS as of LCOS version 10.20 supports the following roles:

- Ingress tunnel router (ITR)
- Egress tunnel router (ETR)

The role of the map server/map resolver is currently not supported.

3.2.1 Configuration

LISP routing is configured in LANconfig under **Routing protocols** > **LISP**. The switch **Locator/ID separation protocol (LISP) activated** is used to switch this routing protocol on or off.



☐ Locator/ID separation protocol (LISP) activated

LISP instances
In this table you can configure the parameters of LISP instances.

EID mapping
You can define the relationships between endpoint identifiers (EIDs) and routing locators (RLOCs) here.

ETR settings
Define the parameters of the egress tunnel router (ETR) role here.

ITR settings
Define the parameters of the ingress tunnel router (ITR) role here.

Additional settings

☐ Disable TTL propagation

Map-Cache-Limit: 0

Disable TTL propagation

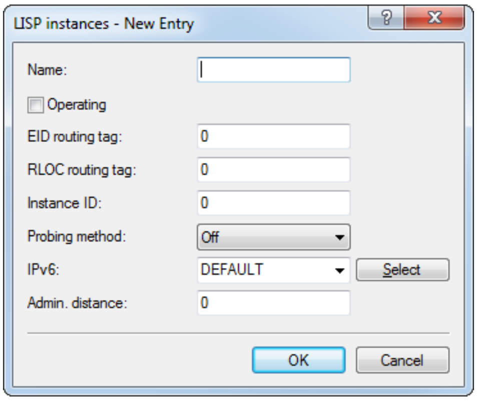
When enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

LISP instances

This table contains the global configuration of the LISP instances on the device.



LISP instances - New Entry

Name:

☐ Operating

EID routing tag: 0

RLOC routing tag: 0

Instance ID: 0

Probing method: Off

IPv6: DEFAULT

Admin. distance: 0

Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

Entry active

Activates or deactivates this LISP instance.

EID routing tag

Routing tag of the endpoint identifier (EID) of this instance.

RLOC routing tag

Routing tag of the routing locator (RLOC) of this instance.

Instance ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

Probing method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries. Available methods:

- Off: The availability of the RLOCs is not checked periodically.
- RLOC probing: The availability of the RLOCs is periodically checked by LISP RLOC messages.

IPv6

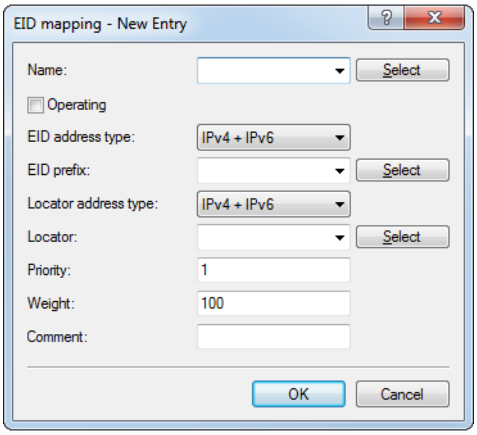
Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

Administrative distance

The administrative distance of this LISP instance.

EID mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.



EID mapping - New Entry

Name:

□ Operating

EID address type: IPv4 + IPv6

EID prefix:

Locator address type: IPv4 + IPv6

Locator:

Priority: 1

Weight: 100

Comment:

Name

References the name of the LISP instance.

Operating

Activates or deactivates this EID mapping.

EID address type

Protocol version of the EID prefix when referencing the EID prefix via an interface or network name. Possible values:

- **IPv4**: Only the IPv4 prefix of the referenced interface is used.
- **IPv6**: Only the IPv6 prefix of the referenced interface is used.
- **IPv4+IPv6**: Both the IPv4 prefix and the IPv6 prefix of the referenced interface are used.

EID prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority of the EID mapping. Default: 1.

Weight

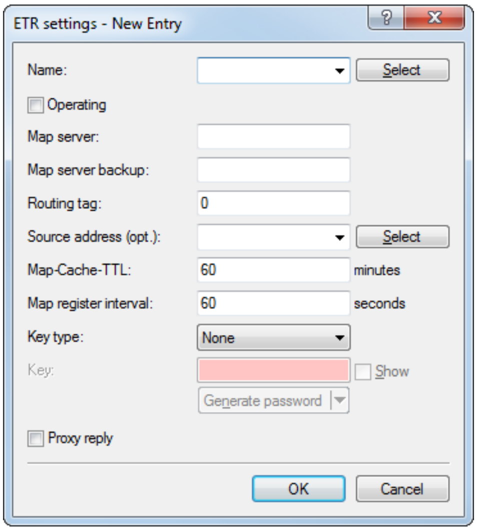
The weight of the EID mapping. Default: 100.

Comment

Enter a descriptive comment for this entry.

ETR settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).



ETR settings - New Entry

Name:

☐ Operating

Map server:

Map server backup:

Routing tag: 0

Source address (opt.):

Map-Cache-TTL: 60 minutes

Map register interval: 60 seconds

Key type: None

Key:

☐ Show

☐ Proxy reply

Name

References the name of the LISP instance.

Operating

Activates or deactivates these ETR settings.

Map-Server

IPv4 or IPv6 address of the LISP map server

Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

Routing tag

Routing tag to be used to access the map server.

Source address (opt.)

Contains the sender address as the named interface that is used with the map server in LISP communication.

Map-Cache-TTL

Time-to-live of the EID mappings in minutes registered with the map server.

Map register interval

Registration interval in seconds in which map registrations are sent to the map server.

Key type

Algorithm used for authentication at the map server. Possible values:

- None
- HMAC-SHA-1-96
- HMAC-SHA-256-128

Key

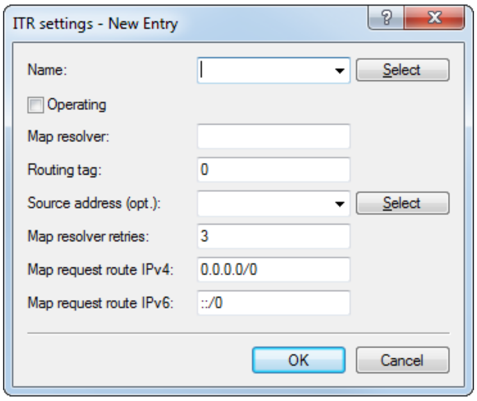
Key or password used to register the EID mapping on the map server.

Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

ITR settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).



ITR settings - New Entry

Name:	
□ Operating	
Map resolver:	
Routing tag:	0
Source address (opt.):	
Map resolver retries:	3
Map request route IPv4:	0.0.0.0/0
Map request route IPv6:	::/0

Name

References the name of the LISP instance.

Operating

Activates or deactivates these ITR settings.

Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

Routing tag

Routing tag used to access the map resolver.

Source address (opt.)

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

Map-Resolver-Retries

Number of retries for map requests to the map resolver. Default: 3

Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

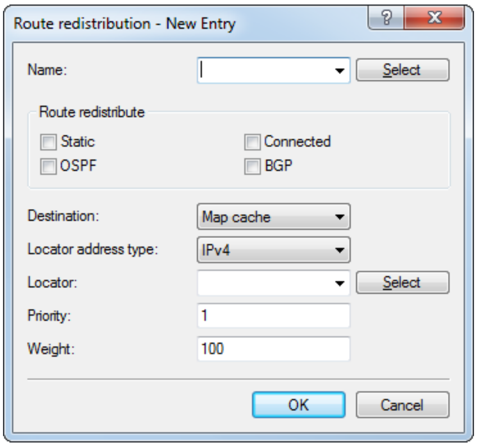
Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

Route redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.



Route redistribution - New Entry

Name:

Route redistribute

□ Static □ Connected

□ OSPF □ BGP

Destination: Map cache

Locator address type: IPv4

Locator:

Priority: 1

Weight: 100

Name

References the name of the LISP instance.

Route redistribute

Specifies the route sources of the imported routes.

- **Static**: The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **Connected**: From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **OSPF**: The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **BGP**: The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

Destination

Specifies the destination of routes imported to LISP. Possible values:

- **Map cache**: Imports the routes into the map cache. LISP performs map requests for these routes.

- **EID table**: Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority. Default: 1

Weight

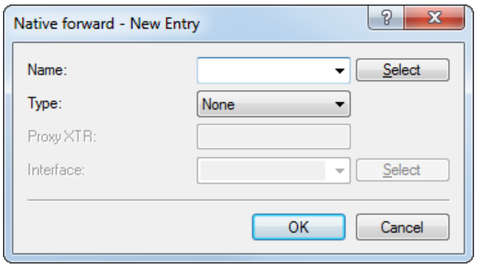
The weight. Default: 100

Native forward

If LISP networks are to communicate with non-LISP networks, proxy routers can be used. These roles are referred to as proxy ingress tunnel routers (proxy ITRs) and proxy egress tunnel routers (proxy ETRs).

If a LISP router receives a negative response from the map resolver, i.e. there is no mapping between the requested EID and an RLOC, the LISP router can either send the associated packets to a proxy xTR (packet with LISP header) or send it via another local interface (packet without LISP header).

LCOS only supports scenarios where PITR and PETR functions are operated on the same router.



Native forward - New Entry

Name:

Type: None

Proxy XTR:

Interface:

Name

References the name of the LISP instance.

Type

Defines how to send packets to non-LISP networks.

- **None**: Packets to non-LISP networks are not forwarded but dropped
- **Proxy XTR**: Packets to non-LISP networks are sent to a ProxyXTR
- **Interface**: Packets to non-LISP networks are sent via a local interface

Proxy XTR

IPv4 or IPv6 address of the proxy XTR used to send packets to non-LISP networks.

Interface

Name of the interface used to send packets to non-LISP networks.

3.2.2 LISP tutorial

In this tutorial we will configure a LISP network on the basis of an ARF network that is named INTRANET and uses tag 1. This involves registering the network prefix as an EID prefix with the MAP server 1.1.1.1. Registration is performed via the WAN remote site INTERNET (default route), which uses tag 0. The IP address of the INTERNET remote site can be dynamic or static. This address is registered as an RLOC address with the MAP server.

Data from the INTRANET should be sent to the LISP tunnel. For this purpose, the router requesting an unknown destination sends a map request to the MAP resolver 1.1.1.1.

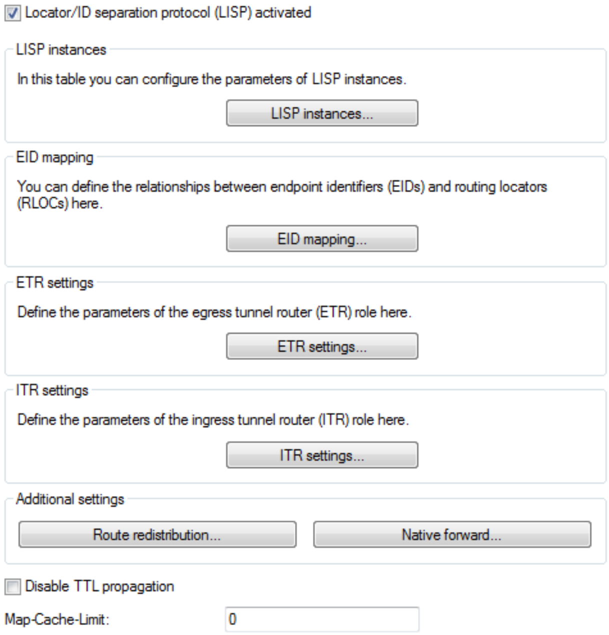
If the map resolver returns a positive mapping, LISP automatically establishes a dynamic tunnel to the remote LISP router and enters the corresponding routes into the routing table.

If the map resolver returns a negative mapping, i.e. the destination prefix is unknown or is not registered on the map server/resolver, then the packet can optionally be sent directly over the INTERNET remote site, without using a tunnel (native forward).

LISP routes do not have to be configured manually. LISP automatically creates routes and later deletes them.

As a matter of principle, entries for the routing tags have to be created manually in the WAN tag table.

1. First, enable the LISP protocol under **Routing protocols** > **LISP** > **Locator/ID separation protocol (LISP) activated**.



☑ Locator/ID separation protocol (LISP) activated

LISP instances

In this table you can configure the parameters of LISP instances.

EID mapping

You can define the relationships between endpoint identifiers (EIDs) and routing locators (RLOCs) here.

ETR settings

Define the parameters of the egress tunnel router (ETR) role here.

ITR settings

Define the parameters of the ingress tunnel router (ITR) role here.

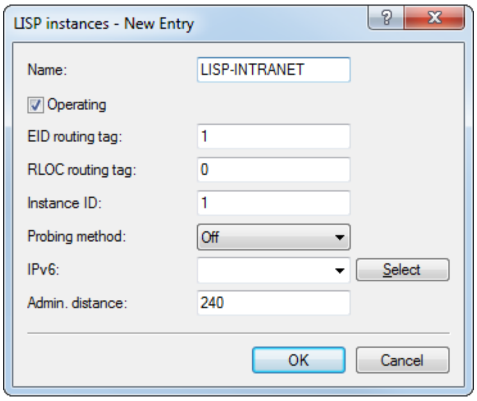
Additional settings

□ Disable TTL propagation

Map-Cache-Limit: 0

2. Create a new entry in the table of LISP instances. Do this by navigating to **Routing protocols** > **LISP** > **LISP instances** and then click on **Add**.
   a) Give this LISP instance a **Name**, e.g. LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **EID routing tag** to 1.
   d) Set the **RLOC routing tag** to the value of the tag of the WAN remote site INTERNET, in this case 0.
   e) Set the **Instance ID** to the value created on the LISP map server, in this case 1 like the tag of the INTRANET.

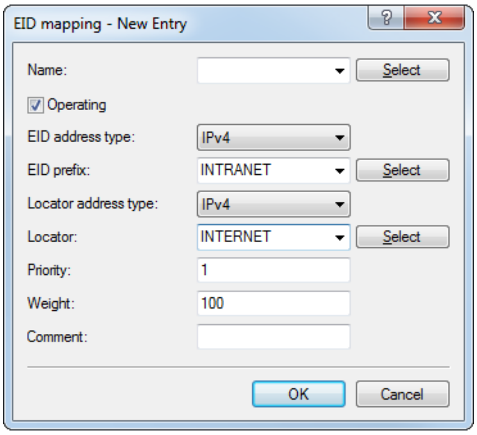
f) Under **IPv6** you can remove the entry **DEFAULT**, as we are only considering IPv4 here.



LISP instances - New Entry

Name:	LISP-INTRANET
☑ Operating	
EID routing tag:	1
RLOC routing tag:	0
Instance ID:	1
Probing method:	Off
IPv6:	
Admin. distance:	240

3. Create a new entry in the EID mapping table, which is used to link the EID prefix and the locator. Do this by navigating to **Routing protocols** > **LISP** > **EID mapping** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set both the **EID address type** and the **Locator address type** to IPv4.
   d) Set the **EID prefix** to INTRANET.
   e) Set the **Locator** to INTERNET.

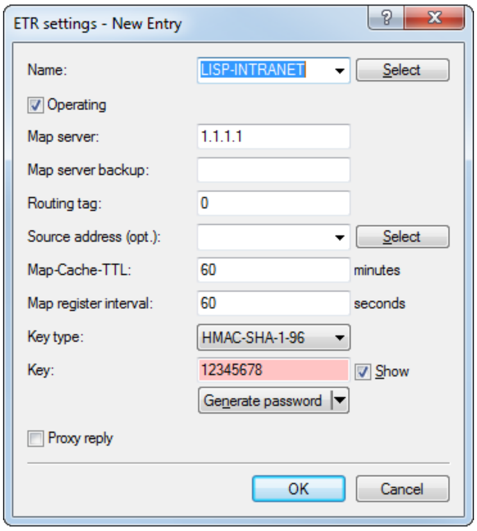


EID mapping - New Entry

Name:	
☑ Operating	
EID address type:	IPv4
EID prefix:	INTRANET
Locator address type:	IPv4
Locator:	INTERNET
Priority:	1
Weight:	100
Comment:	

4. In the ETR settings table, create a new entry containing the parameters for communication with the map server. Do this by navigating to **Routing protocols** > **LISP** > **ETR settings** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **Map server** to 1.1.1.1.
   d) Set the **Routing tag** to 0.

e) Set the **Key type** and the **Key** for connecting to the map server. These must match the type and password configured on the map server. In this example we take HMAC-SHA-1-96 and 12345678.



ETR settings - New Entry

Name: LISP-INTRANET

☑ Operating

Map server: 1.1.1.1

Map server backup:

Routing tag: 0

Source address (opt.):

Map-Cache-TTL: 60 minutes

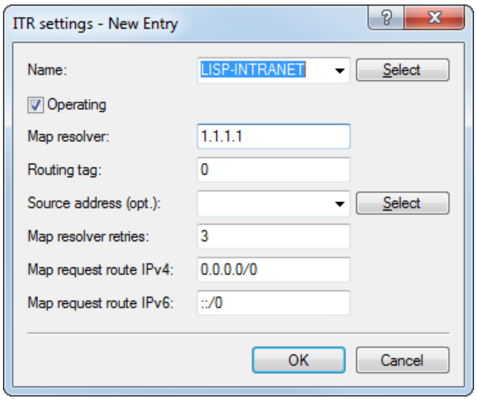
Map register interval: 60 seconds

Key type: HMAC-SHA-1-96

Key: 12345678 ☑ Show

☐ Proxy reply

5. In the ITR settings table, create a new entry containing the parameters for communications with the map resolver. Do this by navigating to **Routing protocols** > **LISP** > **ITR settings** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **Map resolver** to 1.1.1.1.
   d) Set the **Routing tag** to 0.



ITR settings - New Entry

Name: LISP-INTRANET

☑ Operating

Map resolver: 1.1.1.1

Routing tag: 0

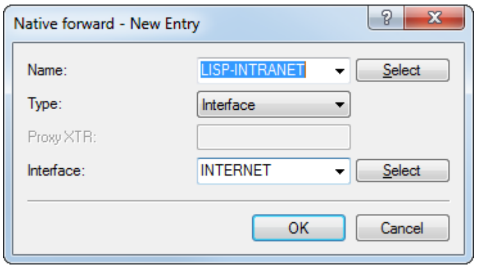
Source address (opt.):

Map resolver retries: 3

Map request route IPv4: 0.0.0.0/0

Map request route IPv6: ::/0

6. Optional: Packets to destinations that are not LISP networks can be sent directly via a local interface, i.e. without using the LISP tunnel. In our example, the interface to be used is INTERNET. Create a new entry in the Native forward table. Do this by navigating to **Routing protocols** > **LISP** > **Native forward** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Set the **Type** to **Interface**.
   c) Set the **Interface** to INTERNET.



Native forward - New Entry

Name: LISP-INTRANET

Type: Interface

Proxy XTR:

Interface: INTERNET

7. Navigate to **Communication** > **Remote sites** > **WAN tag table**, click on **Add** and create an entry for the LISP instance with the instance ID of 1 that you just created.

   For each LISP instance, an entry with the corresponding interface tag for the EID/ARF network must be created in the WAN tag table.

   Do this by creating each entry with the name for the remote site set to LISP-<LISP instance ID>*. The name of each remote site is formed from the keyword LISP supplemented by the corresponding LISP instance ID (in hexadecimal form) and the wildcard *. This unequivocally assigns the incoming traffic from the LISP tunnel to the EID/ARF network.

   The instance ID must be specified in hexadecimal without a leading 0x.

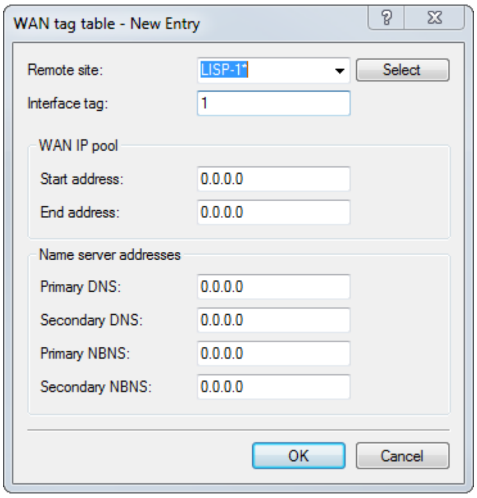
   Representation: LISP-<LISP instance ID>*

   Examples:

   - For LISP instance 1: LISP-1*
   - For LISP instance 15: LISP-F*

   a) Fill out the **Remote site** field as described above, i.e. the LISP instance with instance ID 1 takes the value “LISP-1*”.

   b) Set the **Interface tag** to 1.



Remote site: LISP-1*

Interface tag: 1

WAN IP pool

Start address: 0.0.0.0

End address: 0.0.0.0

Name server addresses

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Primary NBNS: 0.0.0.0

Secondary NBNS: 0.0.0.0

That's it!

3.2.3 Additions to the Setup menu

LISP

Settings for Locator / ID Separation Protocol (LISP).

SNMP ID:

2.93.4

Telnet path:

Setup > **Routing-Protocols**

Instances

This table contains the global configuration of the LISP instances on the device.

SNMP ID:

2.93.4.1

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

SNMP ID:

2.93.4.1.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Operating

Activates or deactivates this LISP instance.

SNMP ID:

2.93.4.1.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

No
Yes

EID-Rtg-Tag

Routing tag of the endpoint identifier (EID) of this instance.

SNMP ID:

2.93.4.1.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

RLOC-Rtg-Tag

Routing tag of the routing locator (RLOC) of this instance.

SNMP ID:

2.93.4.1.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

Instance-ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

SNMP ID:

2.93.4.1.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

Probing-Method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries.

SNMP ID:

2.93.4.1.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Off

The availability of the RLOCs is not checked periodically.

RLOC-Probing

The availability of the RLOCs is periodically checked by LISP RLOC messages.

IPv6

Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

SNMP ID:

2.93.4.1.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

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

Default:

600

Admin-Distance

Administrative routing distance.

SNMP ID:

2.93.4.1.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 3 characters from `[0-9]`

Default:

240

EID-Mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.

SNMP ID:

2.93.4.2

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.2.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

EID-Address-Type

This bitmask specifies the protocol version of the EID prefix when referencing the EID prefix via an interface or network name.

SNMP ID:

2.93.4.2.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

EID-Prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

SNMP ID:

2.93.4.2.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 43 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Locator-Address-Type

This bitmask specifies the protocol version of the RLOC when referencing the EID prefix via an interface name.

SNMP ID:

2.93.4.2.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

SNMP ID:

2.93.4.2.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Operating

SNMP ID:

2.93.4.2.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

No
Yes

Priority

The priority of the EID mapping.

SNMP ID:

2.93.4.2.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

Weight

The weight of the EID mapping.

SNMP ID:

2.93.4.2.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.93.4.2.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 25 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

ITR-Settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).

SNMP ID:

2.93.4.3

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.3.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

SNMP ID:

2.93.4.3.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

Activates or deactivates these ITR settings.

SNMP ID:

2.93.4.3.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

No
Yes

Loopback address

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

SNMP ID:

2.93.4.3.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

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

Rtg-Tag

Routing tag used to access the map resolver.

SNMP ID:

2.93.4.3.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Resolver-Retries

Number of retries for map requests to the map resolver.

SNMP ID:

2.93.4.3.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 3 characters from `[0-9]`

Default:

3

Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

SNMP ID:

2.93.4.3.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 18 characters from `[A-F][a-f][0-9]:.`

Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

SNMP ID:

2.93.4.3.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

ETR-Settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).

SNMP ID:

2.93.4.4

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.4.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Server

IPv4 or IPv6 address of the LISP map server

SNMP ID:

2.93.4.4.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

Activates or deactivates these ETR settings.

SNMP ID:

2.93.4.4.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

Loopback address

Contains the sender address as the named interface that is used with the map server in LISP communication.

SNMP ID:

2.93.4.4.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

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

Rtg-Tag

Routing tag to be used to access the map server.

SNMP ID:

2.93.4.4.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Cache-TTL-Minutes

Time-to-live of the EID mappings in minutes registered with the map server.

SNMP ID:

2.93.4.4.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Register-Interval-Seconds

Registration interval in seconds in which map registrations are sent to the map server.

SNMP ID:

2.93.4.4.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Key-Type

Algorithm used for authentication at the map server.

SNMP ID:

2.93.4.4.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

None
HMAC-SHA-1-96
HMAC-SHA-256-128

Key

Key or password used to register the EID mapping on the map server.

SNMP ID:

2.93.4.4.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

SNMP ID:

2.93.4.4.10

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

SNMP ID:

2.93.4.4.11

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

This item switches the routing protocol Locator / ID Separation Protocol (LISP) on or off.

SNMP ID:

2.93.4.5

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

Disable-TTL-Propagation

With this switch enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

SNMP ID:

2.93.4.7

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

SNMP ID:

2.93.4.8

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

Native-Forward

SNMP ID:

2.93.4.9

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.9.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Type

SNMP ID:

2.93.4.9.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

None
ProxyXTR
Interface

Proxy-XTR

SNMP ID:

2.93.4.9.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

Interface

SNMP ID:

2.93.4.9.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

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

Redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.

SNMP ID:

2.93.4.10

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.10.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Source

This bitmask specifies the route sources of the imported routes.

SNMP ID:

2.93.4.10.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Connected

From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.

Static

The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

OSPF

The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

BGP

The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

Destination

Specifies the destination of routes imported to LISP.

SNMP ID:

2.93.4.10.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Map-Cache

Imports the routes into the map cache. LISP performs map requests for these routes.

Eid-Table

Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

SNMP ID:

2.93.4.10.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Priority

The priority.

SNMP ID:

2.93.4.10.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

Weight

The weight of the EID mapping.

SNMP ID:

2.93.4.2.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

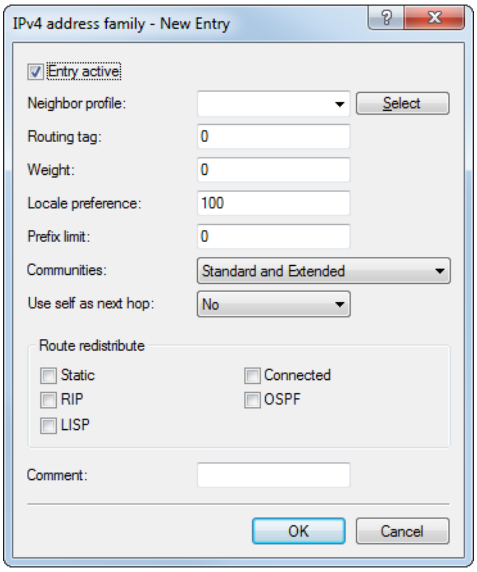
100

3.3 Route redistribution of LISP and RIP routes in BGP

As of LCOS version 10.20, route redistribution allows LISP and RIP routes be redistributed according to BGP. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by BGP.

ⓘ The redistribution of RIP routes is only supported for IPv4 routes.

There are two new switches for these features. In LANconfig, these are located under **Routing protocols** > **BGP** > **IPv4 address family**



IPv4 address family - New Entry

☑ Entry active

Neighbor profile: Select

Routing tag: 0

Weight: 0

Locale preference: 100

Prefix limit: 0

Communities: Standard and Extended

Use self as next hop: No

Route redistribute

□ Static □ Connected

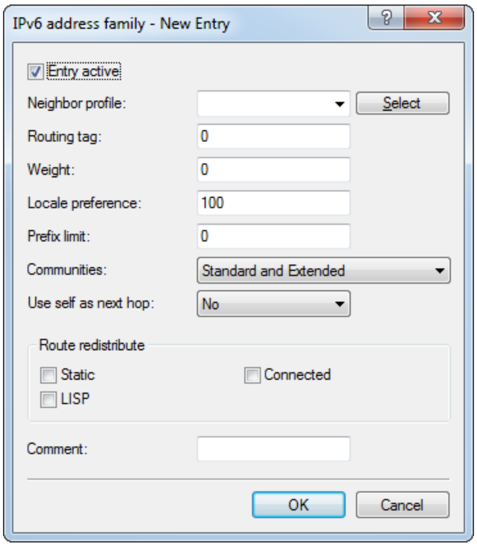
□ RIP □ OSPF

□ LISP

Comment:

OK Cancel

and **Routing protocols** > **BGP** > **IPv6 address family**, respectively.



IPv6 address family - New Entry

☑ Entry active

Neighbor profile: Select

Routing tag: 0

Weight: 0

Locale preference: 100

Prefix limit: 0

Communities: Standard and Extended

Use self as next hop: No

Route redistribute

□ Static □ Connected

□ LISP

Comment:

OK Cancel

If the LISP option is selected, the device distributes LISP routes from the routing table to the BGP neighbors. With the RIP option selected, the device distributes RIP routes from the routing table to the BGP neighbors.

3.3.1 Additions to the Setup menu

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

SNMP ID:

2.93.1.4.1.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

RIP

The device redistributes RIP routes from the routing table to the BGP neighbors.

OSPF

The device distributes OSPF routes from the routing table to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

SNMP ID:

2.93.1.4.2.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

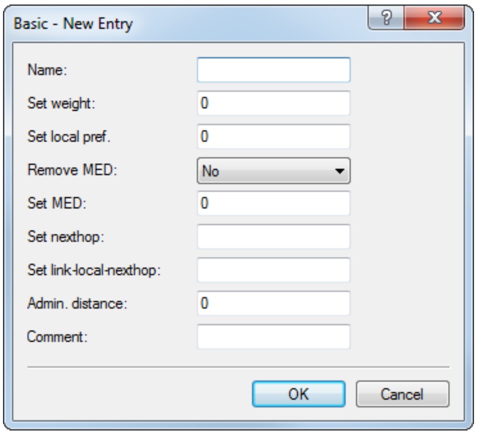
The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

3.4 BGP: Setting administrative distance by policy

In relation to BGP, the parameter **Admin. distance** under **Routing protocols** > **BGP** > **BGP policy** > **Basic** specifies the "administrative distance" entered into the routing table for the received prefixes.



Basic - New Entry

Name:	
Set weight:	0
Set local pref.:	0
Remove MED:	No
Set MED:	0
Set nexthop:	
Set link-local-nexthop:	
Admin. distance:	0
Comment:	

The list of fixed "administrative distances" for the various system services and routing protocols can be displayed on the command line by `show admin-distance`.

3.4.1 Additions to the Setup menu

Set-Admin-Distance

This parameter specifies the "administrative distance" given to prefixes received in the BGP when they are entered into the routing table. The list of fixed "administrative distances" for the various system services and routing protocols can be displayed on the CLI by show admin-distance.

SNMP ID:

2.93.1.5.2.1.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 3 characters from `[0-9]`

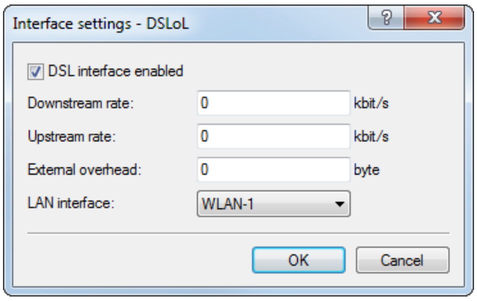
3.5 DSLoL for WLAN routers

IPv4 addresses can only be masked ("NAT") on WAN connections. If you want to masquerade in the direction of a LAN or WLAN interface, then the corresponding LAN or WLAN interface must be declared as a DSL port in order for it to establish a WAN connection (typically by IPoE or DHCPoE).

Until LCOS10.12, this was only possible for access points. From LCOS10.20, DSLoL is also available for WLAN routers.

An example scenario for DSLoL:

A WLAN router should be used to connect to the Internet primarily over WLAN. This is done using the WLAN client mode. If the WLAN is not available, the Internet connection should instead be established via LTE/4G as a backup. For this purpose, an LTE/4G connection is configured as usual, and the other WLAN-based Internet connection is set up by operating DSLoL on the WLAN interface. This is done in LANconfig under **Interfaces** > **WAN** > **Interface settings** > **DSLoL** by selecting the option **DSL interface enabled** and then setting the **LAN interface** to the WLAN that was earlier set up as the WLAN client.


Interface settings - DSLoL

☑ DSL interface enabled

Downstream rate: 0 kbit/s

Upstream rate: 0 kbit/s

External overhead: 0 byte

LAN interface: WLAN-1

The LTE/4G connection is now configured as a backup for the WLAN/DSLoL Internet connection.

4 IPv6

4.1 IPv6 WAN interface

The configuration logic of the IPv6 WAN interfaces has been changed. There is now a DEFAULT entry under **IPv6** > **General** > **WAN interfaces**. It is automatically selected for every remote station if you do not create another entry and select it at the remote site. For all remote stations, the configuration now has a new parameter **IPv6**, which allows you to select the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

ⓘ An entry in the WAN interfaces table can be referenced multiple times by remote sites.

4.1.1 Additions to the Setup menu

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.2.8

Telnet path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.19.19

Telnet path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.21.9

Telnet path:

Setup > **WAN** > **PPTP-peers**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.37.5

Telnet path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.51.11

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.19.9.20

Telnet path:

Setup > **VPN** > **VPN-Peers**

Possible values:

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

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.19.36.1.21

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

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

Default:

DEFAULT

Interface name

Give a name to the device IPv6 WAN interface here. This name is specified at the remote site. It is preset with a default entry. This is selected automatically if nothing is explicitly specified at the remote site. Leaving this entry blank causes IPv6 to be disabled for this interface.

An entry in the WAN interfaces table can be referenced multiple times by remote sites.

SNMP ID:

2.70.7.1

Telnet path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

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

Default:

DEFAULT

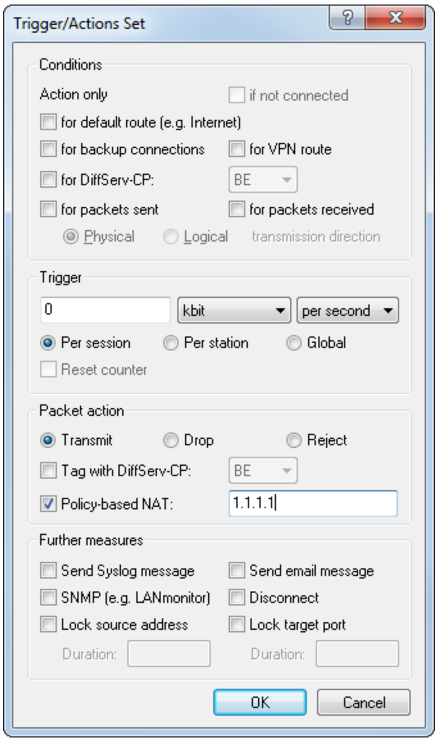
5 Firewall

5.1 WAN policy-based NAT

From LCOS version 10.20 it is possible to use WAN policy-based NAT.

WAN policy-based NAT allows address translation (masking) of connections based on firewall rules. You can now configure which of the WAN-IPv4 addresses assigned by the provider is to be used to mask internal addresses. This is ideal for scenarios where a provider assigns multiple static IPv4 addresses, e.g. for operating mail servers and web servers with different WAN addresses.

For this purpose, the firewall features the new packet option **Policy-based NAT** under **Firewall/QoS** > **IPv4 Rules** > **Action objects**. This action can be used together with the option **Transmit** and allows masking or NAT behind a specified IPv4 address.



Trigger/Actions Set

Conditions

Action only ☐ if not connected
☐ for default route (e.g. Internet)
☐ for backup connections ☐ for VPN route
☐ for DiffServ-CP: BE
☐ for packets sent ☐ for packets received
● Physical ○ Logical transmission direction

Trigger

0 kbit per second
● Per session ○ Per station ○ Global
☐ Reset counter

Packet action

● Transmit ○ Drop ○ Reject
☐ Tag with DiffServ-CP: BE
☑ Policy-based NAT: 1.1.1.1

Further measures

☐ Send Syslog message ☐ Send email message
☐ SNMP (e.g. LANmonitor) ☐ Disconnect
☐ Lock source address ☐ Lock target port
Duration: Duration:

The parameter must be entered as a fixed IP address. Dynamic IP addresses are not supported.

NAT is only possible if a WAN interface is involved. NAT between two LAN interfaces is not supported.

The CLI under (`/Setup/IP-Router/Firewall/Action-Table`) provides the variable `%Y` as an action.

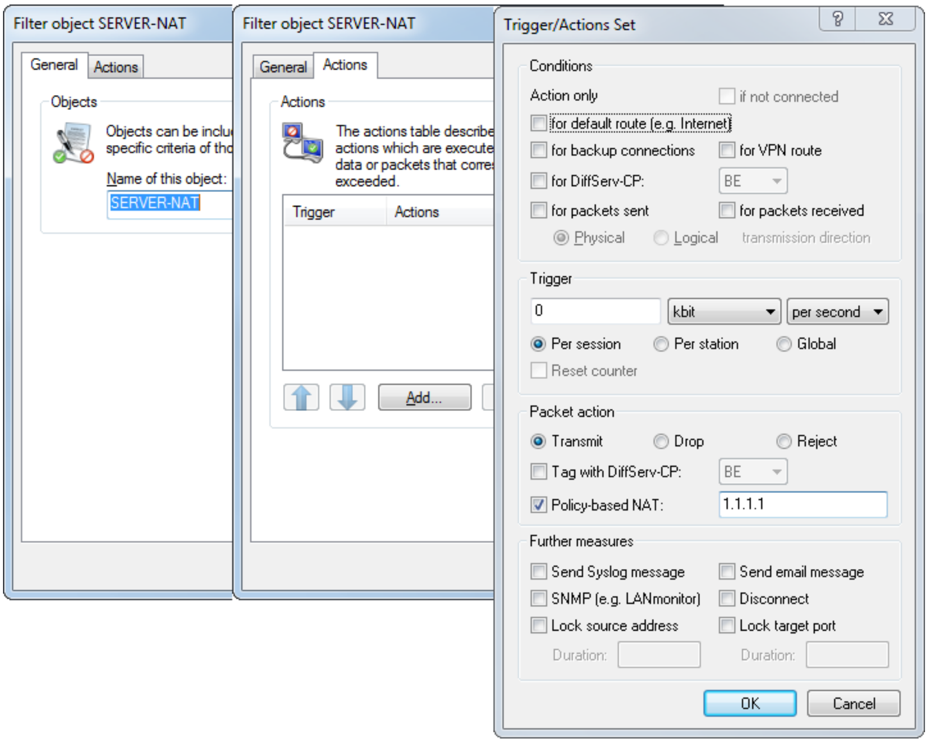
5.1.1 Configuring policy-based NAT with firewall rules

The following example configures an IPv4 network (intranet) with the subnet 192.168.80.0/24. The Internet provider has assigned a number of public IP addresses. Internet access has been set up using the Setup Wizard. Clients on the intranet are automatically masked behind the public IP address that was created with the Wizard.

Now we want to mask a server with the internal IP address 192.168.80.21 behind the public IP address 1.1.1.1.

The “return direction” of the masking, i.e. the server’s accessibility from the outside, is realized by a port-forwarding entry, which is not part of this example.

1. Create a new action object in the firewall under **Firewall/QoS** > **IPv4 rules** > **Action objects**. Under Action, set the packet action to **Transmit** and the **Policy-based NAT** to 1.1.1.1.



Filter object SERVER-NAT

General | Actions

Objects

Objects can be inclu
specific criteria of th

Name of this object: SERVER-NAT

Filter object SERVER-NAT

General | Actions

Actions

The actions table describe
actions which are execute
data or packets that corre
exceeded.

Trigger	Actions

Add...

Trigger/Actions Set

Conditions

Action only

□ if not connected

□ for default route (e.g. Internet)

□ for backup connections

□ for VPN route

□ for DiffServ-CP: BE

□ for packets sent

□ for packets received

● Physical ○ Logical transmission direction

Trigger

0 kbit per second

● Per session ○ Per station ○ Global

□ Reset counter

Packet action

● Transmit ○ Drop ○ Reject

□ Tag with DiffServ-CP: BE

☑ Policy-based NAT: 1.1.1.1

Further measures

□ Send Syslog message

□ Send email message

□ SNMP (e.g. LANmonitor)

□ Disconnect

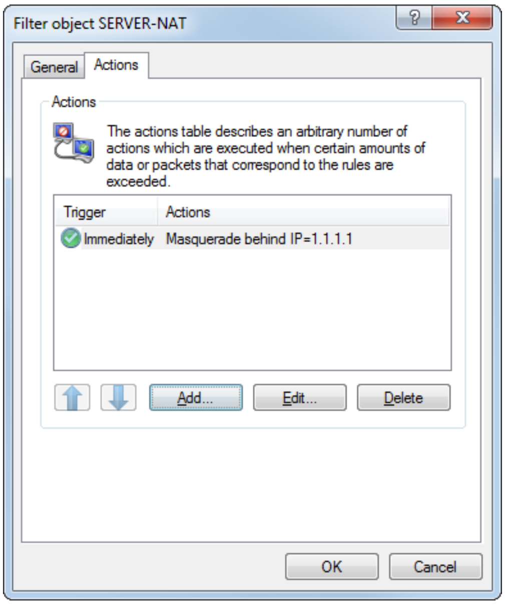
□ Lock source address

□ Lock target port

Duration:

Duration:

OK Cancel



Filter object SERVER-NAT

General | Actions

Actions

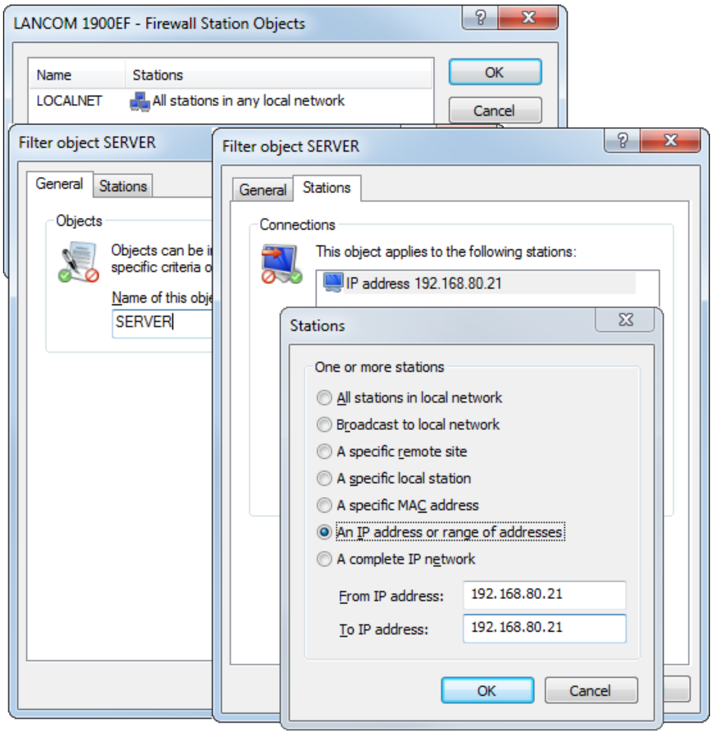
The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

Trigger	Actions
Immediately	Masquerade behind IP=1.1.1.1

Add... Edit... Delete

OK Cancel

2. Under **Firewall/QoS** > **IPv4 rules** > **Station objects** create a new station object defined for the IP address 192.168.80.21.



LANCOM 1900EF - Firewall Station Objects

Name	Stations
LOCALNET	All stations in any local network

Filter object SERVER

General | Stations

Objects

Objects can be i
specific criteria o

Name of this obj
SERVER

Filter object SERVER

General | Stations

Connections

This object applies to the following stations:

IP address 192.168.80.21

Stations

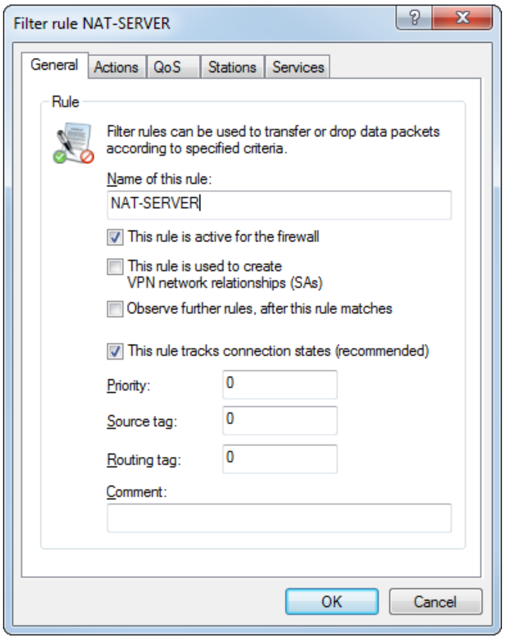
One or more stations

○ All stations in local network
○ Broadcast to local network
○ A specific remote site
○ A specific local station
○ A specific MAC address
● An IP address or range of addresses
○ A complete IP network

From IP address: 192.168.80.21

To IP address: 192.168.80.21

3. Next, go to **Firewall/QoS** > **IPv4 rules** > **Firewall rules** and create a filter rule.



Filter rule NAT-SERVER

General | Actions | QoS | Stations | Services

Rule

Filter rules can be used to transfer or drop data packets according to specified criteria.

Name of this rule:
NAT-SERVER

☑ This rule is active for the firewall

☐ This rule is used to create
VPN network relationships (SAs)

☐ Observe further rules, after this rule matches

☑ This rule tracks connection states (recommended)

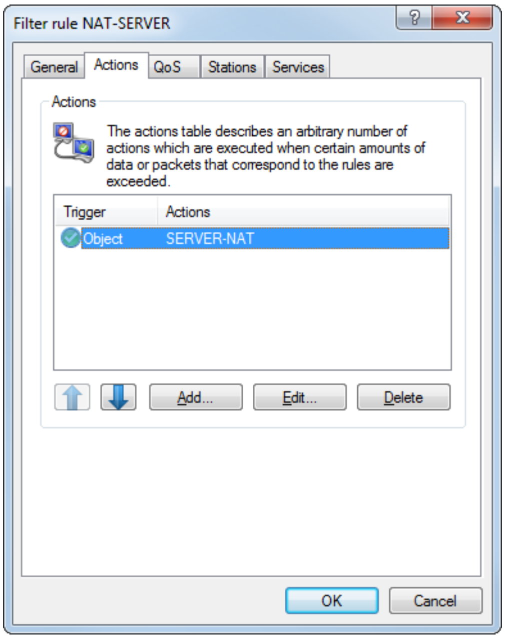
Priority: 0

Source tag: 0

Routing tag: 0

Comment:

4. In this filter rule, go to **Actions** and select the new action “SERVER-NAT” that was defined above.



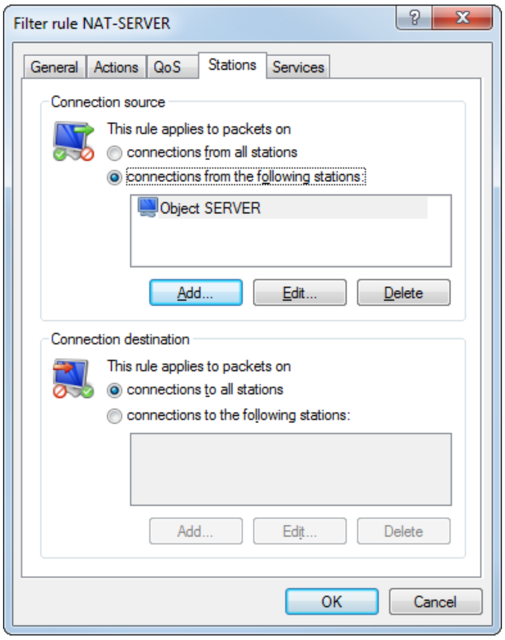
Filter rule NAT-SERVER

Actions

The actions table describes an arbitrary number of actions which are executed when certain amounts of data or packets that correspond to the rules are exceeded.

Trigger	Actions
Object	SERVER-NAT

5. Then go to **Stations** and use the newly created station object. If necessary. you can also specify the Internet line under **Connection destination**.



Filter rule NAT-SERVER

Connection source

This rule applies to packets on

○ connections from all stations

● connections from the following stations:

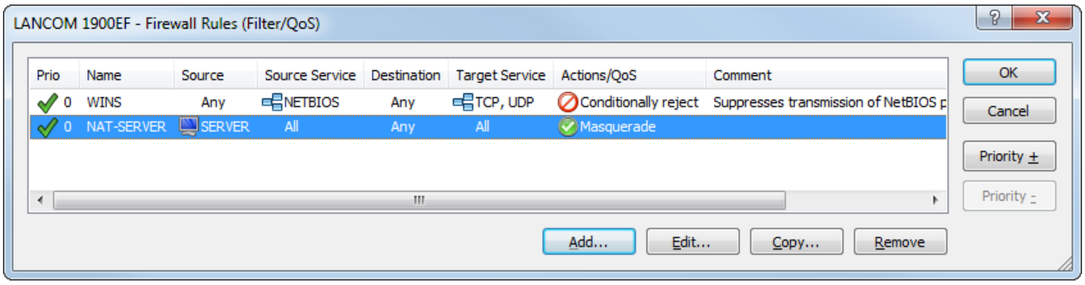
Object SERVER

Connection destination

This rule applies to packets on

● connections to all stations

○ connections to the following stations:



LANCOM 1900EF - Firewall Rules (Filter/QoS)

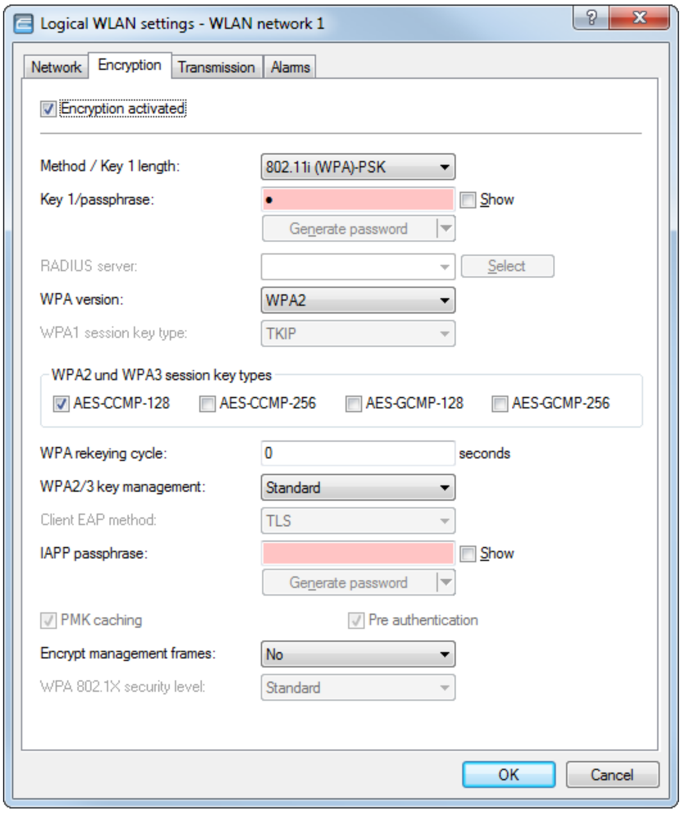
Prio	Name	Source	Source Service	Destination	Target Service	Actions/QoS	Comment
✓ 0	WINS	Any	NETBIOS	Any	TCP, UDP	Conditionally reject	Suppresses transmission of NetBIOS p
✓ 0	NAT-SERVER	SERVER	All	Any	All	Masquerade	

6 Wireless LAN – WLAN

6.1 WLAN encryption settings moved to the logical WLAN settings

To simplify the task of configuration, the WLAN encryption settings now appear as an additional tab in the dialog for the Logical WLAN settings. When configuring an SSID, it is no longer necessary to switch back and forth between the logical WLAN settings dialog and the WLAN encryption settings dialog.

The logical WLAN settings are to be found under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**.



☑ Encryption activated

Method / Key 1 length: 802.11i (WPA)-PSK

Key 1/passphrase: • □ Show

RADIUS server:

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 und WPA3 session key types

☑ AES-CCMP-128 □ AES-CCMP-256 □ AES-GCMP-128 □ AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Standard

Client EAP method: TLS

IAPP passphrase: □ Show

☑ PMK caching ☑ Pre authentication

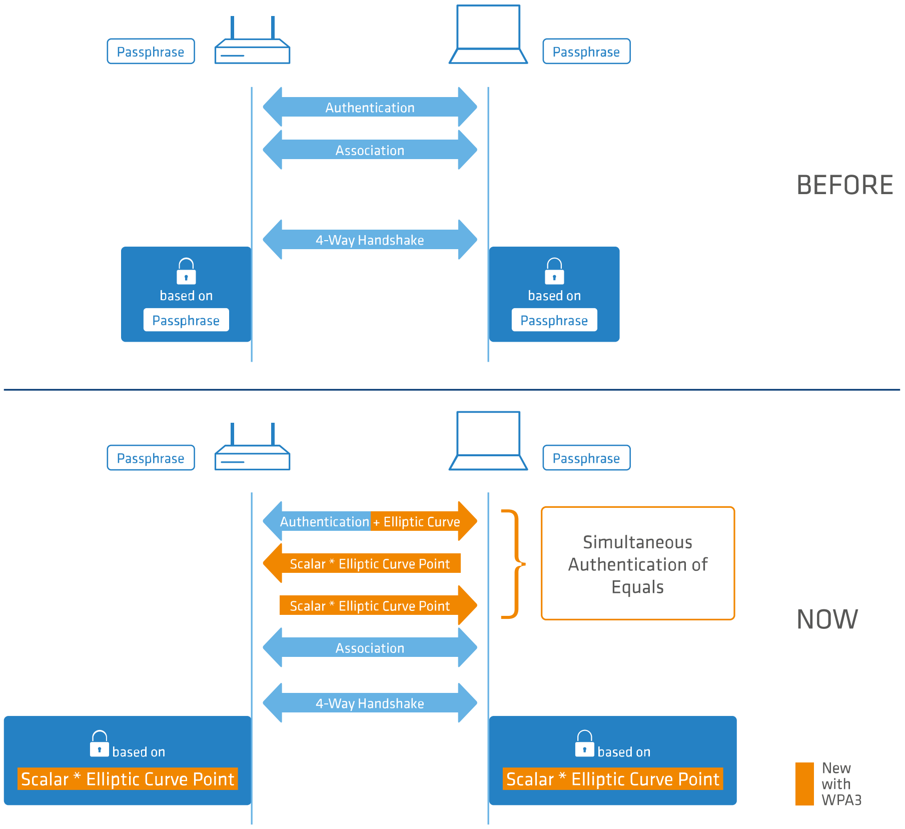
Encrypt management frames: No

WPA 802.1X security level: Standard

6.2 WPA3 (Wi-Fi Protected Access 3)

Compared to the predecessor standard WPA2 introduced by the Wi-Fi Alliance in 2004, the WPA3 standard introduced in 2018 offers improved security by combining various security methods. Like WPA2, WPA3 also exists in the versions WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) authentication method, which only requires a password for authentication but which prevents brute-force and dictionary attacks. Furthermore, for the first time this method offers forward secrecy, i.e. captured WPA3-secured traffic cannot be decrypted subsequently after the attacker gains knowledge of the pre-shared key.


Passphrase
Passphrase
Authentication
Association
BEFORE
4-Way Handshake
based on
Passphrase
based on
Passphrase
Passphrase
Passphrase
Authentication + Elliptic Curve
Scalar * Elliptic Curve Point
Scalar * Elliptic Curve Point
Simultaneous Authentication of Equals
NOW
Association
4-Way Handshake
based on
Scalar * Elliptic Curve Point
based on
Scalar * Elliptic Curve Point
New with WPA3

Also available with WPA3 is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Both variants now require the use of protected management frames (PMF) according to IEEE 802.11w. PMF prevents attackers from computing the WLAN password from captured material gained by using fake management frames to force a disassociation and then eavesdropping the re-authentication.

6.2.1 WPA3-Personal

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

With **WPA3** selected, only WLAN clients that support WPA3-Personal will be able to login. This configuration enforces authentication with the Simultaneous Authentication of Equals (SAE). Similarly, this SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

6.2.2 WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Rather, it set out policies to ensure greater consistency in the application of these protocols and to assure the desired level of security.

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

By selecting **WPA3**, only WLAN clients that support WPA3-Enterprise will be able to log in. This SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

Suite B cryptography

Also available is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

> Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

The switch **WPA 802.1X security level** under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings** is used to enable the optional Suite B encryption. With “Suite B 192 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

> Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

> If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

With “Suite B 128 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

> Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-128 is also enforced.

Because the session key types AES-GCMP-128 and AES-GCMP-256 are not supported by all WLAN modules, the use of Suite B cryptography may be limited or impossible, depending on the device type.

> If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

6.2.3 WPA3 device support

The following table shows which access points and WLAN routers support WPA3-Personal, WPA3-Enterprise and WPA3-Enterprise incl. Suite B/192-bit encryption. For devices featuring a second WLAN module, this is shown separately for both modules.

AP model	WLAN-1	WLAN-2
LN-170x	> WPA3-Personal > WPA3-Enterprise incl. Suite B	> WPA3-Personal > WPA3-Enterprise incl. Suite B
LN-86x	> WPA3-Personal > WPA3-Enterprise incl. Suite B	> WPA3-Personal > WPA3-Enterprise incl. Suite B
LN-830(E) / L-822	> WPA3-Personal > WPA3-Enterprise incl. Suite B	> WPA3-Personal > WPA3-Enterprise
LN-630	> WPA3-Personal > WPA3-Enterprise incl. Suite B	> WPA3-Personal > WPA3-Enterprise
L-330 / L-322 / L-321 / L-151	> WPA3-Personal > WPA3-Enterprise incl. Suite B	> WPA3-Personal > WPA3-Enterprise incl. Suite B
OAP-821 / IAP-821	> WPA3-Personal > WPA3-Enterprise	> WPA3-Personal > WPA3-Enterprise
OAP-822 / OAP-830 / IAP-822	> WPA3-Personal > WPA3-Enterprise	> WPA3-Personal > WPA3-Enterprise
1780EW-4G+	> WPA3-Personal > WPA3-Enterprise	No second WLAN interface installed
All other WLAN routers	> WPA3-Personal > WPA3-Enterprise incl. Suite B	No second WLAN interface installed

6.2.4 Additions to the Setup menu

WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

SNMP ID:

2.23.20.3.9

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default:

WPA2

SAE-Groups

The authentication method SAE (Simultaneous Authentication of Equals) uses elliptic curves. Further information is available from the *Standards for Efficient Cryptography Group*.

SNMP ID:

2.23.20.3.26

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

secp256r1
secp384r1
secp521r1
secp192r1
secp224r1

Default:

secp256r1

secp384r1

secp521r1

WPA2-3-Session-Keytypes

ⓘ From LCOS 10.20 this setting replaces the value 2.23.20.3.13 **WPA2-Session-Keytypes**.

Here you select the methods that users should be offered to generate the WPA session or group keys. The following Advanced Encryption Standard (AES) methods can be offered.

SNMP ID:

2.23.20.3.27

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

AES-CCMP-128
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default:

AES-CCMP-128

WPA 802.1X security level

Setting the 802.1X security level. WPA3 features the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments.

ⓘ Operating CNSA Suite B cryptography requires the use of certain cipher suites. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP128 is also enforced with “Suite B 128 bits”.

ⓘ If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

SNMP ID:

2.23.20.3.28

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Default

Suite-B 128-bit

Enabled “Suite B 128 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Suite-B 128-bit

Enabled “Suite B 192 bits”. The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Default:

Default

6.3 Enhanced Open

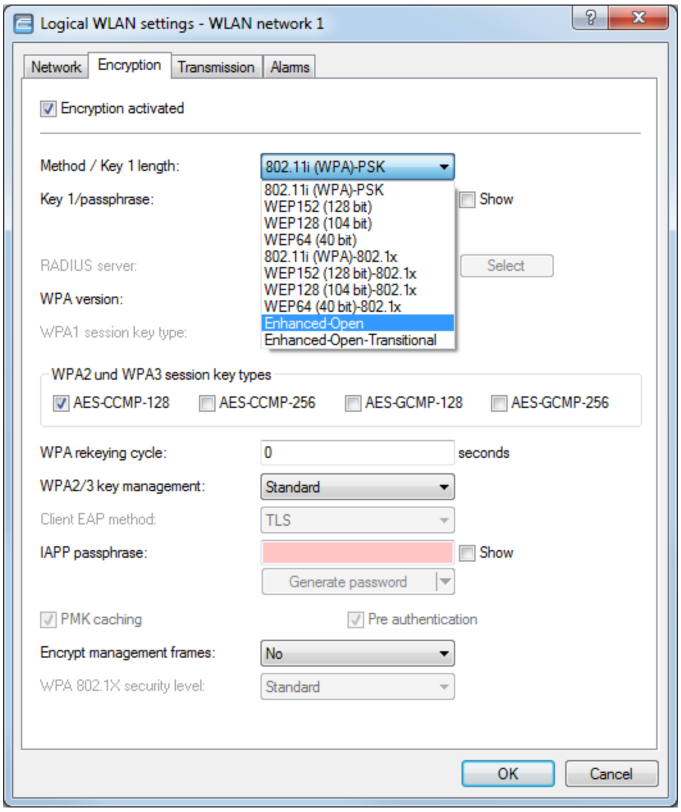
Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. Also, the widespread practice of securing a hotspot with WPA2-PSK and publicly posting the shared key provides limited security. Since WPA2-PSK does not provide Perfect Forward Secrecy, an attacker who knows the key can use it to decrypt recordings of data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot.

Public Spot with Enhanced Open

To use Enhanced Open with the Public Spot, see *Setting up a secure hotspot with Enhanced Open*.

Configuration

Enhanced Open is set as the WLAN encryption method under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. That is all you need to do to encrypt communications for clients that support this method.



Logical WLAN settings - WLAN network 1

Network | Encryption | Transmission | Alarms

☑ Encryption activated

Method / Key 1 length: 802.11i (WPA)-PSK

- 802.11i (WPA)-PSK
- WEP152 (128 bit)
- WEP128 (104 bit)
- WEP64 (40 bit)
- 802.11i (WPA)-802.1x
- WEP152 (128 bit)-802.1x
- WEP128 (104 bit)-802.1x
- WEP64 (40 bit)-802.1x
- Enhanced-Open
- Enhanced-Open-Transitional

Key 1/passphrase: □ Show

RADIUS server: Select

WPA version:

WPA1 session key type:

WPA2 und WPA3 session key types

☑ AES-CCMP-128 □ AES-CCMP-256 □ AES-GCMP-128 □ AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Standard

Client EAP method: TLS

IAPP passphrase: □ Show

Generate password

☑ PMK caching ☑ Pre authentication

Encrypt management frames: No

WPA 802.1X security level: Standard

OK Cancel

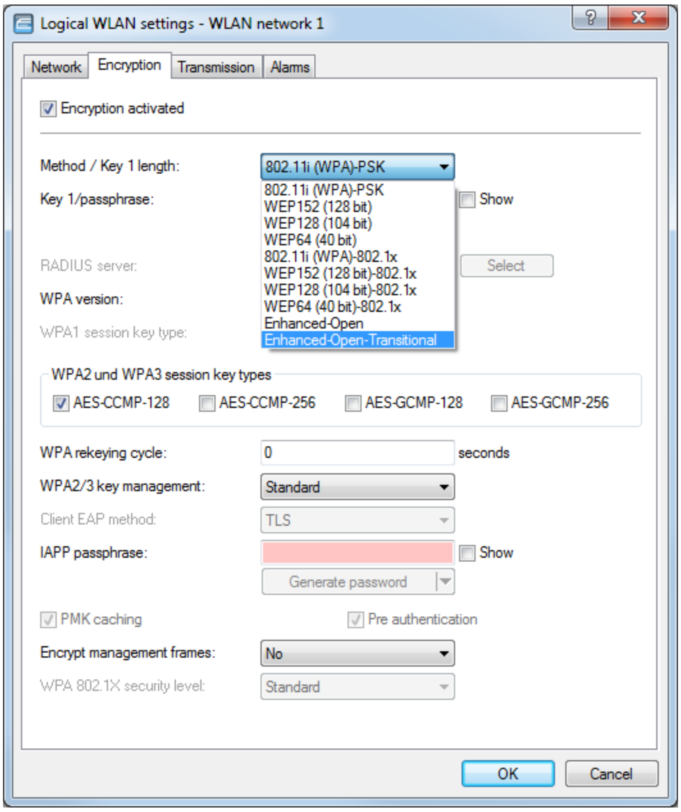
6.3.1 Enhanced Open Transitional mode

The Enhanced Open Transitional mode allows connections to clients that support Enhanced Open and also to those that do not yet support Enhanced Open. With the transitional mode in operation, the regular Enhanced Open SSID is operated in parallel to an unencrypted/open SSID with the same name and otherwise identical settings.

A prerequisite for this is that at least one other SSID is available and unused on the selected radio module. Depending on the device, a total of 15 or 16 SSIDs are available per radio module. If no SSID is available, both the Enhanced Open Transitional SSID and the actual Enhanced Open SSID will not be activated.

Configuration

The Enhanced Open Transitional mode is set as the WLAN encryption method under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**.



Logical WLAN settings - WLAN network 1

Network | Encryption | Transmission | Alarms

☑ Encryption activated

Method / Key 1 length: 802.11i (WPA)-PSK

- 802.11i (WPA)-PSK
- WEP152 (128 bit)
- WEP128 (104 bit)
- WEP64 (40 bit)
- 802.11i (WPA)-802.1x
- WEP152 (128 bit)-802.1x
- WEP128 (104 bit)-802.1x
- WEP64 (40 bit)-802.1x
- Enhanced-Open
- Enhanced-Open-Transitional

Key 1/passphrase: □ Show

RADIUS server: Select

WPA version:

WPA1 session key type:

WPA2 und WPA3 session key types

☑ AES-CCMP-128 □ AES-CCMP-256 □ AES-GCMP-128 □ AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Standard

Client EAP method: TLS

IAPP passphrase: □ Show

Generate password

☑ PMK caching ☑ Pre authentication

Encrypt management frames: No

WPA 802.1X security level: Standard

OK Cancel

6.3.2 Additions to the Setup menu

Method

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Please consider that not all wireless cards support all encryption methods.

SNMP ID:

2.23.20.3.4

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

802.11i-WPA-PSK
WEP-128-Bits
WEP-104-Bits
WEP-40-Bits
802.11i-WPA-802.1X
WEP-128-Bits-802.1X
WEP-104-Bits-802.1X
WEP-40-Bits-802.1X
Enhanced-Open
Enhanced-Open-Transitional

Default:

802.11i-WPA-PSK

Enhanced-Open-Groups

The authentication method Enhanced Open uses elliptic curves.

SNMP ID:

2.23.20.3.22

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

6.4 LANCOM Enhanced Passphrase Security (LEPS)

The encryption method WPA2 protects data traffic in the WLAN from “interception”. The required passphrase is easily handled as a central key; a RADIUS server such as that for 802.1X installations is not required.

Nevertheless, the tap-proof WPA2 method still has some weaknesses:

- One passphrase applies **globally** for **all** WLAN clients
- The passphrase may fall into unauthorized hands if treated carelessly

- A “leaked” passphrase then offers any attacker free access to the wireless network

This means in practice that: Should the passphrase “go missing” or if an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point needs to be changed in the interests of security—in every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients. In the case mentioned above, the situation of an employee leaving the company requires merely his “personal” passphrase to be deleted; all others remain valid and confidential.

With LEPS, LANCOM Systems GmbH Systems has developed two efficient methods that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoid the potential security loopholes that come with global passphrases.

LEPS-U (LANCOM Enhanced Passphrase Security User) assigns an individual password for the SSID to each individual client or to entire groups. LEPS-MAC (LANCOM Enhanced Passphrase Security MAC) additionally authenticates the clients by their MAC address, which is ideal for secure enterprise networks.

6.4.1 LANCOM Enhanced Passphrase Security User (LEPS-U)

LANCOM Enhanced Passphrase Security Users (LEPS-U) allows a set of passphrases to be configured and assigned to individual users or groups. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

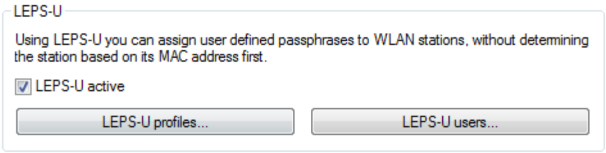
This is useful for onboarding devices into the network. For example, a network operator “onboarding” multiple WLAN devices into different areas of the network does not want to configure each specific device; instead this should done by the users of the devices themselves. In this case, users are given a preshared key for the company WLAN for use with their own devices. The preshared key is used to map each user to a VLAN, thus automatically assigning them to a specific network. The configuration of LEPS-U takes place on the infrastructure side only, which assures full compatibility to third-party products.

The security issue presented by global passphrases is fundamentally remedied by LEPS-U. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should “get lost” or an employee with knowledge of their passphrase leaves the company, then only the passphrase of that user needs to be changed or deleted. All other passphrases remain valid and confidential.

For technical reasons, LEPS-U is only compatible with WPA version WPA2.

Configuration

The **LEPS-U profiles** and **LEPS-U users** are configured in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS-U**. The switch **LEPS-U active** enables the LEPS-U feature.



LEPS-U

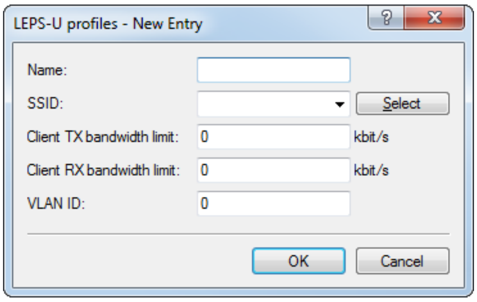
Using LEPS-U you can assign user defined passphrases to WLAN stations, without determining the station based on its MAC address first.

☑ LEPS-U active

When configured in LEPS-U, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. This is done with LEPS-U profiles, which avoids having to repeat all of the settings for every new user. You then create the LEPS-U users with their individual passphrases and link them to one of the LEPS-U profiles created previously.

LEPS-U profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users.



LEPS-U profiles - New Entry

Name:

SSID:

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

VLAN ID: 0

Name

Enter a unique name for the LEPS-U profile here.

SSID

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

Client RX bandwidth limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

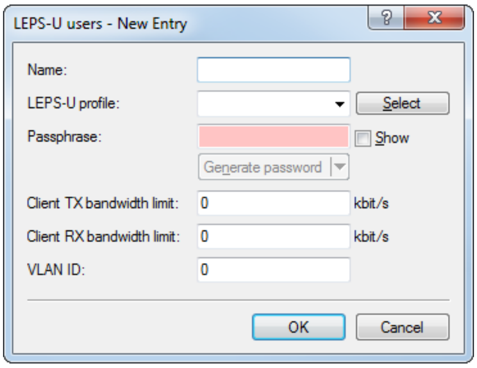
LEPS-U users

Create individual LEPS-U users here. Each LEPS-U user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.

ⓘ There are platform-specific restrictions on the number of LEPS-U users created at the same time.

Device	Users
L-15x, L-3xx, OAP-32x, OAP-8xx, IAP-32x, IAP-82x, LN-630acn	> up to 300 users per SSID > Access Point total: 2,000 users
L-45x, L(N)-8xx, L-13xx, LN-17xx	> per SSID up to 1,000 users

Device	Users
	> Access Point total: 6,000 users


LEPS-U users - New Entry

Name:

LEPS-U profile:

Passphrase:

□ Show

Client TX bandwidth limit: 0 kbit/s

Client RX bandwidth limit: 0 kbit/s

VLAN ID: 0

Name

Enter a unique name for the LEPS-U user here.

LEPS-U profiles

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

Passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

> The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Client RX bandwidth limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

6.4.2 LANCOM Enhanced Passphrase Security MAC (LEPS-MAC)

LEPS-MAC uses an additional column in the ACL (access-control list) to assign an **individual** passphrase consisting of any 8 to 63 ASCII characters to each MAC address. Authentication at the access point is only possible with the correct combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS-MAC thus shuts out a potential attack on the ACL. If WPA2 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN as the combination of MAC address and passphrase requires both to be known before an encryption can be negotiated.

LEPS-MAC can be used both locally in the device and centrally managed by a RADIUS server. LEPS-MAC works with all WLAN client adapters available on the market without any modification. Full compatibility to third-party products is assured as LEPS-MAC only involves configuration in the access point.

Compared to LEPS-U, the administrative overhead is slightly higher because the MAC address has to be entered for each device.

Configuration

The configuration of LEPS-MAC involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. This is done either with an entry in the list under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules** or in the RADIUS server. One entry is generated per MAC address—from the point of view of the RADIUS server, the MAC address is therefore a user. It is also necessary to activate the MAC filter under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**, i.e. data will be transmitted for the WLAN clients entered here.

! The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

ℹ If you are storing client-specific passphrases in the user table of a RADIUS server, a LAN-based device can serve as the central RADIUS server and take advantage of LEPS-MAC.

6.4.3 Additions to the Setup menu

LEPS-U

LANCOM Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

SNMP ID:

2.12.133

Telnet path:

Setup > **WLAN**

Operating

Switches LEPS-U on or off. When switched off, LEPS-U users are ignored during WLAN client authentication.

SNMP ID:

2.12.133.1

Telnet path:

Setup > **WLAN** > **LEPS-U**

Possible values:

No
Yes

Default:

No

Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.12.133.2

Telnet path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U profile here.

SNMP ID:

2.12.133.2.1

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.12.133.2.2

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.12.133.2.3

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.12.133.2.4

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

SNMP ID:

2.12.133.2.5

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 4 characters from [0-9]

Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

SNMP ID:

2.12.133.3

Telnet path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U user here.

SNMP ID:

2.12.133.3.1

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.12.133.3.2

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

SNMP ID:

2.12.133.3.3

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 63 characters from `` [A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ` ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.4

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.5

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.6

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0-9]`

LEPS-U

LANCOM Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

SNMP ID:

2.37.1.25

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration**

Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.37.1.25.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

Name

Enter a unique name for the LEPS-U profile here.

SNMP ID:

2.37.1.25.1.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

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

Network profile

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.37.1.25.1.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

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

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.37.1.25.1.3

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.37.1.25.1.4

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

SNMP ID:

2.37.1.25.1.5

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 4 characters from `[0-9]`

Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

SNMP ID:

2.37.1.25.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

Name

Enter a unique name for the LEPS-U user here.

SNMP ID:

2.37.1.25.2.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

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

Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.37.1.25.2.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

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

WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

SNMP ID:

2.37.1.25.2.3

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 63 characters from `` [A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ` ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.4

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.5

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.6

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0-9]`

6.5 Client Management

With Client Management, Wi-Fi clients are steered to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular band steering and client steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

Compared to the previous client steering feature supported by WLCs, Client Management operates independently and without a WLC. The access points communicate with one another using the protocol IAPP.

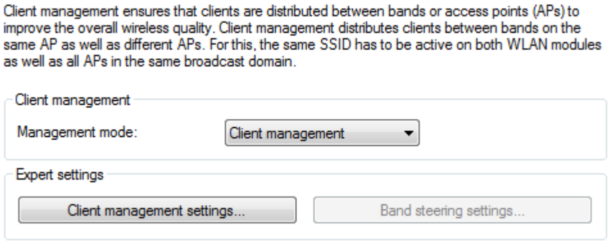
For the access points to communicate with one another, they need to be able to exchange IAPP messages. IAPP messages are transmitted by multicast. If necessary, the infrastructure—and switches in particular—requires exemptions to be created for IGMP snooping or other filtering mechanisms. IAPP uses the multicast group 224.0.1.76.

LANCOM switches in the default setting are already set up correctly for Client Management.

In this way Client Management ensures that clients are evenly distributed across the frequency bands and access points to optimize overall WLAN performance. A requirement for this is that the WLAN modules and access points in a broadcast domain all transmit on the same SSID.

6.5.1 Configuration of Client Management

Client Management is switched on and off under **Wireless LAN** > **Client Management** > **Client Management** > **Management mode**. For new installations, this is turned on by default and usually does not require any special settings. As an alternative for access points with multiple WLAN modules, **AP-based band steering** can also be activated.



Client management ensures that clients are distributed between bands or access points (APs) to improve the overall wireless quality. Client management distributes clients between bands on the same AP as well as different APs. For this, the same SSID has to be active on both WLAN modules as well as all APs in the same broadcast domain.

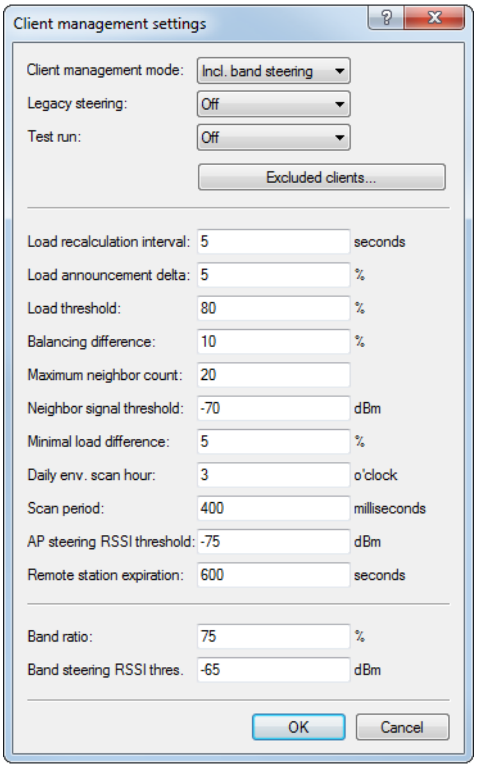
Client management

Management mode: Client management

Expert settings

Expert settings

The settings for Client Management are configured under **Wireless LAN** > **Client Management** > **Expert settings** > **Client Management**. The default settings are ideal for operating Client Management in offices and school environments.



Client management settings

Client management mode: Incl. band steering

Legacy steering: Off

Test run: Off

Load recalculation interval: 5 seconds

Load announcement delta: 5 %

Load threshold: 80 %

Balancing difference: 10 %

Maximum neighbor count: 20

Neighbor signal threshold: -70 dBm

Minimal load difference: 5 %

Daily env. scan hour: 3 o'clock

Scan period: 400 milliseconds

AP steering RSSI threshold: -75 dBm

Remote station expiration: 600 seconds

Band ratio: 75 %

Band steering RSSI thres.: -65 dBm

Client Management mode

Access points with multiple WLAN modules can operate Client Management with and without band steering.

Default setting:with band steering

Legacy steering

Configures whether clients that do not fully support 802.11v are also directed to other access points by Client Management. Even with legacy steering activated, Client Management first steers the 802.11v-capable clients to other access points; only then does it steer the clients that do not support 802.11v. Legacy steering forcibly disconnects these clients from the WLAN. The AP prevents the client from re-associating with it for a certain period, so that the client itself selects another access point. Compared to clients steered with 802.11v, this can lead to a poorer user experience, although this depends mainly on the behavior of the legacy clients.

Default setting: Off

Test run

Operates the Client Management in test mode: Environment scans are performed and steering decisions are made by the system and recorded to the syslog, but no actual client steering takes place. Use the test run to test the behavior of Client Management without actually making changes to your network.

Default setting: Off

Excluded clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering.

Use the table to configure the MAC addresses of the clients that are to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

Load recalculation interval

Configures the interval at which the load on the AP is calculated and decisions are made to steer the clients. Increase the value to reduce the load on the network. Decrease the value to steer clients faster. Values < 2 seconds are not recommended as this negatively impacts network performance. Values > 10 seconds are not recommended as client steering does not happen in time. We recommend that you use the default value.

Default value: 5 seconds

Load announcement delta

Configures the percentage change in current load at which an access point communicates the load to other access points outside of the regular announcement interval. Increase the value in installations with many mobile clients. Decrease the value in installations with fewer moving clients. The default setting has been chosen for office and school environments. Note that this value should be lower than the value configured for the balancing difference to avoid miscalculations.

Default value: 5 %

Load threshold

Configures the load threshold at which the access point starts steering regardless of the load threshold of the neighbor access points. Increase the value in low-quality/high-density scenarios such as stadiums. Decrease the value in high-quality/high-throughput scenarios such as offices/schools.

Default value: 80 %

Balancing difference

Configures the load difference between access points at which clients are steered to the access point with the lesser load. High values lead to less balanced installations, low values lead to more steering of the clients. Increase the value if excessive client steering is happening. Decrease the value to achieve maximum balancing across the installation. The default setting has been chosen for office and school environments.

Default value: 10 %

Maximum neighbor count

Configures the number of neighbor access points that Client Management on this access point takes into consideration. In high-density scenarios, a lower number can be advantageous as clients are predominantly steered to nearby access points and less management communication is required between the access points. Values < 4 are not recommended, as there are not enough available access points for useful steering decisions. Values > 72 are not supported due to limitations of the 802.11 protocol.

Default value: 20 APs

Neighbor signal threshold

Configures the signal strength that an AP must display in order to be classified as a neighbor access point. Increase the value for high-density scenarios (for example: -60, -50). Decrease the value for scenarios where widespread coverage is required (e.g. -80, -90).

Default value: -70 dBm

Minimum load difference

Configures the minimum load difference between neighboring access points for steering to be performed between these access points. Steering is only performed when the configured load threshold is exceeded. To avoid miscalculation, the minimum load difference should not exceed the value for balancing difference. Increase the value for less steering in the installation. Decrease the value for more steering in the installation.

Default value: 5 %

Daily env. scan hour

Configures the time (00-23) at which the daily environment scan is performed as required by Client Management. The exact time of the scan is spread over a 30-minute window to minimize conflicts between concurrent environment scans. The environment scan takes about 15 seconds. No WLAN data is exchanged while the WLAN module is scanning.

Default value: 03:00 hours

Scan period

Configures the length of the environment scan used to identify neighbor access points. The scan period should be 2 to 2.5 times the configured beacon interval; the default value is suitable for the default beacon interval. This value can be configured from 200 ms to 1000 ms.

Default value: 400 ms

AP steering RSSI threshold

The signal strength that a client must have on a remote access point in order to be steered to it.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

Default value: -75 dBm

Remote station expiration

Time for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

Default value: 600 seconds

Band ratio

Configures the intended distribution of clients between the radio bands. The configured ratio specifies what proportion of clients should be steered to the 5-GHz band.

Default value: 75 %

Band steering RSSI threshold

Configures the signal strength (RSSI) that a client "displays" on the other radio band in order to be steered there. The default setting is suitable for office environments.

Default value: -65 dBm

6.5.2 Additions to the Setup menu

Client Steering

This is where you specify the settings for the Client Management and the WLAN Band Steering for WLAN clients registered at the access point.

SNMP ID:

2.12.87

Telnet path:

Setup > **WLAN**

Operating

This option enables WLAN Band Steering or Client Management in the access point.

SNMP ID:

2.12.87.1

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Client Management

Enables Client Management in the access point. The percentage settings given below refer to the maximum load of an access point. This is set to 80 clients and cannot be changed.

Radio-Band

Enables WLAN band steering in the access point.

No

Switches this feature off. With this setting, these features are managed by a WLC, for example.

Default:

No

Dry-Run

Client Management performs a test run. The scans are performed, decisions are calculated and logged, but not executed.

SNMP ID:

2.12.87.6

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

Load-Recalculation-Interval

Interval in seconds, after which the load of the access point is calculated in Client Management. This results in the decision as to whether clients should be steered. If yes, then steering also takes place within this interval.

A higher value reduces the network load and has a limited positive effect in very large networks. A lower value leads to faster client steering. However, you should not go below 2 or above 10 seconds.

SNMP ID:

2.12.87.7

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Special values:

0

This value disables the delay.

Default:

5

Load-Announcement-Delta

If Client Management detects a change in load that exceeds the specified percentage value, then messages outside of the usual interval report this load to the neighboring access points that were discovered by scan. The value should be increased in environments with many moving devices. The default of 5% (4 clients) is suitable for environments with few moving devices, e.g. in offices or classrooms.

SNMP ID:

2.12.87.8

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

5

Load-Threshold

Percentage load threshold at which Client Management on an access point attempts to steer devices associated with it, irrespective of the load on neighboring access points. Increase the value in difficult environments with poor transmission quality or a high density of associated devices. In optimal environments with a high transmission quality and high throughput, such as in offices or classrooms, the load threshold can be reduced. The default of 80% (64 clients) lies between these extremes.

SNMP ID:

2.12.87.9

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

80

Balancing-Difference

Relating to Client Management, this is the percentage difference in load between two neighboring access points, at which point the access point with the higher load attempts to steer clients to the access point with a lower load. A high value leads to an unbalanced scenario, while a low value leads to more steering attempts. If too many steering attempts are observed, this value should be increased. If a balanced scenario is a priority, then you have to reduce this value. The default of 10% (8 clients) difference should be suitable an office or classroom environment.

SNMP ID:

2.12.87.10

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 10 characters from `[0-9]`

Default:

10

Maximum-Neighbor-Count

Relating to Client Management, this is the number of neighboring access points taken into account for client steering and for the exchange of information between the access points. High-density environments benefit from a lower value, as clients can be steered to nearby access points with reduced communication between the access points. As a minimum you should consider 4 access points. The maximum is 72 access points, which is a limitation of the 802.11 protocol. Increasing the value to more than the default value of 20 produces no significant improvements.

SNMP ID:

2.12.87.11

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

20

Neighbor-Signal-Threshold

Signal strength in dBm at which Client Management classifies an access point as a neighbor. Lower values (-80, -90) are useful for networks that cover a wider area. Higher values (-60, -50) are useful in high-density environments.

SNMP ID:

2.12.87.12

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-70

Legacy-Steering

Normally, Client Management only attempts to steer clients to a different access point that correctly supports the 802.11v protocol. If you set this parameter to "Yes" then steering is attempted for every client. During a steering event, the client is denied access to the access point for a period. The intention is to force it to switch to another access point. From the user's perspective, the WLAN simply appears to be gone for a while.

SNMP ID:

2.12.87.13

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

Minimal-Load-Difference

Relating to Client Management, this is the minimum percentage load difference between access points at which client steering takes place. Only applies if the load threshold is exceeded. Should not be set to a larger value than "Balancing-Difference" as the calculations could be incorrect. Also, no lower than 2%, otherwise there is a risk that a client is moved back and forth between two access points.

A low value results in more steering events in high-load environments. This may be useful in environments where the clients are relatively stationary. A high value results in fewer steering events, which is useful in environments with high loads and numerous mobile clients.

SNMP ID:

2.12.87.14

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

5

Daily-Env-Scan-Hour

Time at which an environment scan is performed when Client Management is enabled. The scan is performed at random within a 30-minute time window to minimize the chance of access points conflicting. A scan takes about 15 seconds with "Scan-Period" in the default setting. The access point is unavailable to clients throughout the scan, so the least possible number of clients should be active at the selected time. The default is 3 o'clock in the morning.

SNMP ID:

2.12.87.15

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

0 … 23

Default:

3

Scan-Period

Time in milliseconds that the client-management environment scan searches for other access points on a given channel. This should be 2 to 2.5 times your own beacon interval. The default value works with a common beacon interval. Higher values are only necessary with higher beacon intervals, although this increases the risk of scan conflicts when the access point is starting or during the nightly scans.

SNMP ID:

2.12.87.16

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

200 … 1000

Default:

400

AP-Steering-RSSI-Threshold

The signal strength in dBm that a client must have on a remote access point in order to be directed to it by Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

SNMP ID:

2.12.87.17

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-75

Remote-Station-Expiration

Time in seconds for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions made by the Client Management. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

SNMP ID:

2.12.87.18

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 5 characters from `[0-9]`

Default:

600

Blacklist-Clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering. Either explicitly or via wildcards. This provides the best user experience for compatible clients without affecting incompatible clients.

SNMP ID:

2.12.87.19

Telnet path:

Setup > **WLAN** > **Client-Steering**

MAC address

The MAC addresses of the clients to be excluded from client steering. The wildcard character * can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

SNMP ID:

2.12.87.19.1

Telnet path:

Setup > **WLAN** > **Client-Steering** > **Blacklist-Clients**

Possible values:

Max. 20 characters from ``[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Default:

empty

Start-Environment-Scan

This action manually starts the Client Management environment scan. This can be used if new access points have been added and they are not yet visible in the table of neighboring access points. Start the action using `do Start-Environment-Scan`.

SNMP ID:

2.12.87.20

Telnet path:

Setup > **WLAN** > **Client-Steering**

Client Management mode

Client Management operating mode. You can choose either to steer the clients between access points only or to additionally use band steering, which optimizes the frequency bands used by each access point.

SNMP ID:

2.12.87.21

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

AP-Steering
AP+Band-Steering

Default:

AP+Band-Steering

Band-Ratio

Ratio of distribution between bands in percent. This is used for the band-steering feature of Client Management.

The ratio indicates how many 5-GHz clients are able to connect to this access point. If more clients are connected at 5 GHz, clients are steered to 2.4 GHz. If more clients are connected at 2.4 GHz, clients are steered to 5 GHz.

Decrease the percentage if you are working with a channel width of 20 MHz in the 5-GHz band and your 2.4-GHz spectrum is free, i.e. there are few conflicting SSIDs and few other users such as Bluetooth. Choose a higher ratio if your 2.4-GHz band is full.

SNMP ID:

2.12.87.22

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

75

Band-Steering-RSSI-Threshold

Signal strength in dBm that a client must have on the other band in order for it to be steered. This is used for the band-steering feature of Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to a band with a poor signal quality. Clients may even refuse to be steered to a band with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the band.

The default value is ideal for office environments.

SNMP ID:

2.12.87.23

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-65

Roaming-Targets

With Client Management enabled, the table under `/Status/WLAN/Roaming-Targets` is filled out automatically. The targets added manually to this table are also included into the list of neighbors by an 802.11k advertisement, even if they are out of range. The number of automatically added roaming targets is limited by *2.12.87.11 Maximum-Neighbor-Count* on page 87.

SNMP ID:

2.12.132

Telnet path:

Setup > **WLAN**

Name

Enter the name for the roaming target here.

SNMP ID:

2.12.132.1

Telnet path:

Setup > **WLAN** > **Roaming-Target**

Possible values:

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

7 Quality of Service

7.1 Configurable DSCP tags for internal LANCOM services

From LCOS 10.20, internal LCOS applications can be marked with configurable DiffServ CodePoints (DSCP). This allows downstream hardware to recognize and prioritize these packets. Further information about DiffServ CodePoints is available in the Reference Manual under the section Quality of Service.

7.1.1 Additions to the Setup menu

DSCP marking

Internal LCOS applications can be marked with configurable DiffServ CodePoints (DSCP). This allows downstream hardware to recognize and prioritize these packets. Further information about DiffServ CodePoints is available in the Reference Manual under the section Quality of Service.

ⓘ This configuration marks only the control messages of the respective protocols.

SNMP ID:

2.11.94

Telnet path:

Setup > **Config**

Application

Column with the internal applications.

SNMP ID:

2.11.94.1

Telnet path:

Setup > **Config** > **DSCP-Marking**

DSCP

Column with the DiffServ codepoints. Default values are listed for the possible internal applications.

SNMP ID:

2.11.94.2

Telnet path:

Setup > **Config** > **DSCP-Marking**

Possible values:

BGP

CS6

OSPF

CS6

RIP

CS6

IKE

CS6

ⓘ Incl. Dynamic VPN UDP packets, but not supported with SSL encapsulation.

TACACS

BE/CS0

SNMP

BE/CS0

L2TP

CS6

PPTP

CS6

LISP

CS6

TFTP

BE/CS0

ICMP

BE/CS0

8 Virtual Private Networks – VPN

8.1 OCSP server

As of LCOS version 10.20, LANCOM devices support a server/responder for the Online Certificate Status Protocol (OCSP).

The Online Certificate Status Protocol (OCSP) is a procedure defined in RFC 6960 for checking the validity of a certificate at a central instance. Unlike certificate revocation lists (CRLs), the full CRL does not need to be downloaded periodically; instead, an on-demand OCSP request is made to the OCSP server when the connection is established, which ensures that the information about the validity of the certificate is always up-to-date. Only a small amount of data is transmitted since only the validity information for a certificate is sent. Compared to the CRL-based method, the validity information is always up-to-date and verification is faster.

The OCSP server can only be used in conjunction with a certification authority (CA) on the same device (LANCOM Smart Certificate). The OCSP server is not able to provide validity information for certificates from other CAs.

In order for the OCSP server to be used to generate certificates per LANCOM Smart Certificate, it must be assigned a certificate and a new entry is required in the profile for certificate creation in order to identify the OCSP server.

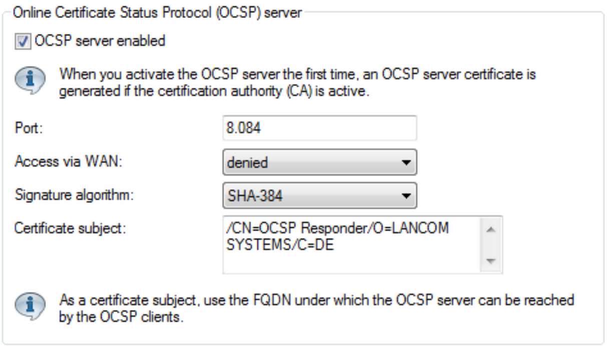
8.1.1 Configuring the OCSP server

Take the following steps to configure the OCSP server:

1. Enable the OCSP server under **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** > **OCSP server enabled**.
2. Assign a certificate to the OCSP server.

   Operating the OCSP server requires it to receive a certificate from the CA whose certificates it should provide information about. This certificate is used to sign the OCSP responses.

   For this purpose, go to **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** and configure the **Certificate subject** for the OCSP server. When the server is activated for the first time, this information is used to automatically generate the certificate for the OCSP server.

   Online Certificate Status Protocol (OCSP) server

   ☑ OCSP server enabled

   When you activate the OCSP server the first time, an OCSP server certificate is generated if the certification authority (CA) is active.

   Port: 8.084

   Access via WAN: denied

   Signature algorithm: SHA-384

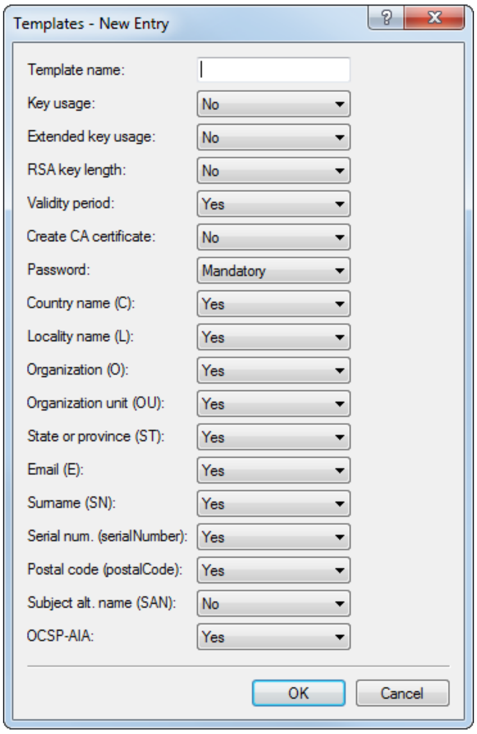
   Certificate subject: /CN=OCSP Responder/O=LANCOM SYSTEMS/C=DE

   As a certificate subject, use the FQDN under which the OCSP server can be reached by the OCSP clients.

   In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

3. Provide information about the OCSP server to the Smart Certificate preconfiguration

   a) Under **Certificates** > **Certificate handling** > **CA web interface** > **Templates**, you can specify that when Smart Certificate CA generates a certificate, the field "OCSP-AIA" (Authority Information Access) is available for configuration. If you use the "Default" template, this is automatically the case. If you use a custom template, then set the field “OCSP-AIA” to Yes.



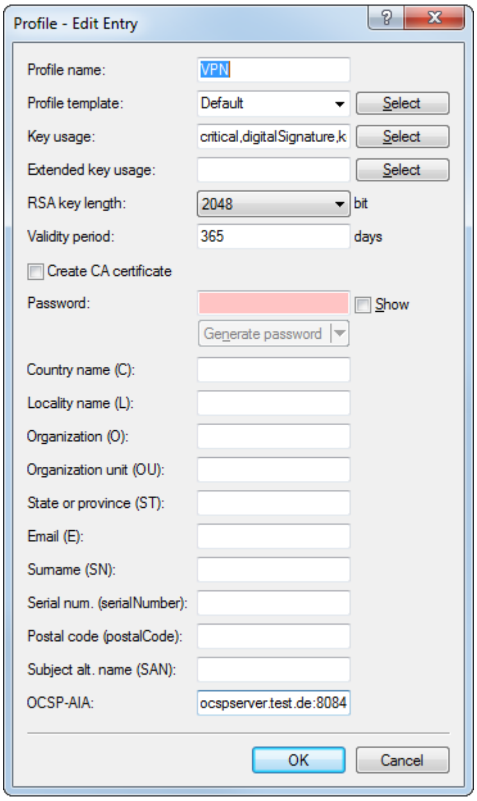
Template name:	
Key usage:	No
Extended key usage:	No
RSA key length:	No
Validity period:	Yes
Create CA certificate:	No
Password:	Mandatory
Country name (C):	Yes
Locality name (L):	Yes
Organization (O):	Yes
Organization unit (OU):	Yes
State or province (ST):	Yes
Email (E):	Yes
Surname (SN):	Yes
Serial num. (serialNumber):	Yes
Postal code (postalCode):	Yes
Subject alt. name (SAN):	No
OCSP-AIA:	Yes

b) Under **Certificates** > **Certificate handling** > **CA web interface** > **Profile** you set a default value for the field OCSP-AIA in the desired Smart Certificate profile.

ⓘ This step is optional. If you do not specify a default value here, you must manually specify a value when creating a certificate.

Configure the name or IP address where the OCSP server is available to the OCSP clients. This was already used earlier when generating the OCSP server certificate. Also add the port number where the OCSP server can be reached. The default setting is port 8084.

In the example, the default value for the profile "VPN" is adapted to "ocspserver.test.de:8084":

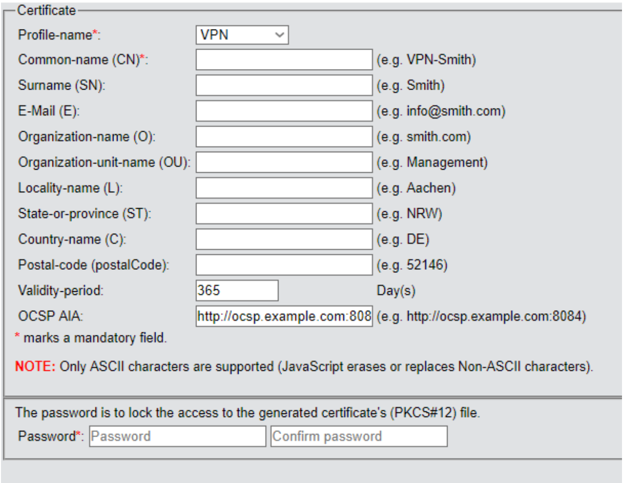


Profile - Edit Entry

Profile name:	VPN	
Profile template:	Default	Select
Key usage:	critical,digitalSignature,k	Select
Extended key usage:		Select
RSA key length:	2048	bit
Validity period:	365	days
□ Create CA certificate		
Password:		□ Show
	Generate password	
Country name (C):		
Locality name (L):		
Organization (O):		
Organization unit (OU):		
State or province (ST):		
Email (E):		
Surname (SN):		
Serial num. (serialNumber):		
Postal code (postalCode):		
Subject alt. name (SAN):		
OCSP-AIA:	ocspserver.test.de:8084	

This concludes the configuration of the OCSP server.

If you now use Smart Certificate in WEBconfig to generate a certificate , the OCSP AIA is automatically added to it, so enabling the client to contact the OCSP server for a validity check during connection establishment.



Certificate

Profile-name*:	VPN	
Common-name (CN)*:		(e.g. VPN-Smith)
Surname (SN):		(e.g. Smith)
E-Mail (E):		(e.g. info@smith.com)
Organization-name (O):		(e.g. smith.com)
Organization-unit-name (OU):		(e.g. Management)
Locality-name (L):		(e.g. Aachen)
State-or-province (ST):		(e.g. NRW)
Country-name (C):		(e.g. DE)
Postal-code (postalCode):		(e.g. 52146)
Validity-period:	365	Day(s)
OCSP AIA:	http://ocsp.example.com:808	(e.g. http://ocsp.example.com:8084)

* marks a mandatory field.

NOTE: Only ASCII characters are supported (JavaScript erases or replaces Non-ASCII characters).

The password is to lock the access to the generated certificate's (PKCS#12) file.

Password*: Password Confirm password

The OCSP server refers to its internal certificate list to check the validity. All in all, the Smart Certificate web interface offers a convenient way to withdraw or validate the certificates.

8.1.2 Additions to the Setup menu

OCSP-AIA

Enter the name or IP address where OCSP clients can reach the OCSP server.

SNMP ID:

2.39.2.14.1.19

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

Default:

empty

OCSP-AIA

When creating a certificate using Smart Certificate, the field “OCSP AIA” (OCSP Authority Information Access) can be displayed.

SNMP ID:

2.39.2.14.2.18

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

OCSP server

This table contains the settings for the OCSP server.

SNMP ID:

2.39.7

Telnet path:

Setup > **Certificates**

Operating

Turn the OCSP server on or off here.

SNMP ID:

2.39.7.1

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No

Default:

No

Port

The port used by the OCSP server.

SNMP ID:

2.39.7.2

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

8084

Certificate-Subject

Operating the OCSP server requires it to receive a certificate from the certification authority (CA) whose certificates it should provide information about. This certificate is used to sign the OCSP responses. Here you enter the name or IP address where OCSP clients can contact the OCSP server, e.g. `/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE`

ⓘ In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

SNMP ID:

2.39.7.3

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

/CN=ocspresponder.example.test/O=LANCOM SYSTEMS/C=DE

WAN access

This setting determines if and how the OCSP server can be reached from the WAN.

SNMP ID:

2.39.7.4

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No
Over-VPN

Default:

No

Signature-Algo

The algorithm used to generate the certificate used by the OCSP server.

SNMP ID:

2.39.7.5

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

SHA1
SHA-256
SHA-384
SHA-512

Default:

SHA-256

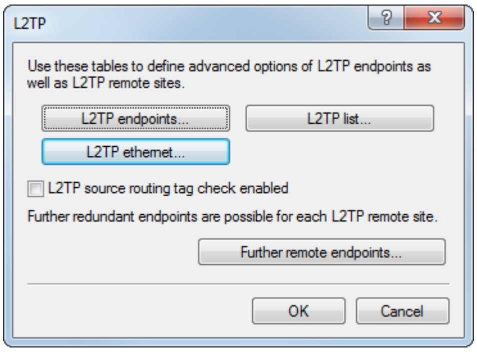
8.2 Layer-3 Ethernet tunnel with Layer-2 Tunneling Protocol version 3 (L2TPv3)

With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers and this allows WLAN traffic to be bridged through tunnels to the central site.

From LCOS 10.20, layer-3 Ethernet tunnels can be configured to use L2TPv3. This is configured in the L2TP endpoints table, available since version 2 of the protocol, and in the new L2TP Ethernet table. For a corresponding scenario, see *Configuring a WLAN scenario for bridging payload data to the central site* on page 104.

With LANconfig, you configure L2TP under **Communication** > **Remote sites** > **L2TP**.

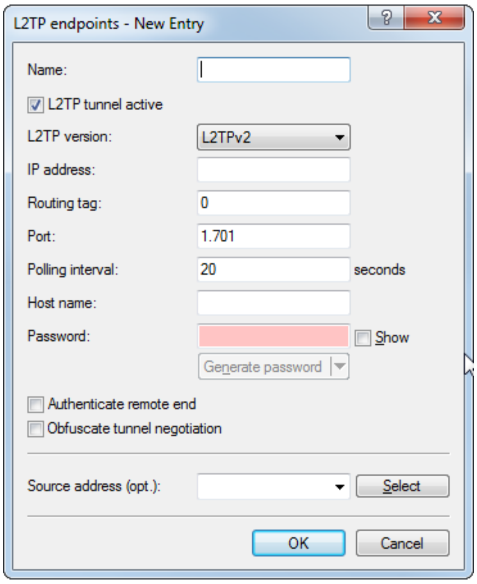

L2TP

Use these tables to define advanced options of L2TP endpoints as well as L2TP remote sites.

□ L2TP source routing tag check enabled

Further redundant endpoints are possible for each L2TP remote site.

For version 3, the configuration of the L2TP endpoints table under **L2TP endpoints** was enhanced with the following parameters:



L2TP endpoints - New Entry

Name:

☑ L2TP tunnel active

L2TP version: L2TPv2

IP address:

Routing tag: 0

Port: 1.701

Polling interval: 20 seconds

Host name:

Password: □ Show

□ Authenticate remote end

□ Obfuscate tunnel negotiation

Source address (opt.):

L2TP tunnel active

Enables the configured L2TP tunnel.

L2TP version

The L2TP protocol version used, either version 2 or 3.

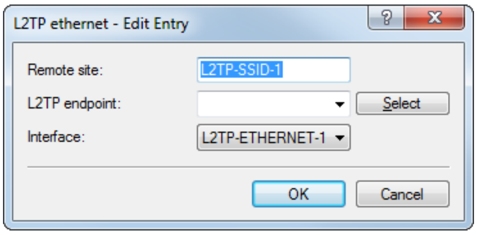
> Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

> L2TPv3 in the LCOS is always encapsulated in UDP. This allows transmissions to pass through NAT gateways without problem.

If you specify an IP address or a host name, an attempt is made to establish a connection. If the corresponding field is left blank, no connection is established, but connections can be accepted. Configured properties such as the station name or password are checked by the remote site when the connection is established.

> A number of implicit dependencies during the connection establishment and authentication are not directly apparent, so we will enlarge on these here:
>
> - The host name transmitted by the remote site is checked to see whether it corresponds to a configured L2TP endpoint. The host name is configured in the L2TP endpoint table of the remote site under **Host name**. If this field is left blank, the device name is used for authentication instead.
> - If this is the case, the connection is established using the configuration for the corresponding L2TP endpoint.
> - If not, the L2TP endpoints table is checked to see if it contains a “wildcard” entry. This is an entry that contains no host/station name or routing tag. The connection is established using the configuration of the “wildcard” entry.
> - If authentication is activated for the corresponding entry in the L2TP endpoints table, authentication is carried out based on the configured password.
> - If the password field is empty and authentication is switched on, a RADIUS authentication is carried out.
> - If authentication is turned off, a “wildcard” entry accepts any incoming tunnel accordingly.

Under **L2TP Ethernet** you link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.



Remote site: L2TP-SSID-1
L2TP endpoint:
Interface: L2TP-ETHERNET-1

Remote site

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

L2TP endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need “to run” via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

Interface

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

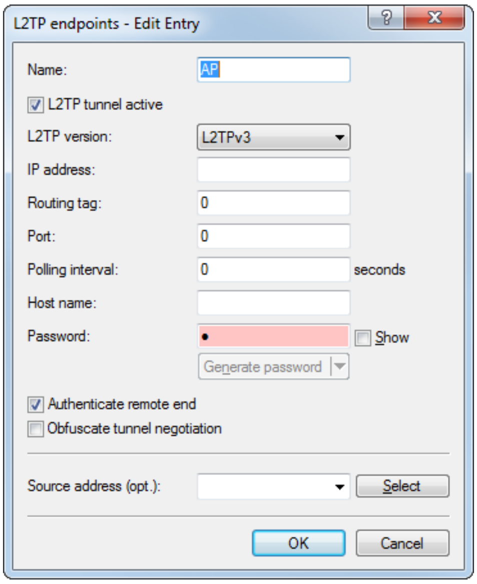
8.2.1 Configuring a WLAN scenario for bridging payload data to the central site

This is an example of how L2TPv3 is used in a scenario where several access points use bridging to transfer their payload data to a central router (referred to here as the “concentrator”), where the data are made available via a separate Ethernet port.

Before LCOS 10.20, this scenario would have required a WLAN controller.

1. Prepare the WLAN configuration on the access points. To enable roaming, SSID names and encryption settings should be configured identically on each AP.
2. Now configure the concentrator, which is to accept the L2TPv3 Ethernet sessions from the individual access points.
   a) Under **Communication** > **Remote sites** > **L2TP** in the L2TP endpoints table, create an entry "DEFAULT”. Enter a descriptive name for the new entry. Set the **L2TP version** to “L2TPv3”. Do not specify an **IP address**. Set a

password to increase security and enable the “Authenticate remote end” option to use the password for authentication during connection establishment. Leave the remaining settings at their default values.



L2TP endpoints - Edit Entry

Name: AP

☑ L2TP tunnel active

L2TP version: L2TPv3

IP address:

Routing tag: 0

Port: 0

Polling interval: 0 seconds

Host name:

Password: • □ Show

Generate password

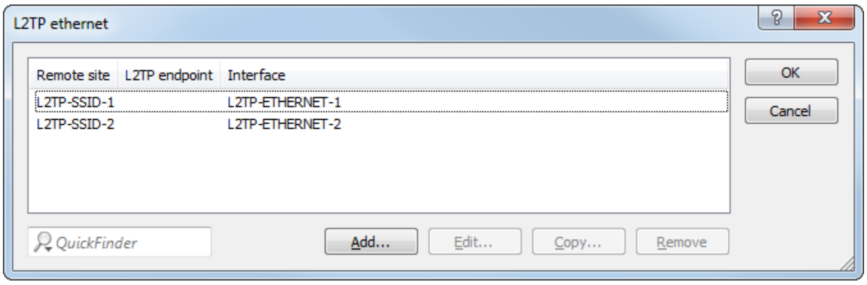
☑ Authenticate remote end

□ Obfuscate tunnel negotiation

Source address (opt.):

The **IP address** is empty. This is then a “wildcard” entry that can accept connections from any remote site.

b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Use **Remote site** to set a name for the Ethernet tunnel, e.g. the name of the SSID to which the tunnel on the access points is to be linked. Leave the field **L2TP endpoint** empty so that any (authenticated) sessions can be accepted. This method avoids having to create an entry for each individual access point in the L2TP endpoint table: The wildcard entry created in the previous step is used instead. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected. If the access points operate multiple SSIDs that are to be bridged to the central site, use this table to create an entry for each SSID, each with a unique name under **Remote site**.

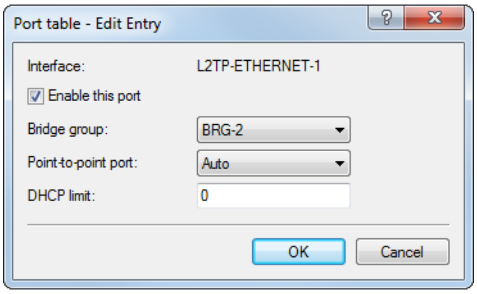


L2TP ethernet

Remote site	L2TP endpoint	Interface
L2TP-SSID-1		L2TP-ETHERNET-1
L2TP-SSID-2		L2TP-ETHERNET-2

In our scenario, the payload data of all connected access points are routed to the virtual interface configured here. Furthermore, the payload data of all access points connected to this virtual interface are bridged to one another—rather like the WLAN controller-based layer-3 tunneling technique.

c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a LAN interface where you set the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.



Interface: L2TP-ETHERNET-1

☑ Enable this port

Bridge group: BRG-2

Point-to-point port: Auto

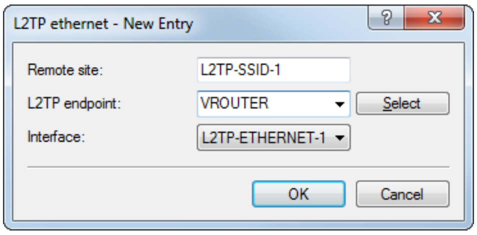
DHCP limit: 0

d) This concludes the configuration of the concentrator.

3. The following example shows how to configure an access point to transfer payload data to the concentrator.

a) Under **Communication** > **Remote sites** > **L2TP**, create a new entry in the L2TP endpoints table. Enter a descriptive name for the new entry. Set the **L2TP version** to “L2TPv3”. Enter the IP address or host name where the access point contacts the concentrator. Enter the password you set when configuring the concentrator and select “Authenticate remote end” to use the password for authentication. Leave the remaining settings at their default values.

b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Under **Remote site**, enter a name that identifies the Ethernet tunnel. This must be the same as the name given to this Ethernet tunnel on the concentrator. In the field **L2TP endpoint**, select the L2TP endpoint table entry that was created in the previous step. This endpoint is then used to establish the Ethernet tunnel. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected.

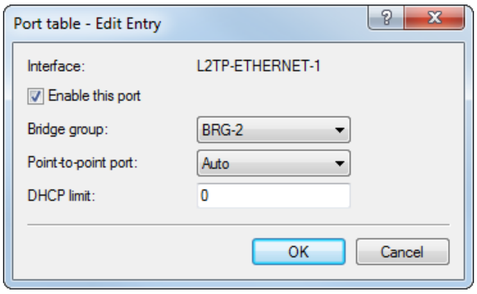


Remote site: L2TP-SSID-1

L2TP endpoint: VROUTER

Interface: L2TP-ETHERNET-1

c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a WLAN interface by setting the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.



Port table - Edit Entry

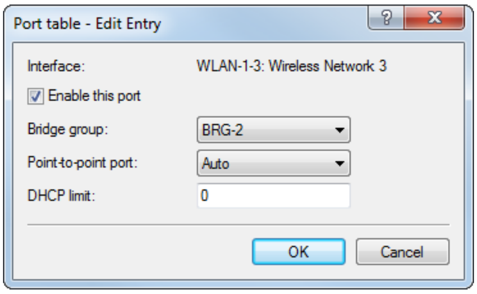
Interface: L2TP-ETHERNET-1

☑ Enable this port

Bridge group: BRG-2

Point-to-point port: Auto

DHCP limit: 0



Port table - Edit Entry

Interface: WLAN-1-3: Wireless Network 3

☑ Enable this port

Bridge group: BRG-2

Point-to-point port: Auto

DHCP limit: 0

d) Carry out the configuration described here for the other access points. Once the configuration has been completed in this way, the identical configuration can be used on all of the access points and no further adaptations are necessary for the individual APs.

8.2.2 Additions to the Setup menu

Version

The L2TP protocol version used for this L2TP endpoint, either version 2 or 3.

Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

SNMP ID:

2.2.35.11

Telnet path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

L2TPv2

Layer 2 Tunneling Protocol Version 2

L2TPv3

Layer 2 Tunneling Protocol Version 3

Operating

This L2TP endpoint is enabled or disabled.

SNMP ID:

2.2.35.12

Telnet path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

No

L2TP endpoint is disabled.

Yes

L2TP endpoint is enabled.

L2TP-Ethernet

This table is used to link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.

SNMP ID:

2.2.39

Telnet path:

Setup > **WAN**

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

SNMP ID:

2.2.39.1

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

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

L2TP endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need “to run” via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

SNMP ID:

2.2.39.2

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

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

Interface

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

SNMP ID:

2.2.39.3

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtual L2TP Ethernet interfaces

8.3 IKEv2

8.3.1 Configuring IKEv2 with LANconfig

IKEv2 is configured under **VPN** > **IKEv2/IPSec**.

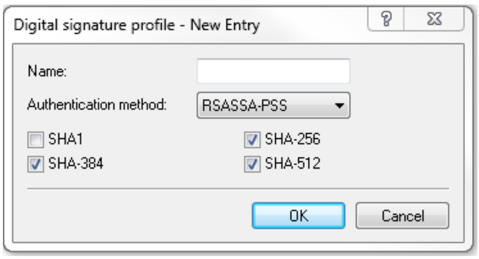
Digital signature profile

This table is used to specify the authentication methods for your VPN connections.

Digital signature profile

From LCOS version 10.20, devices that are set to use the older RSASSA-PKCS1-v1_5 to negotiate with remote sites now also support the newer RSASSA PSS.

Use this table to configure the parameters for the IKEv2 authentication.



Digital signature profile - New Entry

Name:

Authentication method: RSASSA-PSS

□ SHA1 ☑ SHA-256
☑ SHA-384 ☑ SHA-512

Name

Contains the unique name of this entry. You can assign this name in three different places. In the section **Authentication** in the fields **Local dig.signature profile** and **Rem. dig.signature profile**, and under **Extended settings** > **Authentification** > **Identities** > **Rem. dig.signature profile**.

Authentication method

Sets the authentication method for the digital signature. Possible values are:

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)

(!) If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

You also specify the secure hash algorithms (SHA) to be used.

Additions to the Setup menu

Auth-Method

Sets the authentication method for the digital signature.

(!) If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

SNMP ID:

2.19.36.3.4.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

RSASSA-PSS
RSASSA-PKCS1-v1_5

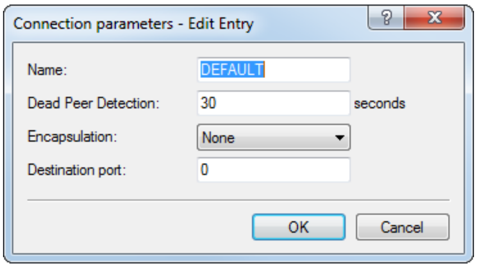
Default:

RSASSA-PSS

Connection parameters

From LCOS 10.20, the new parameters **Encapsulation** and **Destination port** are located in the table **VPN** > **IKEv2/IPSec** > **VPN connections** > **Connection parameters**.

Use this table to specify the parameters of IKEv2 VPN connections that are not included in the SA negotiation. An entry named "DEFAULT" is provided with common settings.



Name: DEFAULT
Dead Peer Detection: 30 seconds
Encapsulation: None
Destination port: 0

Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. SSL or UDP can be set here. Use this in combination to configure any **Destination port**. The IKEv2 tunnel is established either with port 4500 for UDP or with the port set for the **Destination port**. If the destination port is set to 500, this will be ignored and port 4500 is used instead. For SSL, the tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead. If set to "None", the port 500 is taken and the setting in **Destination port** is ignored.

The configurable port can be used for scenarios where a LANCOM router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

Destination port

Here you can specify that the destination port depends on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

Additions to the Setup menu

Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. You can set the ports 443 or 4500 instead. Use this in combination to configure any **Destination-Port**. If the setting is different from 500, UDP encapsulation is performed automatically. The configurable port can be used for scenarios where a LANCOM router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

ⓘ Incoming VPN tunnels continue to be accepted on the default ports 443, 500 and 4500. These cannot be freely configured.

SNMP ID:

2.19.36.4.7

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

UDP
The IKEv2 tunnel is established either with port 4500 or with the setting for the destination port. If the destination port is set to 500, this will be ignored and port 4500 is used instead.

SSL
The IKEv2 tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead.

None
The IKEv2 tunnel is established with port 500. The setting for the destination port is ignored.

Default:

None

Destination-Port

Here you can specify the destination port for the IKEv2 connection depending on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

SNMP ID:

2.19.36.4.8

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

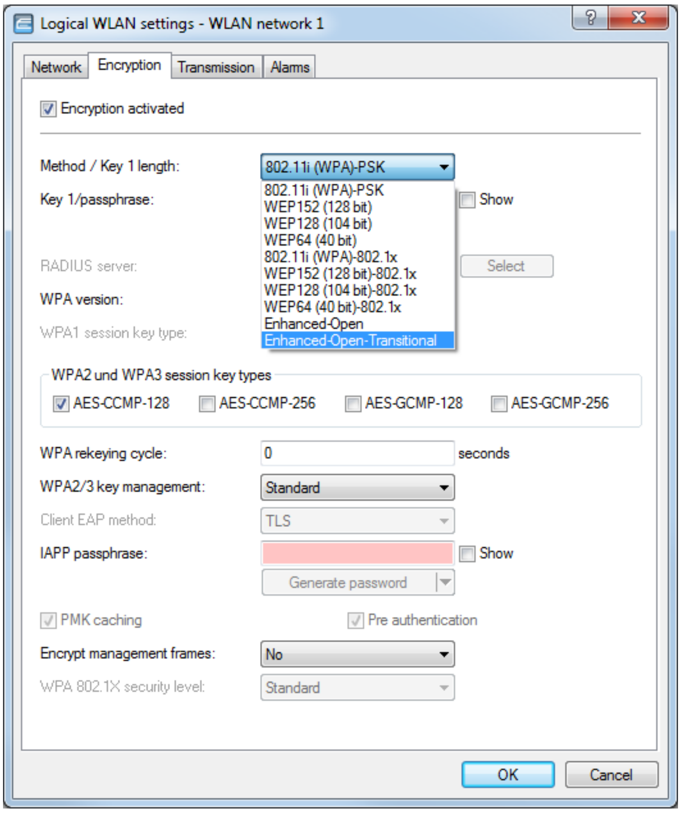
9 Public Spot

9.1 Setting up a secure hotspot with Enhanced Open

Enhanced Open for the first time provides a way to offer a secure, yet easy-to-use hotspot.

Enhanced Open has been combined with the LANCOM Public Spot option.

The WLAN to be used for the hotspot is set up in the usual way with the exception that the encryption method is set to **Enhanced Open Transitional**:



Logical WLAN settings - WLAN network 1

☑ Encryption activated

Method / Key 1 length: 802.11i (WPA)-PSK

- 802.11i (WPA)-PSK
- WEP152 (128 bit)
- WEP128 (104 bit)
- WEP64 (40 bit)
- 802.11i (WPA)-802.1x
- WEP152 (128 bit)-802.1x
- WEP128 (104 bit)-802.1x
- WEP64 (40 bit)-802.1x
- Enhanced-Open
- Enhanced-Open-Transitional

Key 1/passphrase: □ Show

RADIUS server: Select

WPA version:

WPA1 session key type:

WPA2 und WPA3 session key types

☑ AES-CCMP-128 □ AES-CCMP-256 □ AES-GCMP-128 □ AES-GCMP-256

WPA rekeying cycle: 0 seconds

WPA2/3 key management: Standard

Client EAP method: TLS

IAPP passphrase: □ Show

Generate password

☑ PMK caching ☑ Pre authentication

Encrypt management frames: No

WPA 802.1X security level: Standard

Not only is entering a key not required, it is not even possible: A client enabled for Enhanced Open establishes an encrypted connection to the access point without any key having to be entered. To the user, it is just like using an unencrypted, open WLAN: There is no need to enter any previously communicated key as with WPA2-PSK.

The Transitional mode allows an SSID to be used concurrently by clients that support Enhanced Open as well as by clients that do not yet support Enhanced Open. For the latter clients, no encryption is used at all and the SSID works like an open, unencrypted SSID. Once Enhanced Open has become more widespread, you can switch from Transitional mode to regular Enhanced Open mode.

After this, you can proceed as usual with the configuration of the Public Spot module. Since the Public Spot module is independent of the encryption settings of the WLAN interfaces, all of the functions of the Public Spot module can be used without restriction in conjunction with Enhanced Open.

In summary, Enhanced Open is ideal for hotspot operation as it provides a higher level of security than the open hotspots used in the past. The optional Transitional mode ensures that even clients that do not yet support Enhanced Open can be connected in a way that is transparent to the user.

9.2 User list removed

The former user list for the Public Spot (LANconfig: **Configuration** > **Public Spot** > **Users** > **User list**) has been deprecated. Since LCOS 7.70, the preferred way to configure Public Spot users is to use the internal RADIUS server, so this old table is no longer required. If there are still entries in the user list at the time of the upgrade, they will be automatically converted to RADIUS users. These converted users can be identified as such by an entry in the comment field (e.g. "moved by root").

! An entry of the same name that already exists in the RADIUS user table at this time will be overwritten.

10 RADIUS

10.1 Importing and exporting RADIUS user data by CSV file

The internal RADIUS server is basically a user database. Here we describe an easy way to import and export the user entries. This is particularly relevant for Public Spots, where users are generated in large numbers by an external system. For LEPS-MAC, too, this is an easy way to import the data. The format used for the data exchange is csv (comma separated values), whereby a semicolon serves as the default separator of the individual data fields.

10.1.1 Exporting RADIUS user data by CSV file

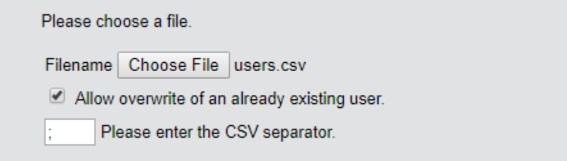
To export the user data of the RADIUS server via WEBconfig, proceed as follows.

Click on **Extras** > **Export RADIUS users**.
The user data is downloaded as the file `users.csv`. The semicolon is the separator; the first row contains the identifiers of the database fields.

10.1.2 Importing RADIUS user data by CSV file

To import the user data of the RADIUS server via WEBconfig, proceed as follows.

1. Generate a file with the required header for the user data by performing an export of the user data as described in *Exporting RADIUS user data by CSV file* on page 115.
2. Create a CSV import file with a header containing the correct database field identifiers determined in the previous step. The import file does not have to contain all the columns.
3. Navigate to the menu item **Extras** > **Import RADIUS users**.
4. Use **Choose file** to select the CSV file to be imported.
5. Enter the CSV separator. By default this is already preset to ";".



Please choose a file.

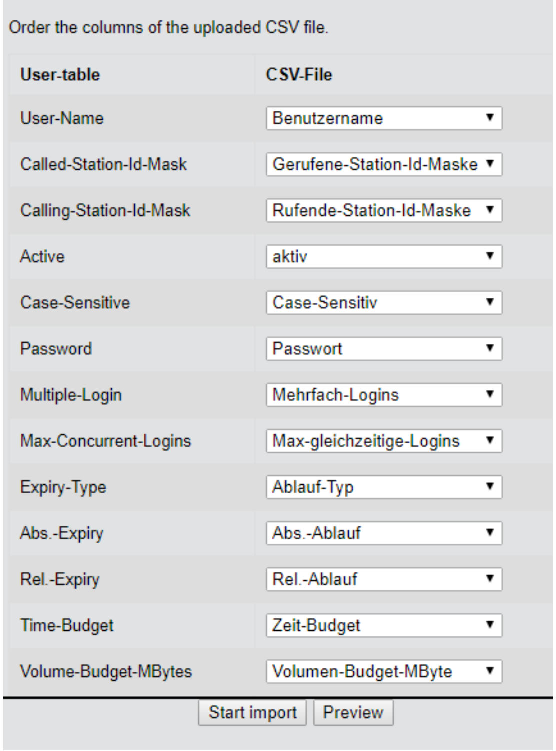
Filename Choose File users.csv

☑ Allow overwrite of an already existing user.

; Please enter the CSV separator.

6. Start the upload.

7. Now check that the columns detected in the CSV file are correctly aligned with the supported columns. You can adjust the alignment in this dialog. No adjustment should be necessary if you used the column names from the previously exported CSV file.



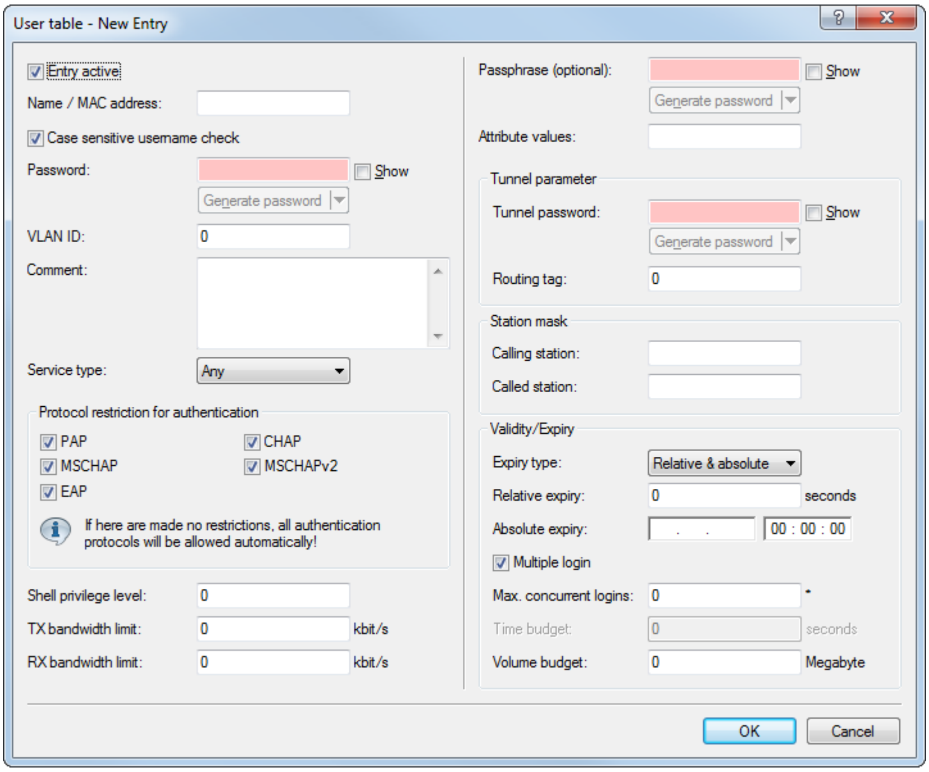
Order the columns of the uploaded CSV file.

User-table	CSV-File
User-Name	Benutzername
Called-Station-Id-Mask	Gerufene-Station-Id-Maske
Calling-Station-Id-Mask	Rufende-Station-Id-Maske
Active	aktiv
Case-Sensitive	Case-Sensitiv
Password	Passwort
Multiple-Login	Mehrfach-Logins
Max-Concurrent-Logins	Max-gleichzeitige-Logins
Expiry-Type	Ablauf-Typ
Abs.-Expiry	Abs.-Ablauf
Rel.-Expiry	Rel.-Ablauf
Time-Budget	Zeit-Budget
Volume-Budget-MBytes	Volumen-Budget-MByte

8. Click **Start import** to complete the process and accept the user data.

10.2 User-defined attributes for RADIUS users in the RADIUS server.

The RADIUS user database under **RADIUS** > **Server** > **User table** now features the parameter **Attribute values**, which can be used to add vendor-specific attributes.



☑ Entry active

Name / MAC address:

☑ Case sensitive username check

Password: □ Show

Generate password

VLAN ID: 0

Comment:

Service type: Any

Protocol restriction for authentication

☑ PAP ☑ CHAP

☑ MSCHAP ☑ MSCHAPv2

☑ EAP

If here are made no restrictions, all authentication protocols will be allowed automatically!

Shell privilege level: 0

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Passphrase (optional): □ Show

Generate password

Attribute values:

Tunnel parameter

Tunnel password: □ Show

Generate password

Routing tag: 0

Station mask

Calling station:

Called station:

Validity/Expiry

Expiry type: Relative & absolute

Relative expiry: 0 seconds

Absolute expiry: . . 00 : 00 : 00

☑ Multiple login

Max. concurrent logins: 0 *

Time budget: 0 seconds

Volume budget: 0 Megabyte

Attribute values

Along with the user-management attributes supported by the LANCOM RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users as a comma-separated list of attributes and values in the form <Attribute_1>=<Value_1>,<Attribute_2>=<Value_2> ...

10.2.1 Additions to the Setup menu

Attribute-Values

User-defined attributes for RADIUS users in the RADIUS server.

Along with the user-management attributes supported by the LANCOM RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users here.

SNMP ID:

2.25.10.7.25

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Comma-separated list of attributes and values in the form
<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2> ...

Max. 251 characters from `` [A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ` ``

Default:

empty

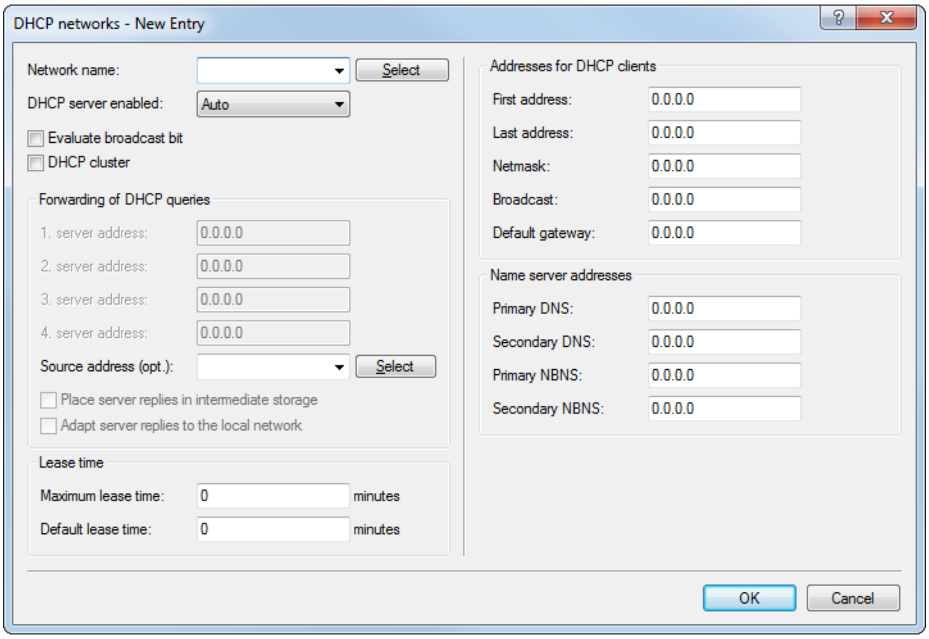
11 Other services

11.1 Automatic IP address administration with DHCP

11.1.1 Configuring DHCPv4 parameters with LANconfig

Source address for DHCP relay agent

In the DHCP network table (LANconfig: **IPv4** > **DHCPv4** > **DHCP networks**) there is a new option for assigning an optional source address to a relay agent.



DHCP networks - New Entry

Network name: [ ] Select

DHCP server enabled: Auto

☐ Evaluate broadcast bit

☐ DHCP cluster

Forwarding of DHCP queries

1. server address: 0.0.0.0

2. server address: 0.0.0.0

3. server address: 0.0.0.0

4. server address: 0.0.0.0

Source address (opt.): [ ] Select

☐ Place server replies in intermediate storage

☐ Adapt server replies to the local network

Lease time

Maximum lease time: 0 minutes

Default lease time: 0 minutes

Addresses for DHCP clients

First address: 0.0.0.0

Last address: 0.0.0.0

Netmask: 0.0.0.0

Broadcast: 0.0.0.0

Default gateway: 0.0.0.0

Name server addresses

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0

Primary NBNS: 0.0.0.0

Secondary NBNS: 0.0.0.0

OK Cancel

Source address (optional)

Here you assign an optional source address to a relay agent. This address (the name of an ARF network, named loopback address) is used to forward client messages.

Additions to the Setup menu

Loopback address

Here you assign a loopback address to a relay agent. The loopback address (the name of an ARF network, named loopback address) is used to forward client messages.

SNMP ID:

2.10.20.22

Telnet path:

Setup > **DHCP**

Possible values:

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

Default:

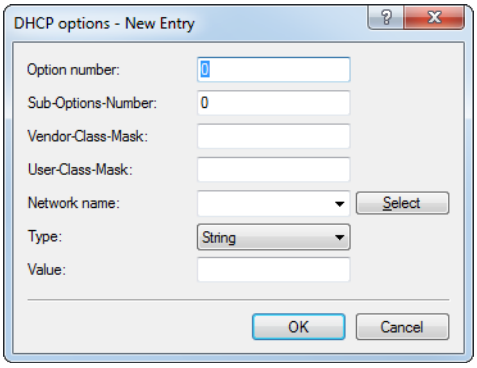
empty

DHCP options

From LCOS version 10.20, LANCOM devices support suboptions for the DHCP options.

The DHCP server uses the DHCP options to transmit additional configuration parameters to the DHCP clients. The vendor class ID (DHCP option 60) shows e.g. the type of device. DHCP option 43 is used by various device manufacturers to distribute additional information about network devices during the initial startup. The parameters themselves are manufacturer-specific.

In LANconfig, the DHCP options are configured under **IPv4** > **DHCPv4** > **DHCP options**. Click on **Add** to create a new entry.



DHCP options - New Entry

Option number: 0
Sub-Options-Number: 0
Vendor-Class-Mask:
User-Class-Mask:
Network name:
Type: String
Value:

Option number

Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP.

> You can find a list of all DHCP options in "RFC 2132 – DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. For example, DHCP requests from LANCOM devices always contain the string "LANCOM" in the vendor-class ID, which is supplemented by the exact device type, if required. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

For LANCOM devices, the entry here would be "*LANCOM*".

User class mask

Filter criterion used by some manufacturers for requests to the DHCP server. See also Vendor-class mask. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

Network name

Name of the IP network where this DHCP option is to be used.

Type

Entry type. This value depends on the respective option. For example, RFC 2132 defines the option "35" (ARP cache timeout) as follows:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

This description tells you that the type "32-bit integer" is used for this option.

You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Value

With this field you define the contents of the DHCP option.

IP addresses are specified with the usual notation for IPv4 addresses, e.g. as "123.123.123.100", integer types are entered as normal decimal numbers, and strings as simple text.

Multiple values in a single field are separated with commas, e.g. "123.123.123.100, 123.123.123.200".

You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Additions to the Setup menu

Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

SNMP ID:

2.10.26.5

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. For example, DHCP requests from LANCOM devices always contain the string “LANCOM” in the vendor-class ID, which is supplemented by the exact device type, if required. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields “Vendor-class mask” and “User-class mask” can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards “*” (any number of characters) and “?” (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

SNMP ID:

2.10.26.6

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

Default:

empty

User class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. This usually allows the manufacturer or even the specific device class of the client to be identified. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields “Vendor-class mask” and “User-class mask” can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards “*” (any number of characters) and “?” (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

SNMP ID:

2.10.26.7

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

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

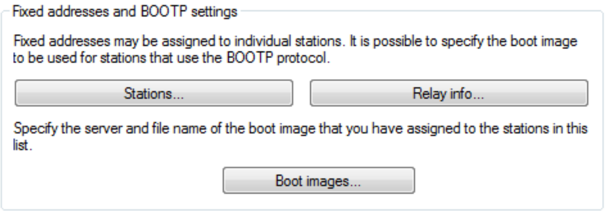
Default:

empty

Assigning IP addresses based on DHCP option 82

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. The switch in question uses DHCP option 82 to supplement the DHCP request with the Circuit ID, which identifies the port that this device is connected to. This information is then used by the DHCP server to assign a specific IP address. This establishes a relationship between an IP address and a location, which simplifies network monitoring.

In LANconfig under **IPv4** > **BOOTP**, you can set the switch-port based assignment of IP addresses for each port separately by clicking on **Relay info**.

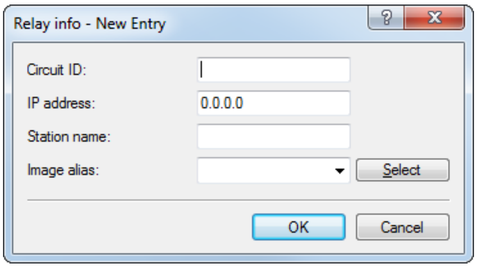


Fixed addresses and BOOTP settings

Fixed addresses may be assigned to individual stations. It is possible to specify the boot image to be used for stations that use the BOOTP protocol.

Specify the server and file name of the boot image that you have assigned to the stations in this list.

After selecting the switch port that is automatically added by the DHCP option 82, you can set the following:



Relay info - New Entry

Circuit ID:

IP address: 0.0.0.0

Station name:

Image alias:

Circuit-ID

This is the storage location for the “Circuit ID” used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the “Circuit ID” is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires “negative” bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

Station name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Image alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

ⓘ Enter the server providing the boot image and the name of the file on the server in the boot image table.

Additions to the Setup menu

Relay-Info-List

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. To this end, the switches provide the “Circuit ID” of the respective ports. Each port is then assigned exactly one IP address, host name and a boot image. The latter works analogous to the BOOTP table.

SNMP ID:

2.10.27

Telnet path:

Setup > **DHCP**

Circuit-ID

This is the storage location for the “Circuit ID” used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the “Circuit ID” is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires “negative” bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

SNMP ID:

2.10.27.1

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

Max. 64 characters from `[A-F][a-f]x[0-9]{}/`

IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

SNMP ID:

2.10.27.2

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Host name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

SNMP ID:

2.10.27.3

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

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

Default:

empty

Image-alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

ⓘ Enter the server providing the boot image and the name of the file on the server in the boot image table.

SNMP ID:

2.10.27.4

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

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

Default:

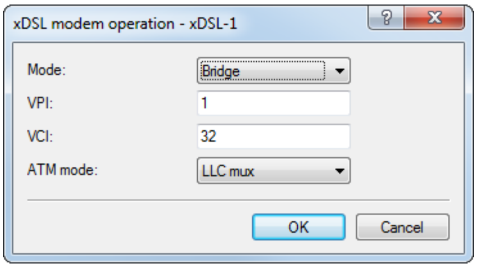
empty

11.2 ADSL/VDSL modem operation (bridge mode)

With the ongoing migration of ISDN connections to All-IP, the ISDN connections available at sites are being converted into additional DSL connections. In order to provide this new bandwidth to the whole of the network, the router needs to be connected to the new DSL line. If the DSL connection of the gateway is already in use, a LANCOM VDSL router can be connected upstream as a pure DSL modem. The access and VoIP data continue to be stored in the main gateway. This allows additional DSL connections to be transparently integrated into the existing scenario.

The configuration is conducted as follows:

1. Connect the LANCOM router, which is to operate as a modem, to the VDSL port.
2. Connect the main gateway to the LANCOM modem by means of an Ethernet cable.
3. Under **Interfaces** > **LAN** > **Port table**, assign the LAN interface and the xDSL interface to an unused bridge group.
4. Under **Interfaces** > **WAN** > **Interface settings** > **xDSL modem operation**, set the VDSL port to bridge mode. In the case of ADSL, you need to correct the ATM parameters (Deutsche Telekom: VPI 1, VCI 32, ATM mode LLC-Mux).



xDSL modem operation - xDSL-1

Mode: Bridge

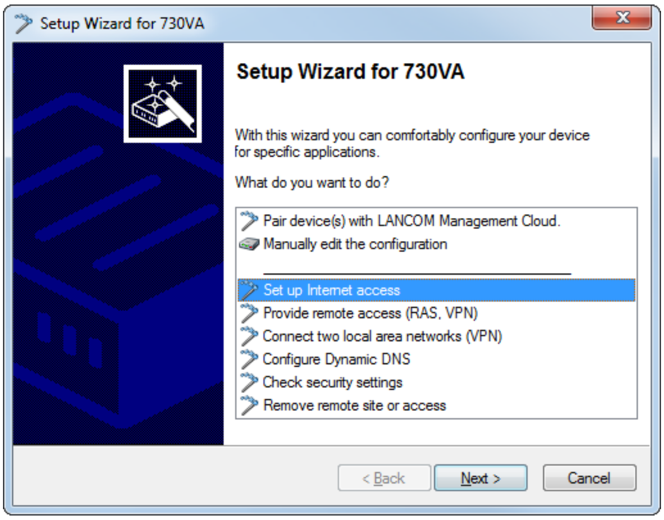
VPI: 1

VCI: 32

ATM mode: LLC mux

5. Deactivate the DHCP server under **IPv4** > **DHCPv4** > **DHCP networks**.
6. Give the router an intranet IP address from an unused range (for example, 192.168.3.254).
7. Set up the Internet connection on the main gateway using the setup wizard:

a. Select your device in LANconfig and start the setup wizard “Set up Internet access”.



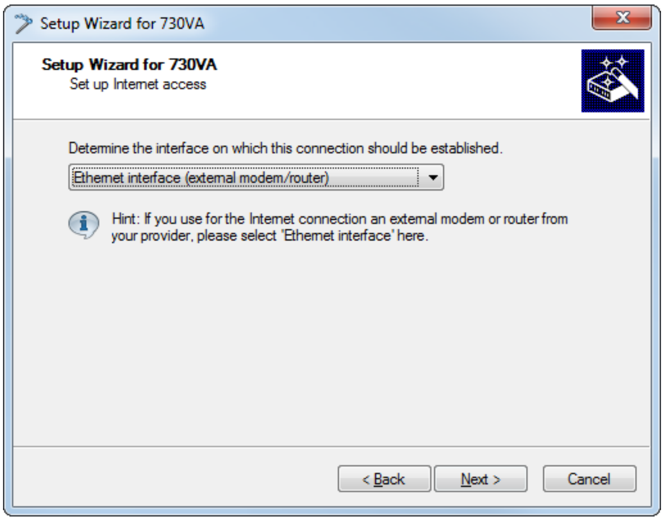
Setup Wizard for 730VA

With this wizard you can comfortably configure your device for specific applications.

What do you want to do?

Setup Wizard for 730VA
Pair device(s) with LANCOM Management Cloud.
Manually edit the configuration
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Configure Dynamic DNS
Check security settings
Remove remote site or access
< Back
Next >
Cancel

b. Follow the instructions in the setup wizard and select the option that best suits your needs. When you reach the step to set the “Interface for this connection”, select the option **Ethernet Interface (external modem/router)**.



Setup Wizard for 730VA
Set up Internet access

Determine the interface on which this connection should be established.

Ethernet interface (external modem/router)

Hint: If you use for the Internet connection an external modem or router from your provider, please select 'Ethernet interface' here.

If the LANCOM modem’s sync status is to be queried from the network, then go to **Communication** > **Remote sites** > **Remote sites (DSL)** and create a remote site named “Management” with a short hold time of “9999” seconds, layer name “IPOE”, and DSL port “1”.

In the IP parameter list under **Communication** > **Protocols**, select the remote site “Management” and give it an IP address from the unused range (e.g. 192.168.3.1/24). Now in the table **IP router** > **Routing** > **IPv4 routing table** add an entry 192.168.3.0/24 to the “Management” remote site with IP masquerading switched off. The modem can now be accessed and queried at the IP address 192.168.3.254.

11.2.1 Additions to the Setup menu

xDSL

The Asymmetrical Digital Subscriber Line (ADSL) and Very High Speed Digital Subscriber Line (VDSL) are transmission methods for high-speed data transmissions over regular telephone lines.

With ADSL and ADSL2+, transmissions (downstream) of up to 24 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 3.5 Mbps (upstream)

- hence the name "asymmetric". As an example, the ADSL-over-ISDN infrastructure operated in Germany supports maximum speeds of 16 Mbps (downstream) and 1125 kbps (upstream).

VDSL is a DSL technology that delivers far higher data rates over normal phone lines than, for example, ADSL or ADSL2+.

SNMP ID:

2.42

Telnet path:

Setup

WAN-Bridge

Here you configure the router for ADSL/VDSL modem operation (bridge mode).

SNMP ID:

2.42.3

Telnet path:

Setup > **xDSL**

Interface

The xDSL interfaces of the device.

SNMP ID:

2.42.3.1

Telnet path:

Setup > **xDSL** > **WAN-Bridge**

Mode

The device is able to work in bridge mode. It then behaves like an ADSL/VDSL modem.

SNMP ID:

2.42.3.2

Telnet path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Router

The device works as a router.

Bridge
The device works in bridge mode.

Default:

Router

ATM-VPI

Virtual Path Identifier (VPI). The value for VPI is communicated by the ADSL/VDSL network operator. The default value is for Deutsche Telekom.

SNMP ID:

2.42.3.3

Telnet path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Max. 3 characters from `[0-9}`

Default:

1

ATM-VCI

Virtual Channel Identifier (VCI). The value for VCI is communicated by the ADSL/VDSL network operator. The default value is for Deutsche Telekom.

SNMP ID:

2.42.3.4

Telnet path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

Max. 5 characters from `[0-9}`

Default:

32

ATM-Muxmode

This setting sets the encapsulation method used for the data packets. The default value is for Deutsche Telekom.

SNMP ID:

2.42.3.5

Telnet path:

Setup > **xDSL** > **WAN-Bridge**

Possible values:

VC-MUX

Multiplexing via ATM by establishing additional VCs as per RFC 2684.

LLC-MUX

Multiplexing via ATM with LLC/SNAP encapsulation as per RFC 2684. Several protocols can be transmitted over the same VC (virtual channel).

Default:

LLC-MUX