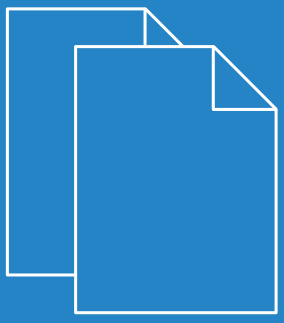
SECURE. **NETWORKS.**

LCOS 10.0
Addendum



LANCOM
Systems

Contents

1 Addendum to LCOS version 10.0

This document describes the changes and enhancements in LCOS version 10.0 since the previous version.

2 Routing and WAN connections

2.1 The Bonjour proxy

As of version 10.0, LCOS provides a Bonjour proxy.

Apple Bonjour allows devices to discover and operate certain approved services automatically and without prior configuration. This procedure is also known as "Zero Configuration Networking" (ZeroConf).

The most popular services include, among others:

- Printer services (with or without Apple Airprint support)
- File services (folder or file shares)
- Apple Airplay
- iTunes

2.1.1 Bonjour basics

Bonjour exchanges information by means of individual multicast DNS packets (mDNS) according to *RFC 6762* and DNS-based service discovery (DNS-SD) according to *RFC 6763*. The clients exchange Bonjour information via the multicast address `224.0.0.251` (IPv4) or `ff02::fb` (IPv6) on port 5353. Bonjour packets are not routed (multicast packet, TTL = 1), which limits their use to the current local area network.

Please note that the Bonjour proxy only serves to aid the discovery of Bonjour services. The actual routing between the communicating parties requires a separate configuration or restriction by means of, for example, routing or firewall entries.

It is often impractical to provide all services on a single network. This is why larger networks are often divided into several subnets. However, Bonjour is unable to operate in this situation.

Example application with two networks

At a school, students use a dedicated IP network to access the WLAN. In parallel to this, the local printer is made available on a second internal IP network. In principal, the appropriate routing and restrictions would make it possible for students to use their smartphones to access the local internal printer. However, because mDNS is only defined as link-local, Bonjour is unable to help students to discover the printer with their smartphones. The LANCOM Bonjour proxy mediates between two networks, which enables students to discover printers in other networks.

Basically, there are two ways of realizing such a scenario:

Multicast routing

A router forwards the search queries and service advertisements between the two networks.

This option causes unnecessary traffic, which makes it rather inefficient.

Caching of services

The router stores discovered mDNS service advertisements in its local cache. A router that receives an mDNS query then responds on behalf of the original service. Before processing the advertisement and before transmitting anything from the cache, the router checks its policies to see whether the service is approved or blocked. The policies are used to control which services are approved for discovery and between which networks.

Please note that reading out the mDNS cache content with the SNMP protocol is not supported.

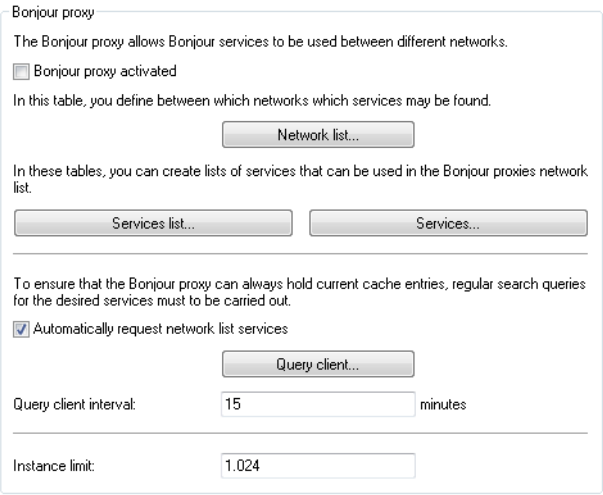
The Bonjour proxy supports an mDNS query client, which at set time intervals queries an interface about the services of interest. This query keeps the cache entries for approved services up to date. In order for the cache to be up-to-date at all times, it is useful to enable automatic searches for services that are permanently available (e.g. print services).

If no automatic queries about frequently used services are configured, the Bonjour proxy may be unable to respond to the corresponding queries even though the services are approved.

Bonjour proxies only operate on logical LAN / WLAN interfaces or on logical networks with an IP address. WAN interfaces / remote stations or tunnels (except for WLC L3 tunnels) and VLANs without address binding are not supported.

2.1.2 Configuration with LANconfig

The Bonjour proxy is configured with LANconfig under **IP router** > **Bonjour**.



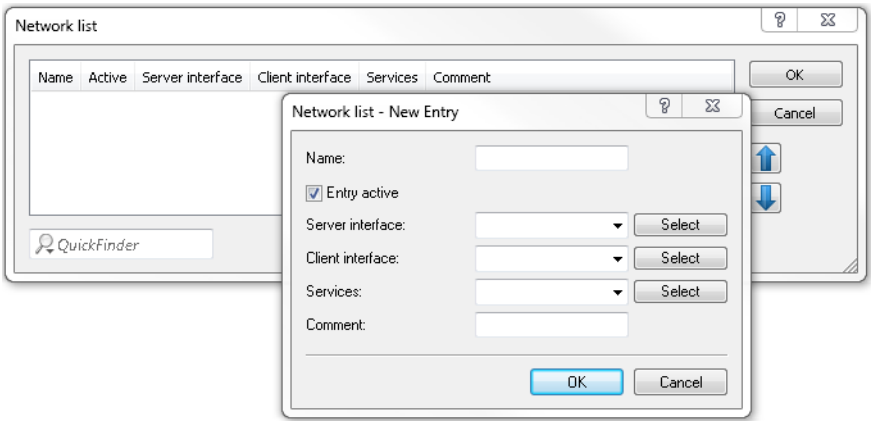
The following settings are available:

Bonjour proxy activated

Use this checkbox to enable or disable the Bonjour proxy.

Network list

Use this table to specify the networks between which Bonjour services may be discovered. To function properly, the networks or interfaces need to be configured with an IPv4 or IPv6 address. This table offers you the following options:



Name

Specify a unique name for this table entry.

Entry active

Enable or disable this table entry.

Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

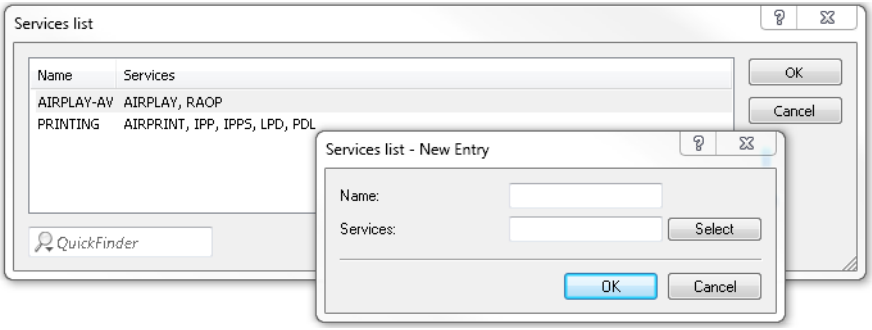
Comment

Enter a comment about this table entry.

Services list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

The following settings are available:



Name

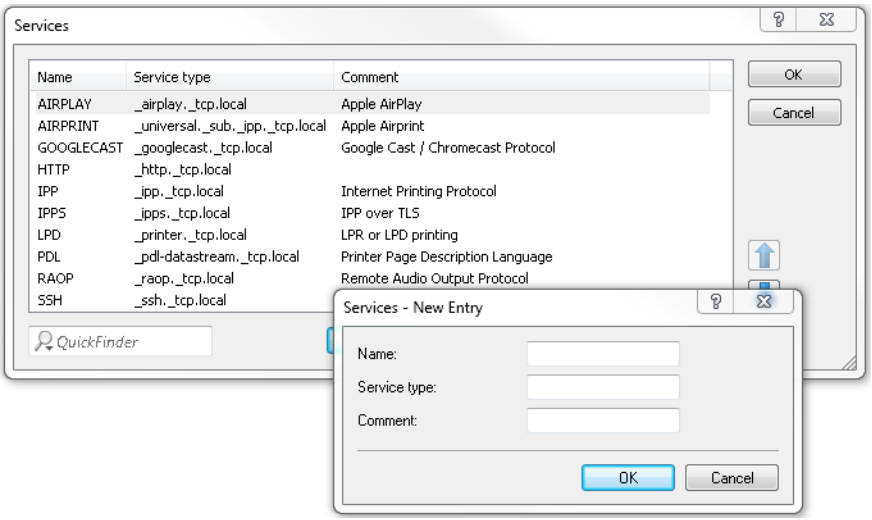
Specify a unique name for this table entry.

Services

Enter a comma-separated list of services that are to be available for use in the **Services** table.

Services

This table is used to specify the Bonjour service types that can be used in the services list. Additional settings are available as follows:



Name

Specify a unique name for this table entry.

Service type

Specify the Bonjour service type as a DNS SRV record, e.g. with `_http._tcp.local`.

Comment

Enter a comment about this table entry.

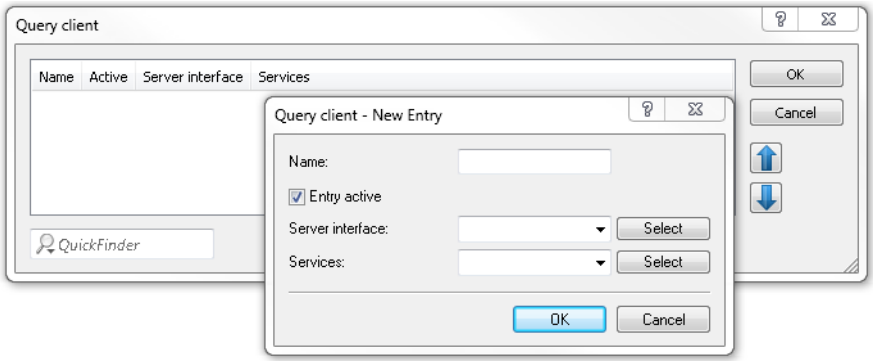
Automatically request network list services

With this item enabled, the device sends regular queries about which services (as specified in the network list) are available from the corresponding server interface. This option is enabled by default. This setting is also recommended.

If this setting is disabled, you need to manually enter the services to be queried into the **Query client** table.

Query client

To keep the Bonjour proxy services cache up-to-date all times, you need to configure regular queries about the desired services. The query client regularly contacts the configured service types for information about their availability.



Name

Specify a unique name for the corresponding entry.

Entry active

Activates or deactivates this table entry.

Server interface

Set an IPv4 network name or an IPv6 interface name that is to offer the Bonjour services (e.g. print services) and which will regularly be used by the router to make the queries.

Services

This references an entry in the list of services. These services are regularly queried by the router at the server interface. This entry may not be empty.

Query client interval

Set the interval in minutes in which the query client updates the Bonjour services configured in the **Query client** table. 15 minutes are defined by default.

Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

2.1.3 Additions to the Setup menu

Bonjour proxy

This menu contains the settings for the Bonjour proxy. The Bonjour proxy allows Bonjour services to be discovered across network boundaries.

SNMP ID:

2.104

Telnet path:

Setup

Operating

This entry is used to enable or disable the Bonjour proxy.

SNMP ID:

2.104.1

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

No

Query client interval

Set the interval in minutes in which the query client requests the Bonjour services configured in the **Query client** table.

SNMP ID:

2.104.2

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 999 Minutes

Default:

15

Special values:

0

Network list

Use this table to specify the networks between which Bonjour services may be discovered.

SNMP ID:

2.104.3

Telnet path:

Setup > **Bonjour-Proxy**

Name

Specify a unique name for this table entry.

SNMP ID:

2.104.3.1

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

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

Default:

empty

Active

This entry is used to enable or disable the Bonjour proxy for the corresponding combination of client and server network.

SNMP ID:

2.104.3.2

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

No
Yes

Default:

No

Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

SNMP ID:

2.104.3.3

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

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

Default:

empty

Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

SNMP ID:

2.104.3.4

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

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

Default:

empty

Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

SNMP ID:

2.104.3.5

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

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

Default:

empty

Comment

Enter a comment about this entry.

SNMP ID:

2.104.3.6

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

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

Default:

empty

Service list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

SNMP ID:

2.104.4

Telnet path:

Setup > **Bonjour-Proxy**

Name

Enter a name for this list here.

SNMP ID:

2.104.4.1

Telnet path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

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

Default:

empty

Services

This table is used to specify the Bonjour service types that can be used in the services list.

Specify multiple services with a comma-separated list.

SNMP ID:

2.104.4.2

Telnet path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

Services

This table lists the default services for communicating between networks. You can extend the table according to your needs.

SNMP ID:

2.104.5

Telnet path:

Setup > **Bonjour-Proxy**

Name

Enter the service name here (e.g. "HTTP").

SNMP ID:

2.104.5.1

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

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

Default:

empty

Service type

Specify the service type here (e.g. `_http._tcp.local`).

SNMP ID:

2.104.5.2

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

empty

Comment

Enter a comment about this service.

SNMP ID:

2.104.5.6

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

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

Default:

empty

Query client

The table lists the services that should be requested by the router at regular intervals.

SNMP ID:

2.104.6

Telnet path:

Setup > **Bonjour-Proxy**

Name

Specify a unique name for the corresponding entry.

SNMP ID:

2.104.6.1

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

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

Default:

empty

Active

Enable or disable this entry.

SNMP ID:

2.104.6.2

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

No
Yes

Default:

No

Server interface

Here you specify the server interface to be used for the client query.

SNMP ID:

2.104.6.3

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

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

Default:

empty

Services

Here you specify which services should be requested.

SNMP ID:

2.104.6.4

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

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

Default:

empty

Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

SNMP ID:

2.104.7

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 4294967295

Default:

1024

Auto-query services

Activate the checkbox if the Query Client should periodically query the configured service types for their availability.

SNMP ID:

2.104.8

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

Yes

2.1.4 Additions to the Status menu

Bonjour proxy

This menu contains the current values of the Bonjour proxy.

SNMP ID:

1.104

Telnet path:

Status

Instance count

This value shows the current number of cached instances of the service.

SNMP ID:

1.104.1

Telnet path:

Status > **Bonjour-Proxy**

MDNS cache

This table contains the cache information of the multicast domain name system (mDNS).

SNMP ID:

1.104.2

Telnet path:

Status > **Bonjour-Proxy**

Service propagation

This table contains information about the propagated services.

SNMP ID:

1.104.3

Telnet path:

Status > **Bonjour-Proxy**

Clear cache

This command clears the current mDNS cache content.

SNMP ID:

1.104.4

Telnet path:

Status > **Bonjour-Proxy**

3 Wireless LAN

3.1 Managing WLAN sessions using RADIUS CoA

As of LCOS version 10.0, RADIUS CoA (Change of Authorization) allows you to modify the attributes of a current WLAN connection or to terminate the connection using the "disconnect" method.

RADIUS COA is not supported by the LANCOM L-151gn Wireless.

CoA can be enabled for each WLAN SSID individually. Using the command-line console, the command "`show wlan dynauth`" displays the WLAN sessions currently active on the CoA module

The following WLAN attributes can be modified by RADIUS CoA:

- LCS-TxRateLimit
- LCS-RxRateLimit
- VLAN-ID

The following attributes are required to modify the VLAN ID:

Tunnel-Type=VLAN

This attribute is preset

Tunnel-Medium-Type=IEEE-802

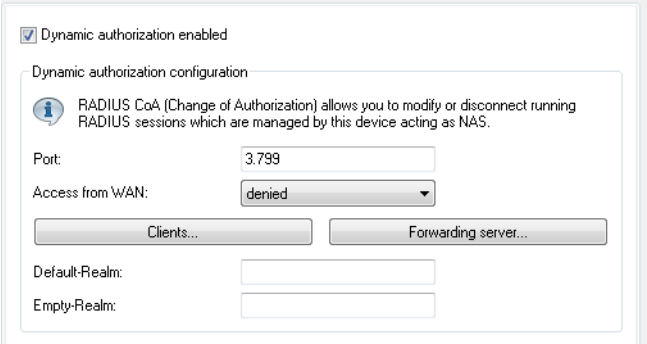
This attribute is preset

Tunnel-Private-Group-Id=42

Specifies a new VLAN ID.

3.1.1 Using LANconfig to configure the management of WLAN sessions using RADIUS CoA

In order to configure dynamic authorization (CoA) with LANconfig, navigate to **RADIUS** > **Dyn. Authorization**.



Dynamic authorization enabled

Activate or deactivate dynamic authorization here.

Port

Contains the default port where CoA messages are received.

Access from WAN

This entry specifies whether messages are accepted from the WAN, via VPN only, or prohibited.

Clients

Enter all of the CoA clients here that are permitted to send messages to the NAS.

Forwarding server

To forward CoA messages, the forwarding servers are specified here.

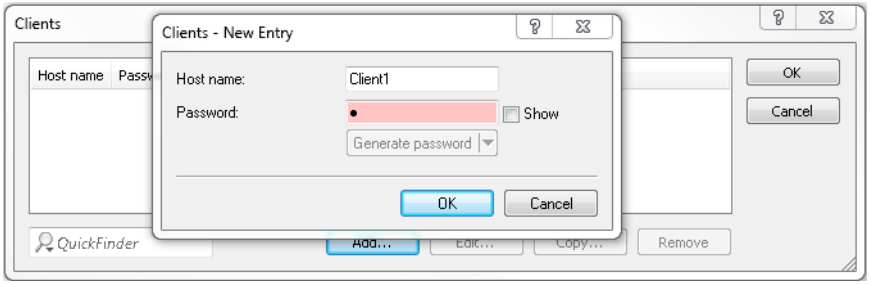
Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Empty realm

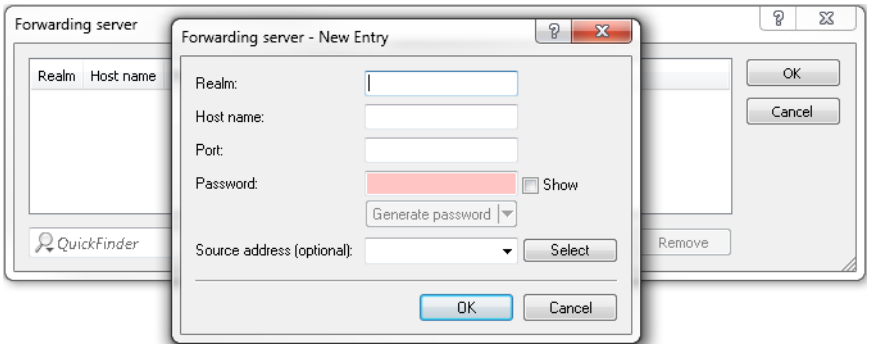
This realm is used when the specified username does not contain a realm.

To add CoA clients for dynamic authorization, click the button **Clients** and add a new entry to the table.



Enter a host name for the client and set a password for the client to access the NAS.

To add new forwarding servers for dynamic authorization, click the button **Forwarding server** and add a new entry to the table.



Realm

Here you enter the realm used by the RADIUS server to identify the forwarding destination.

If applicable, enter any existing forwarding servers that are specified under **RADIUS** > **Server** > **Forwarding** > **Forwarding server**.

Host name

Specify the host name of the forwarding server.

Port

Specify the server port used to forward the requests.

Password

Set a password that is required by the client to access the RADIUS server.

Source address (optional)

Optionally, specify a source address.

Specify which logical WLAN interfaces should use dynamic authorization. You enable or disable them under **Wireless LAN** > **General** > **Logical WLAN settings** with the checkbox **RADIUS CoA activated** for the appropriate interface.

3.1.2 Additions to the Setup menu

Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176*.

SNMP ID:

2.25.19

Telnet path:

Setup > **RADIUS**

Operating

This entry enables or disables the dynamic authorization by RADIUS.

SNMP ID:

2.25.19.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Port

This entry specifies the port on which CoA messages are accepted.

SNMP ID:

2.25.19.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

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

Default:

3799

WAN access

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

SNMP ID:

2.25.19.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Clients

All of the CoA clients that send messages to the NAS are entered into this table.

SNMP ID:

2.25.19.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

HostName

This entry contains the unique identifier of the client that sends messages to the NAS.

SNMP ID:

2.25.19.4.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

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

Default:

empty

Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

SNMP ID:

2.25.19.4.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

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

Default:

empty

Forward-Servers

To forward CoA messages, the forwarding servers are specified here.

SNMP ID:

2.25.19.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

SNMP ID:

2.25.19.5.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

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

Default:

empty

HostName

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

SNMP ID:

2.25.19.5.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

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

Default:

empty

Port

This entry contains the port for communications with the forwarding server.

SNMP ID:

2.25.19.5.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

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

Default:

0

Secret

This entry specifies the secret required to access the forwarding server.

SNMP ID:

2.25.19.5.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

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

Default:

empty

Loopback

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

SNMP ID:

2.25.19.5.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

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

Default:

empty

Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

SNMP ID:

2.25.19.6

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

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

Default:

empty

Empty realm

This realm is used when the specified username does not contain a realm.

SNMP ID:

2.25.19.7

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

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

Default:

empty

Radclient

Use the command `do Radclient [...]` to send CoA messages.

The Radclient command is structured as follows:

```
do Radclient <server[:port]> coa/disconnect <secret> <attribute-list>
```

Outputs all known and active RADIUS sessions

Entering the command `show dynauth sessions` on the command line lists the RADIUS sessions that are known to the CoA module. This outputs the session reported by the Public Spot module. The known attributes for this session are shown in the section "Context":

```
Session with MAC-Address: [a3:18:22:0c:ae:df] Context:
[NAS-IP-Address: 192.168.1.254,User-Name: user46909, NAS-Port-Id:
WLC-TUNNEL-1, Framed-IP-Address: 192.168.1.78]
```

The attributes "NAS-IP-Address" and "Username" identify the active session. If you wish to limit the bandwidth for the active session, you enter the Radclient command with these values along with the attributes "LCS-TxRateLimit" and "LCS-RxRateLimit" in combination with the transmission and reception limits in kbps:

do Radclient 192.168.1.254 coa secret "User-Name=user46909;NAS-IP-Address=192.168.1.254;LCS-TxRateLimit=5000;LCS-RxRateLimit=5000"

Note that the identification attributes and the attributes being modified must be specified with the same rights in the attribute list.

Terminate an active RADIUS session

A running RADIUS session is terminated by using the Radclient command to send a disconnect message:

```
do Radclient 192.168.1.254 disconnect secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254"
```

The Radclient command integrated in LCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

SNMP ID:

2.25.19.8

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Dyn-Auth

This entry enables or disables dynamic authorization by RADIUS CoA on the corresponding interface.

SNMP ID:

2.23.20.1.28

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

No
Yes

Default:

No

4 WLAN management

4.1 WLC script rollout for certain versions of LCOS

As of LCOS version 10.0, you have the option of specifying WLC-controlled script rollouts for certain versions of LCOS. This allows different versions of LCOS with their differing configurations to integrate into a common WLAN installation.

4.1.1 Using LANconfig to configure WLC script rollout

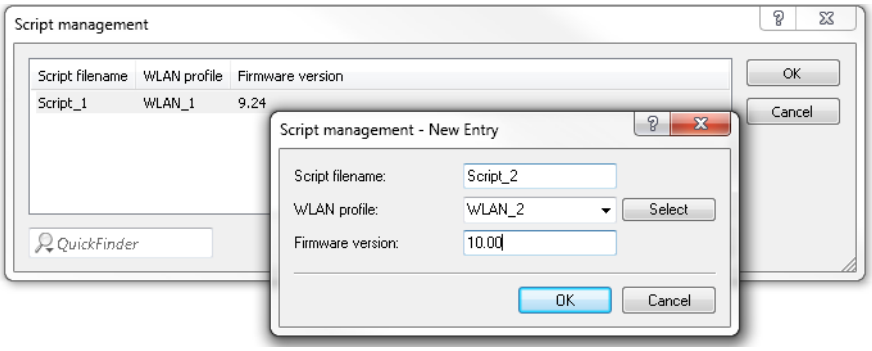
Under certain circumstances, you may need to work with configurations based on different versions of LCOS within a single WLAN installation. LANconfig features script management, so that you can rollout scripts with particular firmware versions for your various WLAN profiles.

Please note that it is not possible to assign multiple scripts with different firmware versions to an individual WLAN profile.

In LANconfig, the script management table is located under **WLAN Controller** > **AP Update** > **Script management**.

You specify new scripts for your WLAN profiles by adding new entries to the table.

The dialog in LANconfig has changed as follows:



> **Firmware version**

By specifying a firmware version, you determine the LCOS version set in the script that is rolled out.

Please enter the firmware version in the form **xx.yy**, e.g. 10.00 or 9.24.

4.1.2 Additions to the Setup menu

Firmware version

Use this item to set the firmware version for which the corresponding script is to be rolled out.

Please enter the firmware version in the form **xx.yy**, e.g. 10.00 or 9.24.

SNMP ID:

2.37.27.16.3

Telnet path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

Possible values:

Max. 6 characters from `[0-9].`

Default:

empty

5 Public Spot

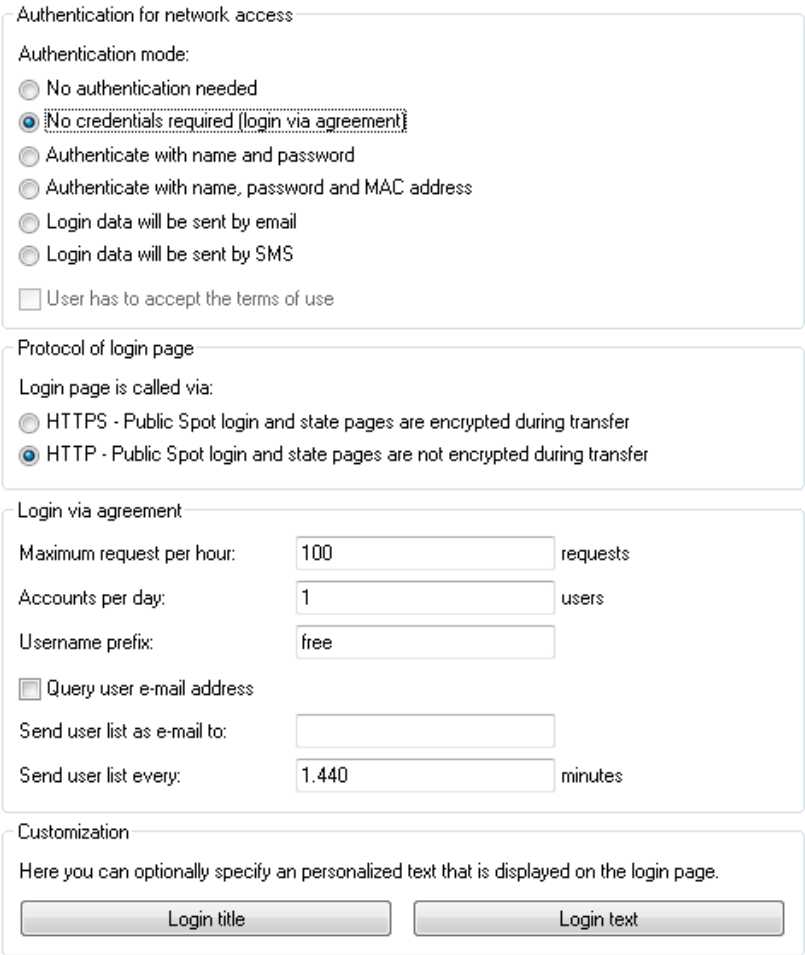
5.1 Requesting the user e-mail address upon "login via agreement"

As of LCOS version 10.0, you can optionally require users who wish to authenticate at your Public Spot to enter an e-mail address.

5.1.1 Configuring an address request with LANconfig

Users wishing to authenticate at your Public Spot can optionally be required to register themselves first by entering an e-mail address. The network access authentication setting is located in the dialog **Public Spot** > **Authentication** in the section "Login via agreement".

Changes to the dialog are as follows:



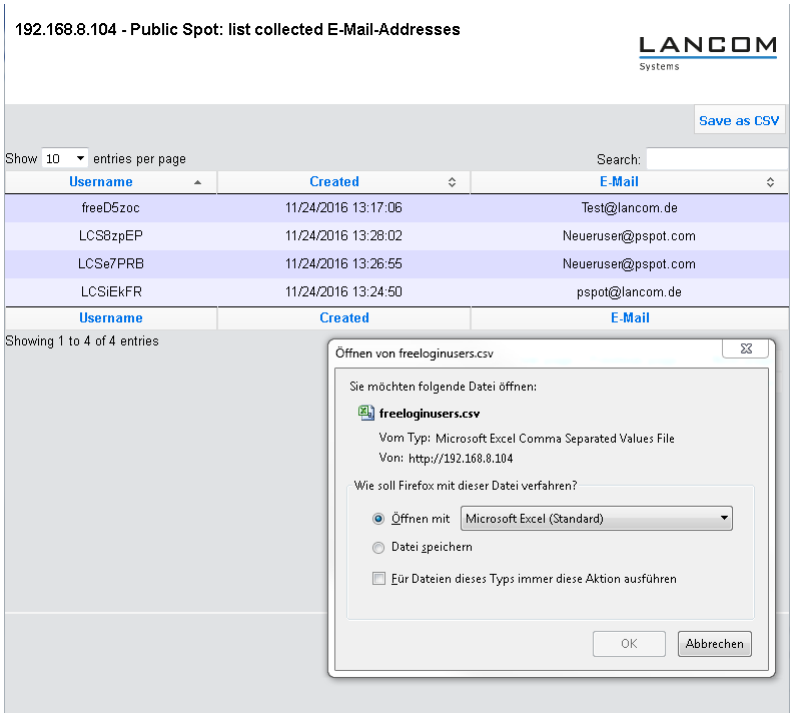
> **Query user e-mail address**: Enable this check box in order to query the user's e-mail address as a requirement for using the Public Spot. The device automatically enters the e-mail address specified here into the comments box of

the newly created RADIUS user. Once a day a list of all of the available addresses is stored in the flash memory of the device. This list is boot persistent.

- **Send user list as e-mail to**: Enter the e-mail address where the address list is to be sent. Only new entries that have been added since the last submission are sent. The address list is transmitted as a CSV file.
- **Send user list every**: This sets the interval at which the updated address list is sent to the specified e-mail address. This value is specified in minutes.

The Setup Wizard **Public Spot: list collected e-mail-addresses** in WEBconfig allows you to view the registered addresses and to export them as a CSV file.

Please note that this wizard is only visible when the "Query user e-mail address" option is enabled. It may be necessary to login to the device again.



5.1.2 Additions to the Setup menu

Require e-mail

This entry allows you to specify whether the e-mail address of the user should be requested.

SNMP ID:

2.24.41.4.4

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

No
Yes

Default:

No

E-Mail-List-Recipient

This entry contains the e-mail address to which the list of requested e-mail addresses is sent.

If you have already set the recipient e-mail address in LANconfig, it will be shown here.

SNMP ID:

2.24.41.4.7

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

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

Default:

empty

5.1.3 Additions to the Status menu

Free login

This menu enables you to see or delete users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17

Telnet path:

Status > **Public-Spot**

Users

This entry displays all of the active users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17.1

Telnet path:

Status > **Public-Spot** > **Free-Login**

Possible values:

User name
Displays the name of the created user.

Created
The time when the user was created.

E-mail
Displays the e-mail address entered for the created user

This field contains information only if the option "Query user e-mail address" is enabled.

Delete user

This menu enables you to delete users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17.2

Telnet path:

Status > **Public-Spot** > **Free-Login**

5.2 Configuring the headline of the Public Spot login page

As of LCOS version 10.0, you have the option of adding a headline to the login page of your Public Spot.

You can enter the title of your login page in six different languages. The available languages are English, German, French, Italian, Spanish and Dutch. The language used for the title of your Public Spot login page depends on the browser language set by the user.

5.2.1 Customized text or login title for the login page

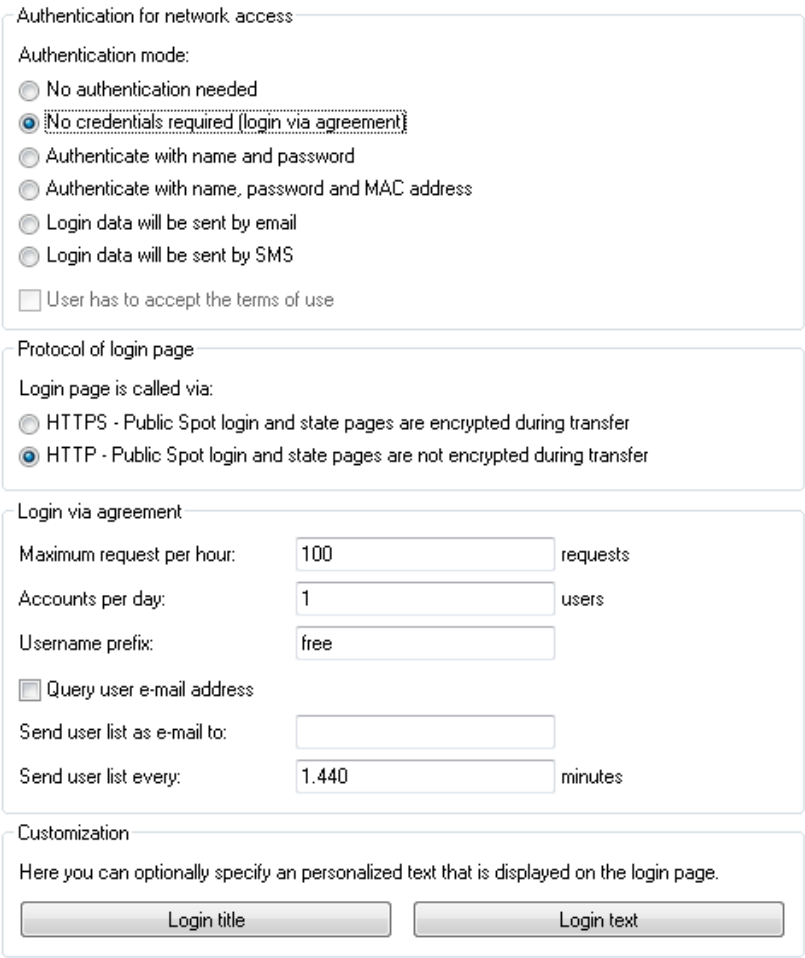
The Public Spot module gives you the option to specify customized **login text** and a **login title**, which appear on the login page in the box of the login form. The title and the text can be entered for a number of languages (English, German, French, Italian, Spanish and Dutch). The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text or title is specified for a language, then the device falls back to the English login text (if available).

Please note that the login text and the login title are separate items.

Carry out the following steps to set up customized text or title on the login page.

1. In LANconfig, open the configuration dialog for the device.

2. Navigate to the dialog **Public Spot** > **Authentication**, click on the button **Login text** or **Login title** and select a language.



3. In the dialog that opens, enter the text that your Public Spot should display to users. You can enter an HTML string with max. 254 characters composed of:

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

LANconfig automatically transforms umlauts into their respective equivalents (ü to `ue`; ß to `ss`; etc.). To type umlauts, use their HTML equivalents (such as `ü` for ü), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

```
Welcome!<br/><i>Please complete this form.</i>)
```

4. Click **OK** to complete your entries and load the configuration back to the device.

Once the configuration has been written successfully, the new login text and login title appears the next time the Public Spot page is called.

5.2.2 Additions to the Setup menu

Login instructions

This menu is used to set a login title for your Public Spot page. You can define the title in six languages (English, German, French, Italian, Spanish and Dutch).

SNMP ID:

2.24.61

Telnet path:

Setup > **Public-Spot-Module**

Language

This entry displays the language selected for the login title.

SNMP ID:

2.24.61.1

Telnet path:

Setup > **Public-Spot-Module** > **Login-Instructions**

Contents

Enter the login title for your Public Spot here.

SNMP ID:

2.24.61.1

Telnet path:

Setup > **Public-Spot-Module** > **Login-Instructions**

Possible values:

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

Default:

empty

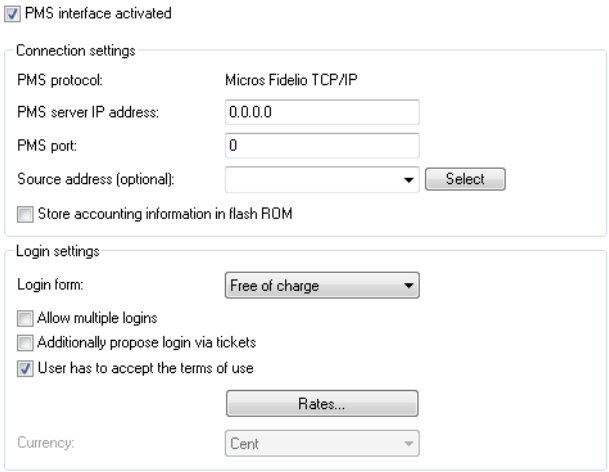
5.3 Confirmation of the terms of use on the PMS-login page

As of LCOS version 10.0, you have the option of requiring your users to accept the terms and conditions of use of your Public Spot on the PMS-login page.

5.3.1 Using LANconfig to configure confirmation of the terms of use on the PMS-login page

In LANconfig, navigate to **Public-Spot** > **PMS interface**, go to the "Login settings" section, and activate the checkbox **User has to accept the terms of use**.

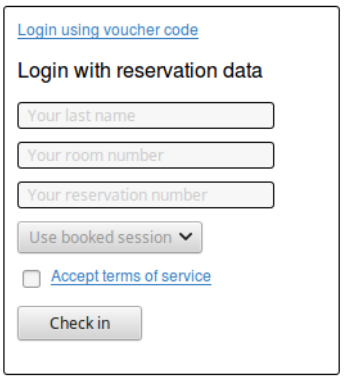
Please note that using this option requires the PMS interface to be enabled.



The dialog for the PMS interface has changed as follows:

> **User has to accept the terms of use**: Enable this checkbox in order for hotel guests to accept the terms and conditions for the use of your hotspot.

With the option enabled, the PMS-login page displays the checkbox for confirming the terms of use.



5.3.2 Additions to the Setup menu

User-Must-Accept-GTC

With this setting you enable or disable the confirmation of the terms of use on the PMS-login page.

SNMP ID:

2.64.11.14

Telnet path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

No

The user is not prompted to accept the terms of use.

Yes

The user is prompted to accept the terms of use.

Default:

No

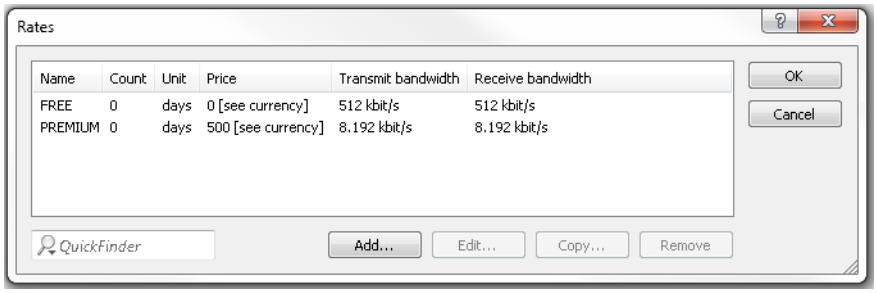
5.4 Tx and Rx bandwidths configurable for rates in the PMS module

As of LCOS version 10.0, you have the option to limit the transmit and receive bandwidths for each of the rates configured in the PMS module, and to give each rate an appropriate name (e.g. "Free" and "Premium"). When choosing a rate on the Public Spot login page, users see the rates along with their configured names.

If rates are already entered in the configuration at the time of a firmware update, these are automatically given a name according to the pattern **Rate_1** to **Rate_n**.

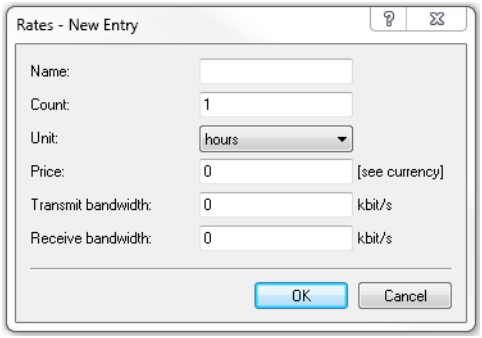
5.4.1 Using LANconfig to configure Tx and Rx bandwidths for rates in the PMS module

To configure the rates in the PMS interface of your device, go to the menu **Public-Spot** > **PMS-Interface** > **Rates**.



You can edit existing rates or add new entries to the table. Changes to the dialog are as follows:

> **Rates**: If you offer fee-based Internet access, this table is used to manage the tariff rates for the accounting.



> **Name**: Specify a descriptive name for the rate here.
> **Count**: Enter the rate for the time quota, for example, `1`. Combined with the unit, this is the value shown in the screenshot above, e.g., 1 hour.
> **Unit**: Select the unit for the time quota from the list. Possible values are: `Minutes`, `Hours`, `Days`
> **Price** Enter the amount charged for the time quota. In combination with the currency selected in the Login settings, the value amounts to 50 cents, for example.
> **TX bandwidth**: Here you specify the maximum transmit bandwidth for this rate.
> **RX bandwidth**: Here you specify the maximum receive bandwidth for this rate.

A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

5.4.2 Additions to the Setup menu

Name

Use this entry to specify a name for this rate.

SNMP ID:

2.64.15.4

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

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

Default:

empty

Tx bandwidth

Use this entry to restrict the transmit (Tx) bandwidth.

SNMP ID:

2.64.15.5

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

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

Default:

0

Special values:

0

The value "0" disables the restriction of the transmit bandwidth.

Rx bandwidth

Use this entry to restrict the receive (Rx) bandwidth.

SNMP ID:

2.64.15.6

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

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

Default:

0

Special values:

0

The value "0" disables the restriction of the receive bandwidth.

5.5 Support for RADIUS CoA

As of LCOS version 10.0, the Public Spot module optionally accepts RADIUS CoA commands.

RADIUS COA is not supported by the LANCOM L-151gn Wireless.

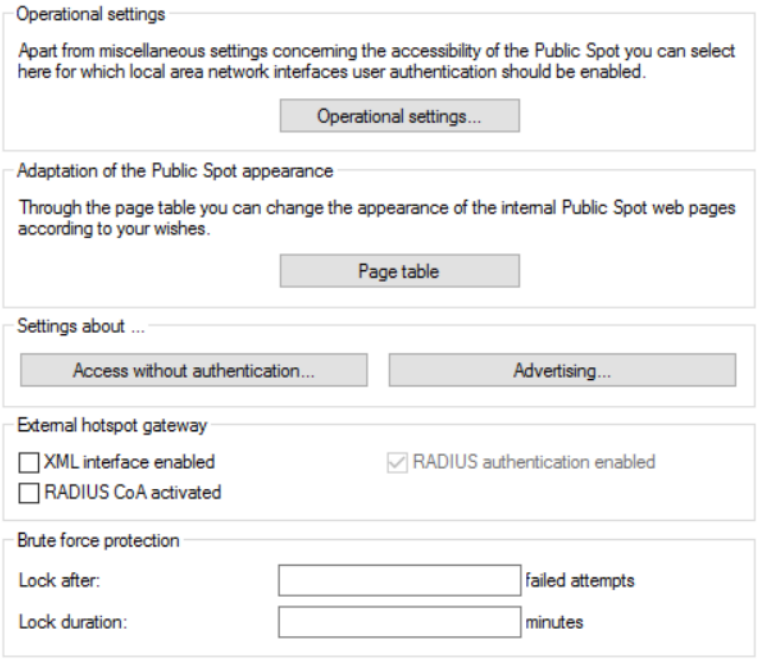
5.5.1 Enabling the acceptance of RADIUS CoA requests by the Public Spot

- The following steps assume that you have a functioning Public Spot that can be connected to an external hotspot gateway.
- The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

The following section explains how you enable RADIUS-CoA support as per RFC3576 in the Public Spot.

1. In LANconfig, open the device configuration and navigate to **Public Spot** > **Server**.



2. Set a checkmark under **RADIUS CoA activated**.
3. Now write the configuration back to the device.

From now on, the Public Spot processes any RADIUS CoA requests received from an external hotspot gateway.

5.5.2 Additions to the Setup menu

Accept CoA

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

With this entry you enable or disable the dynamic authorization of Public Spot users by means of RADIUS CoA via an external hotspot gateway.

SNMP ID:

2.24.55

Telnet path:

Setup > **Public-Spot-Module**

Possible values:

No

Dynamic authorization disabled. If there is a change to the RADIUS connection attributes, authorized users remain unaffected until their session expires.

Yes

Dynamic authorization enabled. The external gateway is able to modify the connection attributes of authorized users, or to disconnect existing sessions.

Default:

No

6 RADIUS

6.1 Support of tunnel-password and LCS-routing-tag attributes

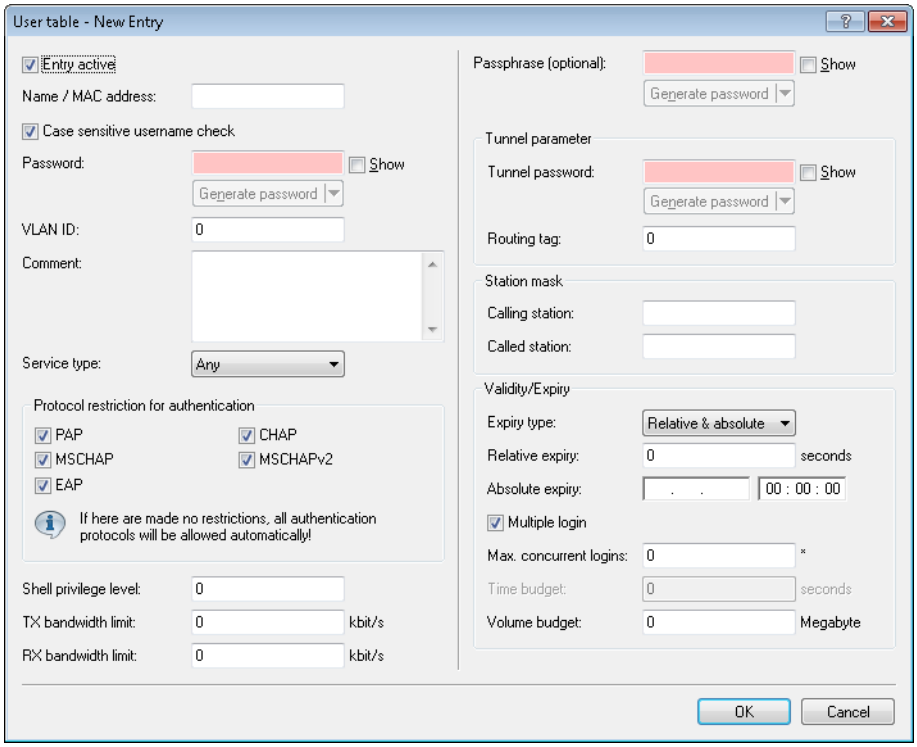
As of LCOS version 10.0, LANCOM RADIUS servers support the attributes "Tunnel-Password" and "LCS-Routing-Tag", which you can specify for each user account.

This helps an organization to store user data on a central RADIUS server and to minimize the effort required for the configuration of VPN scenarios.

6.1.1 Using LANconfig to configure Tunnel-Password and Routing-Tag attributes

In LANconfig, specify the attributes of "Tunnel-Password" and "Routing-Tag" under **RADIUS** > **Server** > **User table**.

Add a new entry to the table or edit an existing entry.



In the "Tunnel parameter" section, set values for the corresponding attributes:

Tunnel-Password

Here you enter the password used by the corresponding user to authenticate for a VPN connection via IKEv2 or L2TP.

Routing tag

Specify the routing tag to be used for the connection.

6.1.2 Additions to the Setup menu

Tunnel-Password

This entry sets the connection password for each user.

SNMP ID:

2.25.10.7.23

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

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

Default:

empty

LCS-Routing-Tag

Specify the routing tag for this connection.

SNMP ID:

2.25.10.7.24

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

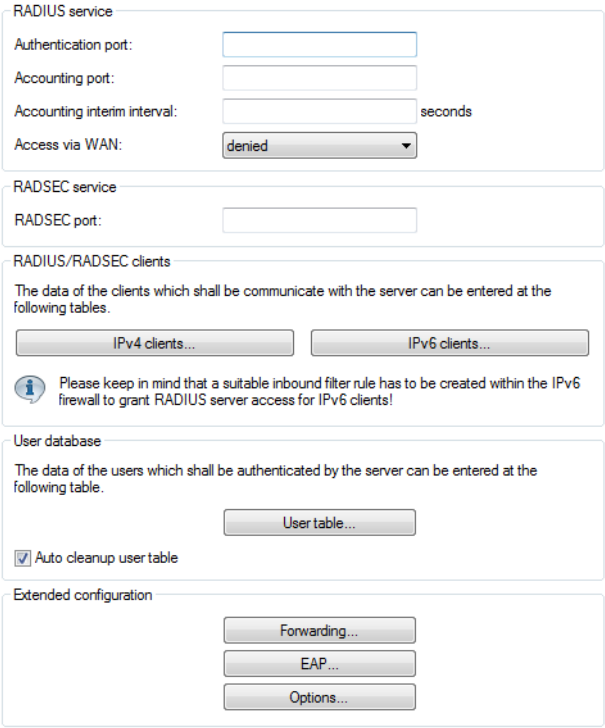
Max. 5 characters from `[0-9]`

Default:

0

6.2 Restricting WAN access to the RADIUS server

As of version 10.0, LCOS allows the restriction of access from the IPv4 network.



WAN access to the RADIUS server

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

6.2.1 Additions to the Setup menu

IPv4-WAN-Access

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

SNMP ID:

2.25.10.22

Telnet path:

Setup > **RADIUS** > **Server**

Possible values:

No

The RADIUS server rejects WAN traffic from the IPv4 network.

Yes

The RADIUS server accepts WAN traffic from the IPv4 network.

VPN

The RADIUS server accepts only WAN traffic from the IPv4 network that arrives at the device over a VPN connection.

Default:

No

7 Voice over IP – VoIP

7.1 Client-side support for SIPS/SRTP

As of LCOS version 10.0, the Voice Call Manager allows you to configure the encrypted transmission of authentication data from SIP users by means of SIPS (session initiation protocol security) and SRTP (secure real-time transport protocol).

7.1.1 Using LANconfig to configure SIPS/SRTP support

You configure SIPS and SRTP with LANconfig under **Voice Call Manager** > **Users** > **SIP users**. Add a new user to the table or edit existing entries.

The SIP user dialog has been improved as follows:

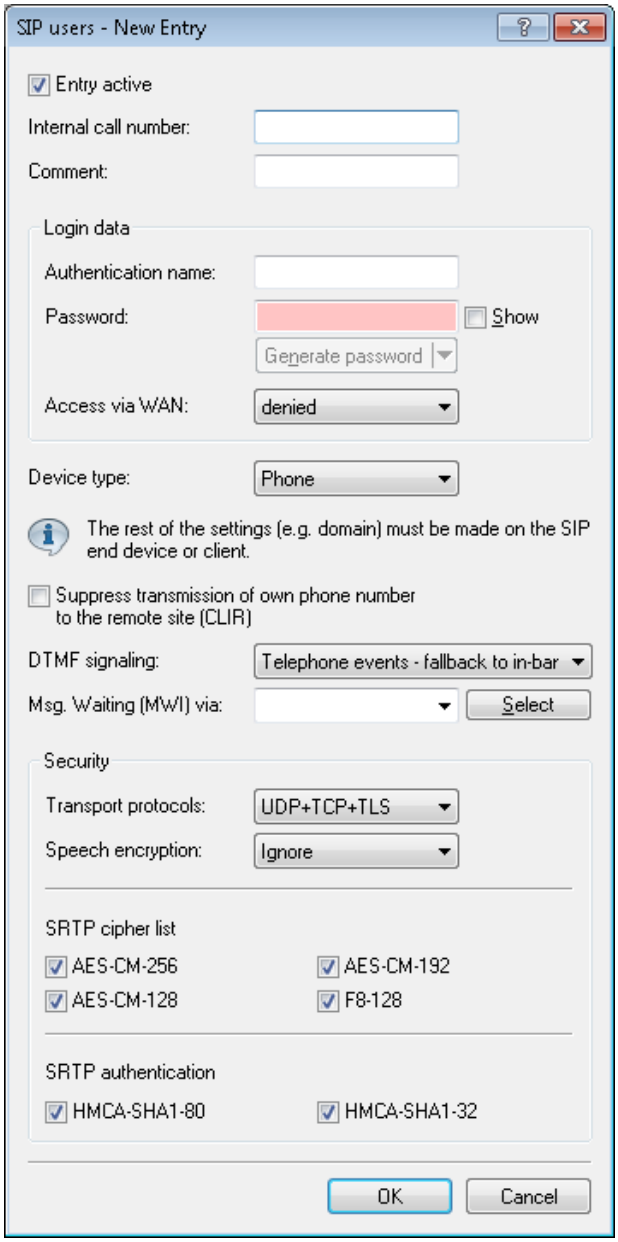


Figure 1: Adding a new entry to the SIP user table

Transport protocols

Select a protocol used by this user to communicate with the local SIP server. If the appropriate protocol is not selected, SIP requests from this user will be rejected with a SIP error response (SIP/406). This ensures that no users are able to register with a protocol that has not been allowed here.

UDP

All SIP packets to this SIP user are transmitted via connectionless UDP. Most SIP users support this setting.

TCP

All SIP packets to this SIP user are transmitted via connection-oriented TCP. The TCP connection is maintained for the duration of the registration.

TLS

All SIP packets to this SIP user are transmitted connection-oriented. Also, all SIP packets are encrypted.

Speech encryption

Use this entry to specify the protocol used to transmit the voice data (RTP/SRTP) of a call to the local SIP server.

Reject

There is no encryption proposal for calls by this user. Calls by this user with an encryption proposal are rejected. The voice channel is never encrypted.

Ignore

There is no encryption proposal for calls by this user. However, calls from this user with an encryption proposal are accepted. However, the voice channel is never encrypted.

Prefer

Calls by this user cause an encryption proposal. Calls from this user without an encryption proposal are also accepted. The voice channel is only encrypted if the user supports encryption.

Force

Calls by this user cause an encryption proposal. Calls by this user without a corresponding encryption proposal are ignored. The speech channel is either encrypted or is not established.

If you require the encrypted transmission of voice data, the signaling must also use an encrypted channel. Otherwise an attack on the unsecured signaling could potentially expose the key for the voice data. Please be aware that your provider may decrypt your voice data and re-transmit it newly encrypted or even unencrypted. The use of SRTP is no guarantee of end-to-end encryption.

SRTP cipher list

Here you specify the encryption method used for communication with the user. Select one or more of the following methods:

AES-CM-256

Encryption is performed using AES256. The key length is 256 bits.

AES-CM-128

Encryption is performed using AES128. The key length is 128 bits.

AES-CM-192

Encryption is performed using AES192. The key length is 192 bits.

F8-128

Encryption is performed using F8-128. The key length is 128 bits.

SRTP authentication

With this setting you restrict the amount of (proposed or accepted) SRTP suites that are negotiated with the corresponding user. If you do not select one or more of the ciphers shown below for encrypting the SRTP packets, the device will never propose the corresponding SRTP suite(s) and they are never selected. In this way you can force the best possible encryption.

HMAC-SHA1-80

SIP-user authentication is performed with the hash algorithm HMAC-SHA1-80. The hash length is 80 bits.

HMAC-SHA1-32

SIP-user authentication is performed with the hash algorithm HMAC-SHA1-32. The hash length is 32 bits.

7.1.2 Additions to the Setup menu

Transport

This entry is used to select a protocol used by this user to communicate with the local SIP server.

SNMP ID:

2.33.3.1.1.22

Telnet path:

Setup > **Call-Manager** > **Users** > **SIP-User**

Possible values:

UDP

All SIP packets to this SIP user are transmitted via connectionless UDP. Most SIP users support this setting.

TCP

All SIP packets to this SIP user are transmitted via connection-oriented TCP. For this purpose, a TCP connection is established and maintained for the duration of the registration.

TLS

Like TCP, but all of the SIP packets are encrypted.

Default:

UDP

TCP

TLS

SRTP

With this entry, you configure the secure real-time transport protocol (SRTP) for the encryption and transmission of SIP-user authentication data.

SNMP ID:

2.33.3.1.1.23

Telnet path:

Setup > **Call-Manager** > **Users** > **SIP-User**

Possible values:

Reject

Encryption is not proposed for this user's calls. Calls by this user with an encryption proposal are rejected. The voice channel is never encrypted.

Ignore

Encryption is not proposed for calls by this user. Calls by this user with an encryption proposal are also accepted. However, the voice channel is never encrypted.

Prefer

Encryption is offered for this user's calls. Calls by this user without an encryption proposal are accepted. The voice channel is only encrypted if the user supports encryption.

Forced

Encryption is offered for this user's calls. Calls by this user without an encryption proposal will fail. The speech channel is either encrypted or is not established.

Default:

Ignore

SRTP ciphers

Here you select the encryption method for communications with the user.

SNMP ID:

2.33.3.1.1.24

Telnet path:

Setup > **Call-Manager** > **Users** > **SIP-User**

Possible values:

AES-CM-256

Encryption uses the AES256 method and a key length of 256 bits.

AES-CM-192

Encryption uses the AES192 method and a key length of 192 bits.

AES-CM-128

Encryption uses the AES128 method and a key length of 128 bits.

F8-128

Encryption uses the F8-128 method and a key length of 128 bits.

Default:

AES-CM-256

AES-CM-192

AES-CM-128

F8-128

SRTP-Message-Auth-Tags

Here you specify the authentication method for this user.

SNMP ID:

2.33.3.1.1.25

Telnet path:

Setup > **Call-Manager** > **Users** > **SIP-User**

Possible values:

HMAC-SHA1-80

Authentication is performed using the hash algorithm HMAC-SHA1-80 (hash length 80 bits).

HMAC-SHA1-32

Authentication is performed using the hash algorithm HMAC-SHA1-32 (hash length 32 bits).

Default:

HMAC-SHA1-80

HMAC-SHA1-32

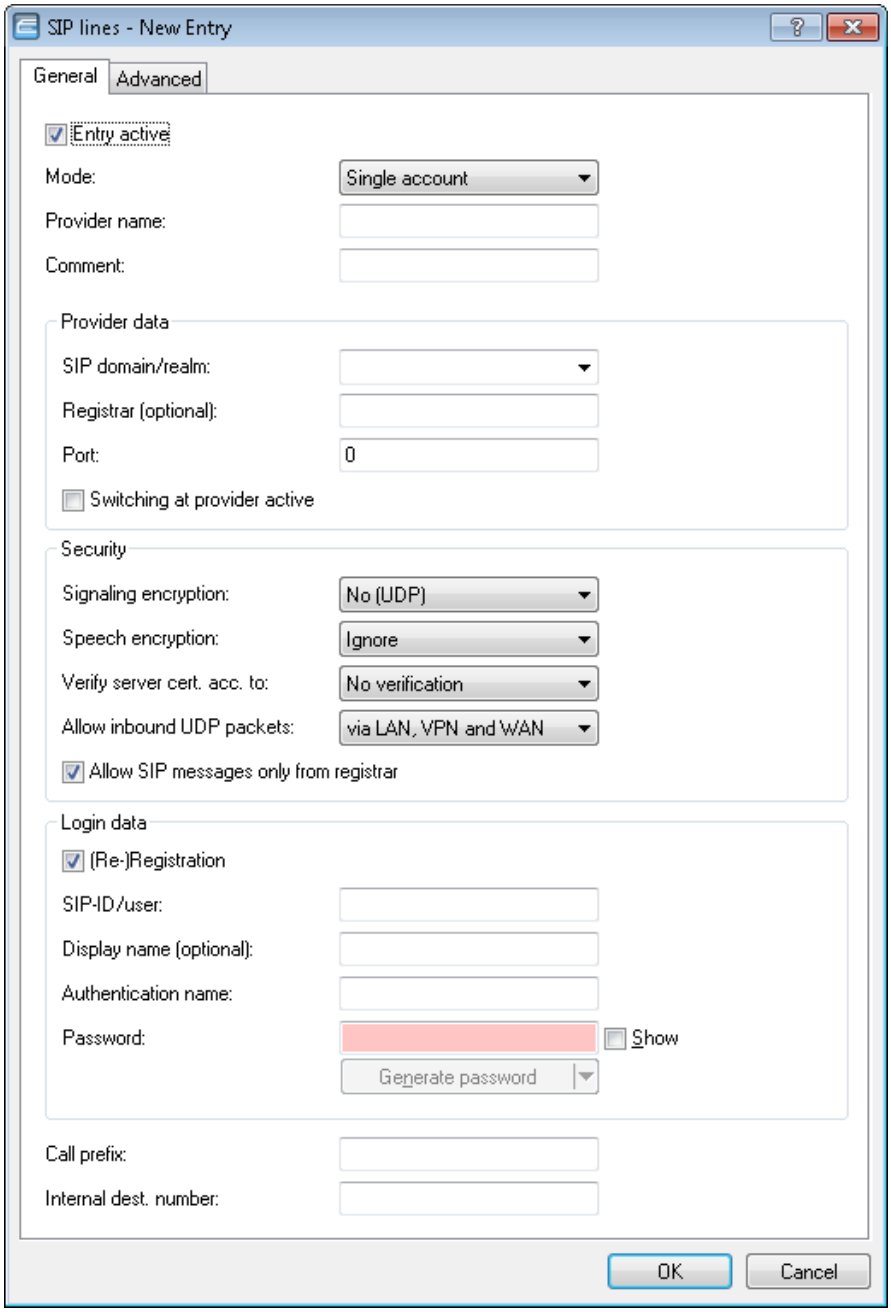
7.2 Restricting the processing of incoming UDP packets on SIP lines

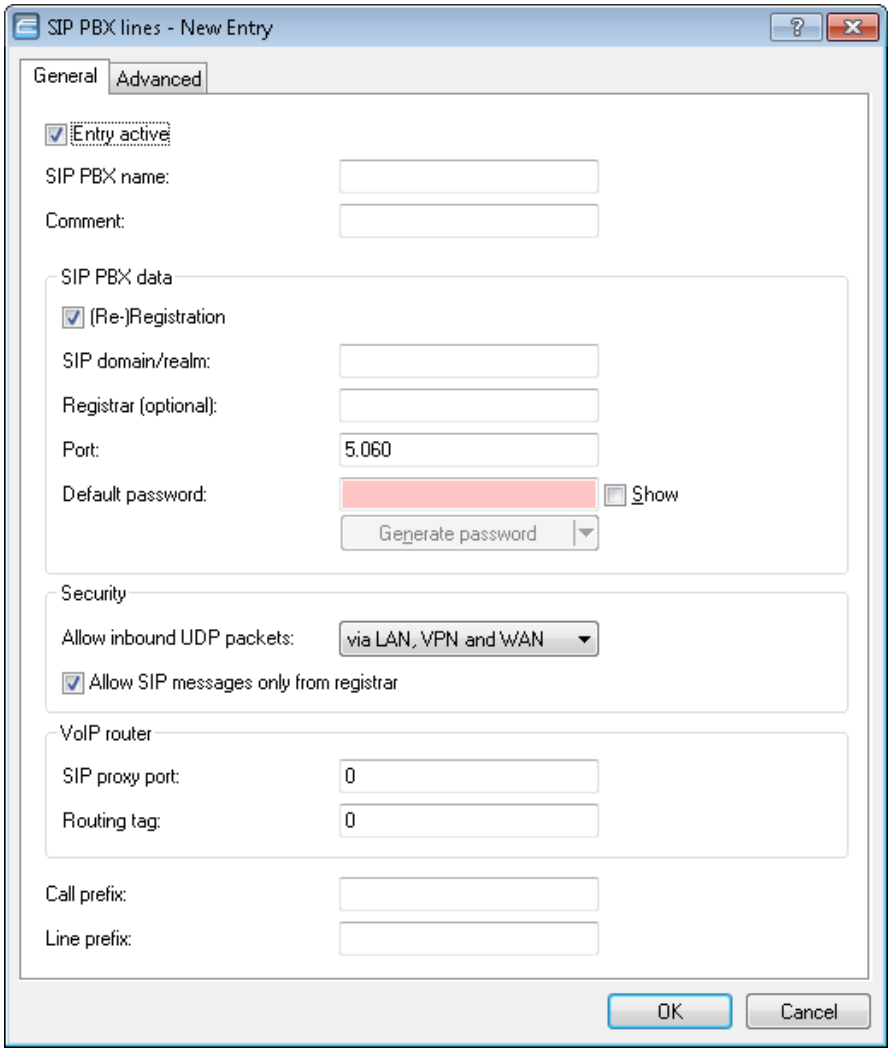
As of LCOS version 10.0, you have the option of controlling the reception of incoming UDP packets, for the case where the provider line uses UDP to communicate with the registrar.

7.2.1 Using LANconfig to configure restrictions on the processing of incoming UDP packets

The settings are configured under **VoIP Call Manager** > **Lines** by clicking the button **SIP lines** or **SIP PBX lines**.

Changes to the user interface are as follows:





Allow inbound UDP packets

If the provider line uses UDP to communicate with the registrar, it receives UDP packets on the desired local port. With this setting you specify the network context in which a UDP packet is accepted. The device only accepts a packet from the WAN / VPN / LAN if you have activated the corresponding setting. Otherwise the packet is dropped.

Allow SIP messages only from registrar

Enable this checkbox if you want to receive SIP messages only through the registrar.

7.2.2 Additions to the Setup menu

Allow inbound UDP from

With this setting you specify the network context in which the device accepts a UDP packet.

SNMP ID:

2.33.4.1.1.33

Telnet path:

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

Possible values:

LAN
VPN
WAN

Default:

LAN

VPN

WAN

Allow inbound UDP from

With this setting you specify the network context in which a UDP packet is accepted.

SNMP ID:

2.33.4.2.1.22

Telnet path:

Setup > **Call-Manager** > **Line** > **SIP-PBX** > **PBX**

Possible values:

LAN
VPN
WAN

Default:

LAN

VPN

7.3 Terminating a SIP trunk in the LAN

As of LCOS version 10.0, you have the possibility to connect a SIP PBX with your device via a trunk line, provided that the PBX is located in the same network.

SIP users

Users who are connected to the LAN by means of SIP. For the configuration of the user, it is unimportant if the LAN is accessed locally or via VPN (via the Internet). Along with SIP phones, you have also the option of setting up a SIP PBX as a user (internal SIP trunk connection).

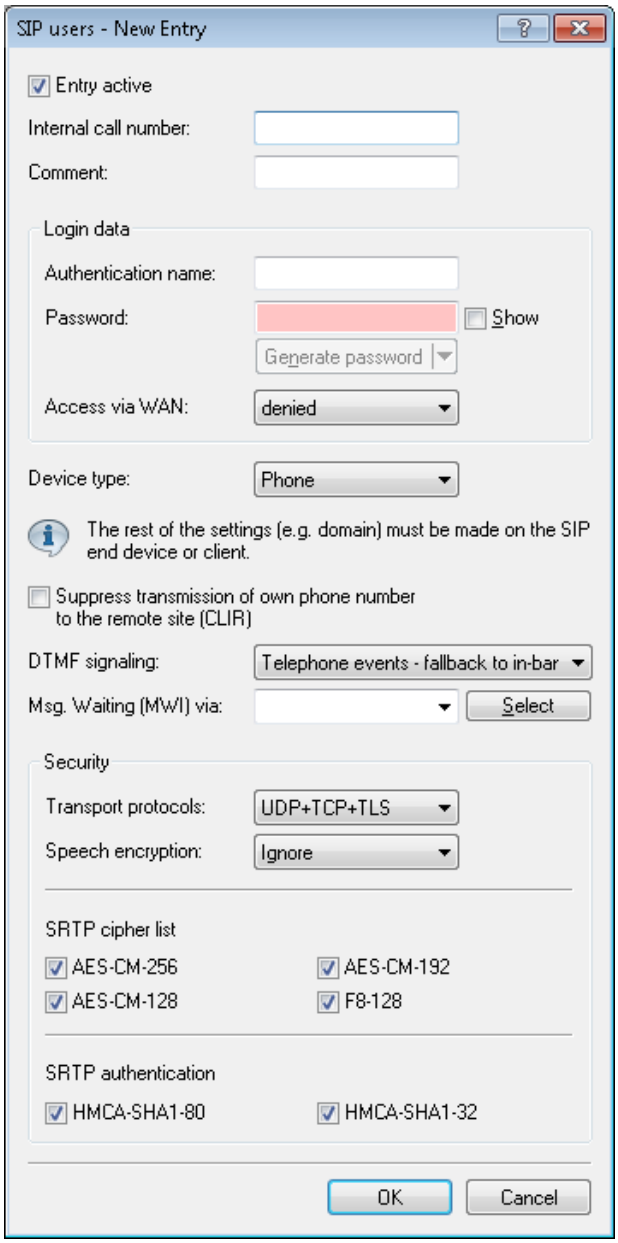


Figure 2: Adding a new entry to the SIP user table

Internal telephone number

- Telephone number of the SIP phone
- Name of the user (SIP URI)
- Switchboard number of the SIP PBX, followed by a #. Your SIP PBX must be in the same network as your device, either locally or connected via VPN (internal SIP trunk connection).

8 LANCOM Management Cloud (LMC)

As of LCOS version 10.0, it is possible to integrate LANCOM devices into the "LANCOM Management Cloud".

The LANCOM Management Cloud is the world's first hyper-integrated management system for the intelligent organization, optimization and control of your entire network architecture. State-of-the-art software-defined networking technology drastically simplifies the provision of integrated networks, so that the manual configuration of individual devices has become a thing of the past.

You have the option of connecting to the public LANCOM Management Cloud (public cloud) or to set up a privately hosted LANCOM Management Cloud (private cloud).

8.1 Basics of the LANCOM Management Cloud

The LANCOM Management Cloud (LMC) is capable of managing any size of "software-defined" networks. The LMC handles the configuration of all of the network components to minimize the amount of work involved in monitoring and configuration.

Further information about the LANCOM Management Cloud is available from *https://www.lancom-systems.com/cloud*.

If you wish to use the LANCOM Management Cloud for the configuration and monitoring of your device, the device needs to be paired with the LMC.

8.2 Pairing devices with the LANCOM Management Cloud

This chapter describes the different ways of pairing LANCOM devices with the LMC. Existing devices are paired in a different way than Cloud-ready devices.

Cloud-ready devices are LANCOM devices that the manufacturer has already equipped with LCOS version 10.0 or higher (LANCOM switches: Switch OS 3.30) and that have a PIN for pairing with the LMC.

Existing devices are LANCOM devices that have been updated from an older LCOS version to version 10.0 (LANCOM switches: Switch OS 3.30) or higher, which readies them for management by the LMC.

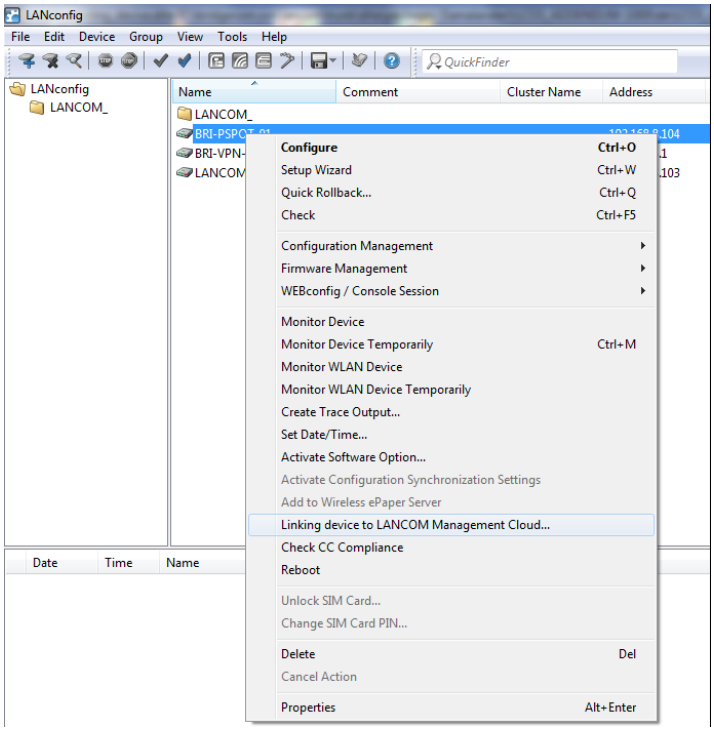
If you have a Cloud-ready device, no pairing is required. All you have to do in this case is to add your device to your account in the LANCOM Management Cloud and enter the serial number and PIN. If you wish, you can alternatively perform a pairing for Cloud-ready devices as well.

If you wish to link an existing device with the LANCOM Management Cloud, you need to conduct the pairing separately, as described below.

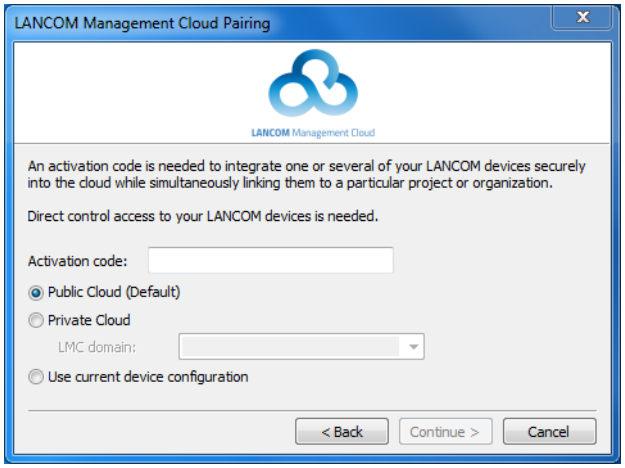
8.2.1 Pairing existing devices via LANconfig

1. In the first step, you need to generate an activation code in the LANCOM Management Cloud.
2. Click on the corresponding LANCOM device with the right-hand mouse button.

3. In the context menu, select the entry **Linking device to LANCOM Management Cloud**.



4. Follow the Wizard's instructions to enter the activation code.
   Three options are available:
   - Public Cloud (default): You use the LANCOM Cloud.
   - Private Cloud: You use your own Cloud.
   - Use the settings currently stored in the device: A public or private cloud is used depending on the existing configuration in the device.



8.2.2 Pairing existing devices via the command line

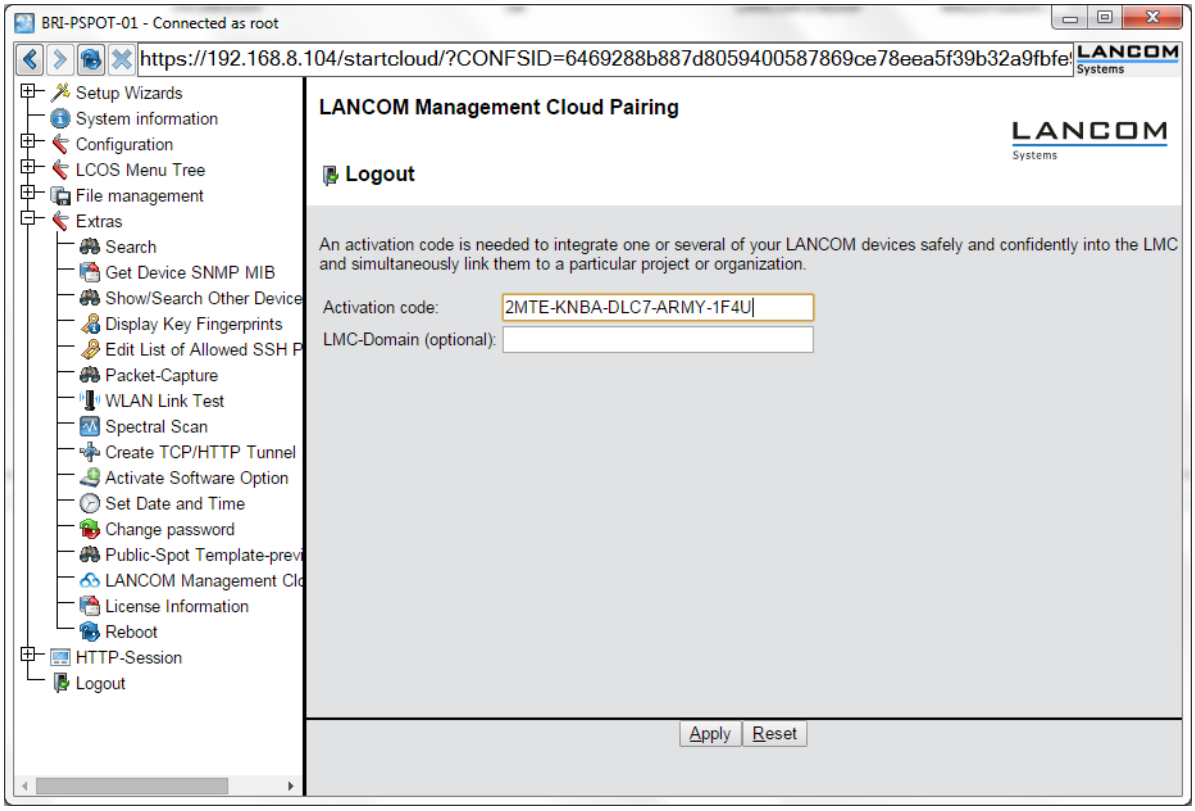
To conduct pairing from the command line, enter the command `startlmc`.

1. Launch a command line utility.
2. Enter the pairing command using the activation code as a parameter, e.g. `startlmc 2MTE-KNBA-DLC7-LPIZ-ARMY-1F4U`.

An on-screen message will inform you if the pairing process has started successfully, or you will see an error message.

8.2.3 Pairing existing devices via WEBconfig

1. Start WEBconfig.
2. Under **Extras** > **LANCOM Management Cloud Pairing** you enter your activation code.



3. Click on the **Send** button.

8.3 Delivery of the LMC domain by the LCOS DHCP server

As of LCOS version 10.0, LCOS devices that automatically receive their IP address from the DHCP server now additionally receive a DHCP option 43 in their DHCP packets.

The DHCP server enriches its DHCP packets with the DHCP option 43 (vendor specific option) to distribute this information to requesting clients on the network. This includes the domain name, which is required for the device to operate with the LANCOM Management Cloud (LMC). In this way, a LANCOM device is able to communicate directly with a private LMC installation without having to be configured first.

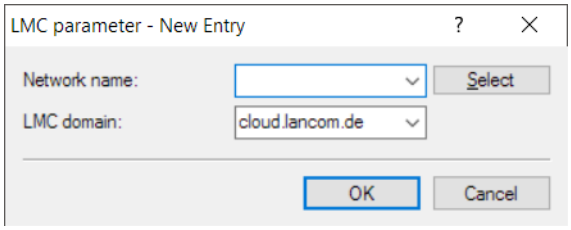
If you operate a LCOS as a DHCP server, you enter the necessary LMC URLs into the configuration in cleartext. The DHCP server in LCOS adds the URLs to the DHCP option 43 and delivers them in the response packets sent to requesting LCOS devices. To do this, the DHCP server evaluates DHCP option 60 (vendor class identifier) in the DHCP requests from the clients. A DHCP option 43 configured in this way takes precedence over a DHCP option 43 that was manually configured in the DHCP options table on the DHCP server.

The vendor class identifier in the request must contain LANCOM. If a device from a different manufacturer sends a request to the LCOS-internal DHCP server, the response packet does not offer DHCP option 43.

8.3.1 Using LANconfig to configure DHCP option 43 to deliver the LMC domain

Configuration

In LANconfig, the LMC domain for the individual networks is configured under **IPv4** > **DHCPv4** > **LMC parameter**.



Network name

Here you specify the network to which the device delivers the LMC domain via DHCP option 43.

LMC domain

Enter the domain name for the LANCOM Management Cloud here.

By default, the domain is set to the public LMC for the first connection. If you wish to manage your device with your own Management Cloud (private cloud or on-premises installation), please enter your LMC domain.

8.3.2 Additions to the Setup menu

LMC options

In this table, you configure the cloud parameters for the LMC (LANCOM Management Cloud).

SNMP ID:

2.10.25

Telnet path:

Setup > **DHCP**

Network name

Here you specify the network to which the device delivers the LMC domain via DHCP option 43.

SNMP ID:

2.10.25.1

Telnet path:

Setup > **DHCP** > **LMC-Options**

Possible values:

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

Default:

empty

LMC domain

Enter the domain name for the LANCOM Management Cloud here.

By default, the domain is set to the public LMC for the first connection. If you wish to manage your device with your own Management Cloud (private cloud or on-premises installation), please enter your LMC domain.

SNMP ID:

2.10.25.6

Telnet path:

Setup > **DHCP** > **LMC-Options**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default:

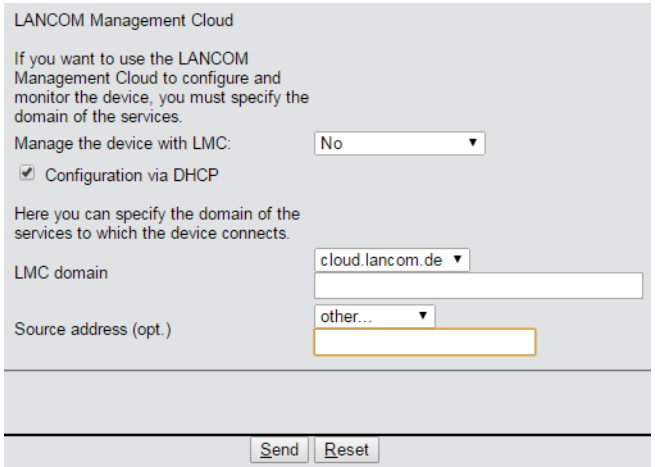
empty

8.4 Manual upfront configuration of your device for management by the LANCOM Management Cloud

You specify:

- Whether your device is to be managed by the LMC.
- Whether the LMC domain is to be retrieved from a DHCP server.
- Which domain your device connects to.
- The source address (optional).

1. Navigate to **Management** > **LMC**.



2. Select one of the three options under **Manage the device with LMC:**
   - **No**: The device does not connect to the LMC.
   - **Yes:** The LMC manages the device. (Default for devices without a WLAN interface)
   - **Only without WLC**: Devices within a network managed by a WLC do not connect to the LANCOM Management Cloud. (Default for devices with a WLAN interface)

3. To obtain the LMC domain from a DHCP server, place a check mark in **Configuration via DHCP**.

   In order for the DHCP server to provide the LMC domain, the DHCP server requires sub-option 18 of the DHCP option 43 to be set to the LMC domain. For more information about the configuration of LMC parameters, see the section *Delivery of the LMC domain by the LCOS DHCP server* on page 58.

4. Under **LMC domain** you set the domain of the LANCOM Management Cloud that the device should connect to.
5. Enter an optional **Source address (opt.)** to be used instead of the one otherwise automatically selected for the source address. If you have configured a loopback address, you can specify it here as the source address.

8.5 Additions to the Status menu

8.5.1 LMC

This menu contains all information about the LANCOM Management Cloud (LMC).

SNMP ID:

1.98

Telnet path:

Status

Transport status

This table contains information about the transport status of the LMC services.

SNMP ID:

1.98.1

Telnet path:

Status > **LMC**

Clear transport status

This action empties the table *1.98.1* ***Transport status***.

SNMP ID:

1.98.2

Telnet path:

Status > **LMC**

Possible arguments:

none

Log table

This table contains information about events for each service. The log entries contain a sequential number, the exact time of the event, and the related service.

SNMP ID:

1.98.3

Telnet path:

Status > **LMC**

Clear log table

This action empties the table *1.98.3* ***Log table***.

SNMP ID:

1.98.4

Telnet path:

Status > **LMC**

Possible arguments:

none

Customer device ID

This entry shows the ID of the device that has connected to the LMC.

SNMP ID:

1.98.5

Telnet path:

Status > **LMC**

Round trip time

This entry shows the response time in milliseconds of the device that has connected to the LMC.

SNMP ID:

1.98.6

Telnet path:

Status > **LMC**

Pairing status

This entry indicates the pairing status between your device and the LANCOM Management Cloud.

SNMP ID:

1.98.7

Telnet path:

Status > **LMC**

Show certificate

This action allows you to view the LMC certificate.

SNMP ID:

1.98.8

Telnet path:

Status > **LMC**

Possible arguments:

none

Control status

The entry indicates whether the connection to the control service of the LMC is ready for use. The control service is responsible, among other things, for changes to the device configuration via the LMC.

SNMP ID:

1.98.9

Telnet path:

Status > **LMC**

Monitor status

The entry indicates whether the connection to the monitoring service of the LMC is ready for use. The monitoring service is responsible, among other things, for the periodic reading-out of monitoring data.

SNMP ID:

1.98.10

Telnet path:

Status > **LMC**

Config log

This table contains information about device configuration changes made via the LMC.

SNMP ID:

1.98.11

Telnet path:

Status > **LMC**

Zero-touch support

This entry indicates whether the device that has connected to the LMC is "Cloud-ready". Cloud-ready devices have a factory pre-configured PSK (pre-shared key) and they can register with the LMC by means of their serial number and PIN.

SNMP ID:

1.98.12

Telnet path:

Status > **LMC**

Pairing token present

This entry indicates whether your device has temporarily cached the pairing token (activation code) for pairing with the LMC. Temporary caching serves various purposes, for example to automatically resume the pairing process after the device is restarted following a crash or power outage. After completing the pairing process, the device deletes the pairing token from its cache.

SNMP ID:

1.98.13

Telnet path:

Status > **LMC**

Possible values:

Yes

Pairing token accepted by the administrator and cached. Pairing continues.

No

No pairing token cached. Pairing is already complete or has not taken place yet.

8.6 Additions to the Setup menu

8.6.1 LMC

In this menu, you configure the cloud parameters for the LMC (LANCOM Management Cloud).

SNMP ID:

2.102

Telnet path:

Setup

Operating

With this entry you enable or disable the ability to manage your LANCOM device with the LMC.

SNMP ID:

2.102.1

Telnet path:

Setup > **LMC**

Possible values:

No

The device does not connect to the LMC.

Yes

LMC is used to manage the device. If not done already, you need to conduct a first-time pairing of the device with the LANCOM Management Cloud. This is the default setting for devices without a WLAN interface.

Please note that without this pairing, it is not possible for the device to communicate with the Management Cloud.

Only without WLC

Devices within a network managed by a WLC do not connect to the LMC. This is the default setting for devices with a WLAN interface.

Delete certificate

Use this action to delete the LMC certificate.

SNMP ID:

2.102.7

Telnet path:

Setup > **LMC**

Possible arguments:

none

DHCP client auto renew

With this parameter you specify the behavior of the device in the event that there is a change to the DHCP settings in the network and the LMC client is unable to connect to the LMC.

If the LMC client is unable to reach its configured LMC, it is likely that the IP address range of the network has changed. A device that is configured as a DHCP client retains the IP address that was previously allocated to it until the DHCP lease time expires. By enabling this parameter, the device requests a new DHCP address (DHCP-Renew) regardless of the remaining DHCP lease time.

SNMP ID:

2.102.8

Telnet path:

Setup > **LMC**

Possible values:

No

If the LMC client loses its connection to the LMC, no DHCP-Renew is triggered.

Yes

If the LMC client loses its connection to the LMC, a DHCP-Renew is triggered. If the DHCP-Renew is not successful, the DHCP process is restarted. The device then tries to get an IP address from any DHCP server in order to reconnect to the LMC.

Default:

Yes

Loopback address

Use this entry to set a loopback address for the LANCOM Management Cloud.

SNMP ID:

2.102.12

Telnet path:

Setup > **LMC**

Possible values:

Max. 16 characters from `[0-9].`

Default:

empty

Configuration via DHCP

This entry enables or disables the reception of information via DHCP option 43, which is required to connect to the LMC.

SNMP ID:

2.102.13

Telnet path:

Setup > **LMC**

Possible values:

No
Yes

Default:

Yes

DHCP status

This menu contains the status values relating to the LMC domain that the device obtained via DHCP option 43.

SNMP ID:

2.102.14

Telnet path:

Setup > **LMC**

DHCP LMC domain

This entry shows the LMC domain obtained by the device via DHCP option 43.

SNMP ID:

2.102.14.5

Telnet path:

Setup > **LMC**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

cloud.lancom.de

LMC domain

Enter the domain name for the LANCOM Management Cloud here.

If you wish to manage your device with your own Management Cloud (private cloud or on-premises installation), please enter your LMC domain.

SNMP ID:

2.102.15

Telnet path:

Setup > **LMC**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` `

Default:

cloud.lancom.de

9 Diagnosis

9.1 Layer-7 application detection

As of LCOS version 10.0, layer-7 application detection allows you to identify bandwidth-intensive services on your network.

When a client establishes a connection over a tracked interface, layer-7 application detection begins analyzing and recording the traffic volumes.

The results of the recording and the usage statistics depend on the configuration that was specified for this connection.

Layer-7 application detection monitors the destination port of an application. If a connection Is detected arriving at port 80 or 443 (HTTP or HTTPS), the connection establishment is further analyzed. If a different destination port is used, the application is identified according to the applications entered into the "Port-based tracking" list.

If the establishment of an HTTP/HTTPS connection is detected, this connection is subjected to deeper analysis. For HTTP connections, the application detection additionally extracts the destination host from the destination URL in the HTTP GET request.

The only part to be used is the host; additional parts of the URL are truncated

If an HTTPS connection is detected, the layer-7 application detection attempts to identify the destination host in the following sequence:

- Server name indication from the TLS "Client Hello"
- Common name from the transmitted TLS server certificate
- Reverse DNS request to the server IP address

For HTTP and HTTPS connections, the destination host name found is compared with the "HTTP/HTTPS tracking" list. This list contains the most widely used Web services/applications, including the components of their host names.

If neither the service nor the connection appear in the list, i.e. the application cannot be identified, then it is classified as a general HTTP or HTTPS service on the port.

Allocation in this way requires the "Port-based tracking" list to include the entries HTTP and HTTPS.

If the destination service is known for every connection on a tracked interface, the combination with the connecting client makes is possible to track the connection and to determine which client caused what amount of traffic to / from a service.

The values found are available from the corresponding tables in the LCOS menu tree under **Status** > **Layer-7-App-Detection**.

Layer-7 application detection can be operated either centrally or decentrally on your network. Both options prevent traffic being listed multiple times:

Central

Layer-7 application detection is enabled on a central router in the LAN, and it is disabled on all other LANCOM devices.

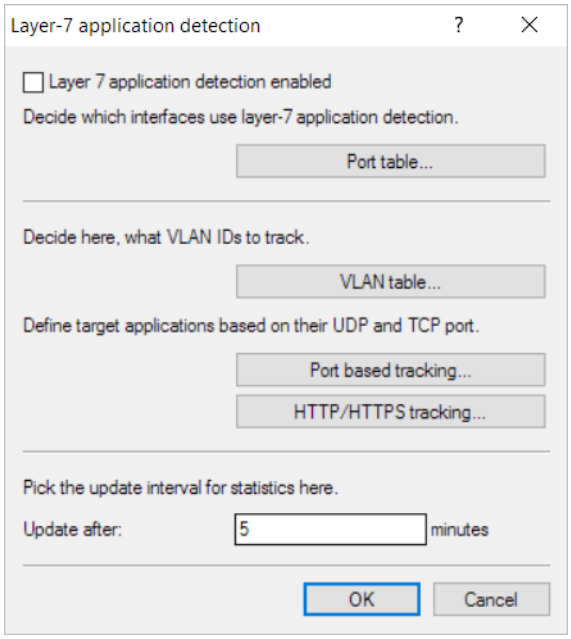
Decentral

Layer-7 application detection is enabled only on the final bridges in the LAN, e.g. on access points or LANCOM routers with the clients connected directly to their LAN interfaces.

To avoid distorted results, the traffic should pass through just one single device or bridge running the layer-7 application detection.

9.1.1 Configuring layer-7 application detection with LANconfig

In LANconfig, you enable and configure layer-7 application detection under **Firewall/QoS** > **General** > **Layer-7 application detection**.



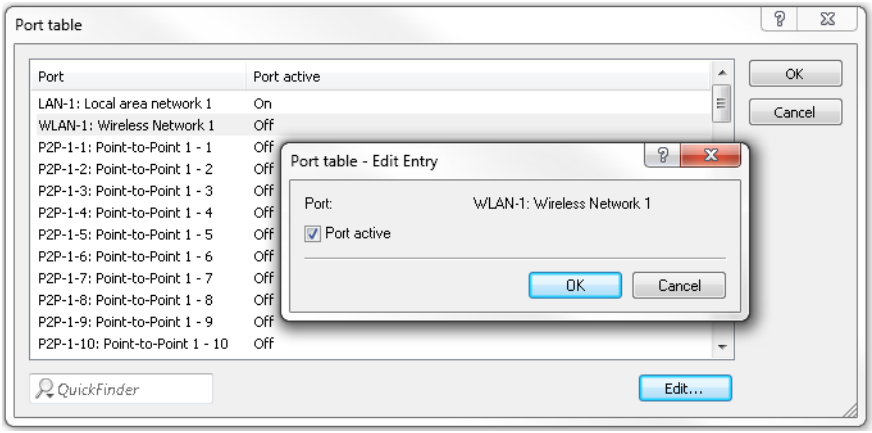
Use this dialog to specify the following parameters:

Layer-7 application detection enabled

This entry is used to enable or disable layer-7 application detection.

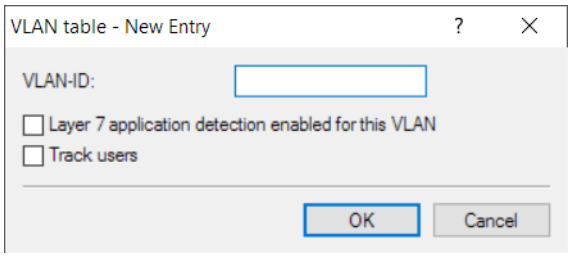
Port table

Here you specify the ports that are to be tracked by layer-7 application detection. Enable or disable the available ports correspondingly.



VLAN table

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

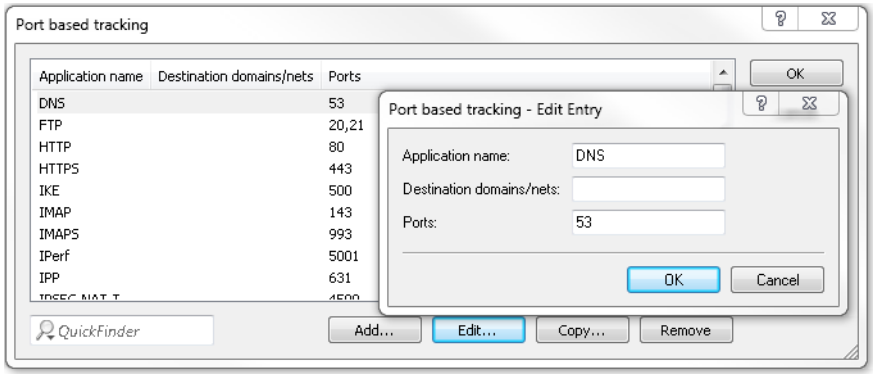


- **Layer-7 application detection enabled for this VLAN**: The device tracks general and application-specific data.
- **Track users:** The device tracks user-specific data (user or client name and MAC address) in the specified VLAN.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

Port-based tracking

Here you select the applications to be tracked. Optionally you can chose default applications or you can specify your own applications. You also specify the destination domains or the destination networks of the application. Extend the list according to your needs.

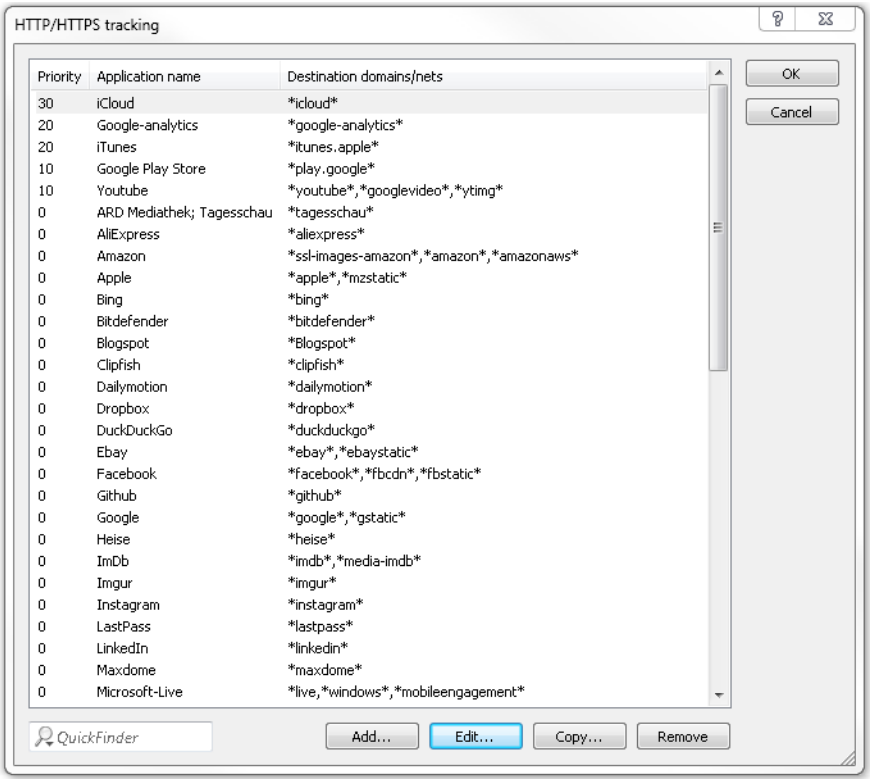


You can specify several destination domains, destination networks or ports by using a comma-separated list in CIDR notation (classless inter-domain routing). You have the option of using IPv4 or IPv6 destination networks.

HTTP/HTTPS tracking

Use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

Use wildcards ("*" for multiple characters or "?" for exactly one character) to define the parts of the host name.



Priority	Application name	Destination domains/nets
30	iCloud	*icloud*
20	Google-analytics	*google-analytics*
20	iTunes	*itunes.apple*
10	Google Play Store	*play.google*
10	Youtube	*youtube*,*googlevideo*,*ytimg*
0	ARD Mediathek; Tagesschau	*tagesschau*
0	AliExpress	*aliexpress*
0	Amazon	*ssl-images-amazon*,*amazon*,*amazonaws*
0	Apple	*apple*,*mzstatic*
0	Bing	*bing*
0	Bitdefender	*bitdefender*
0	Blogspot	*Blogspot*
0	Clipfish	*clipfish*
0	Dailymotion	*dailymotion*
0	Dropbox	*dropbox*
0	DuckDuckGo	*duckduckgo*
0	Ebay	*ebay*,*ebaystatic*
0	Facebook	*facebook*,*fbcdn*,*fbstatic*
0	Github	*github*
0	Google	*google*,*gstatic*
0	Heise	*heise*
0	ImDb	*imdb*,*media-imdb*
0	Imgur	*imgur*
0	Instagram	*instagram*
0	LastPass	*lastpass*
0	LinkedIn	*linkedin*
0	Maxdome	*maxdome*
0	Microsoft-Live	*live,*windows*,*mobileengagement*

Multiple host-name parts can be specified in a comma-separated list.

By specifying the priority you have the additional option of setting the order in which services are evaluated if certain host-name parts appear in multiple entries (e.g. *google).

Update after

Specify an interval in minutes for updating the usage statistics.

9.1.2 Additions to the Setup menu

Layer-7 app detection

This menu is used to configure layer-7 application detection.

SNMP ID:

2.101

Telnet path:

Setup

Operating

This entry is used to enable or disable layer-7 application detection.

SNMP ID:

2.101.1

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

No
Yes

Default:

No

IP port applications

Set the target ports for the layer-7 application detection, or add new entries to the table.

SNMP ID:

2.101.2

Telnet path:

Setup > **Layer-7-App-Detection**

Application name

Specify a unique name for this application.

SNMP ID:

2.101.2.1

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

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

Default:

empty

Targets

Define targets for this application.

Specify multiple targets with a comma-separated list.

SNMP ID:

2.101.2.2

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

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

Default:

empty

Ports

Specify the ports to be tracked.

SNMP ID:

2.101.2.3

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

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

Default:

empty

Port table

Here you activate or deactivate the ports to be tracked by layer-7 application detection.

The contents of the table are device dependent.

SNMP ID:

2.101.4

Telnet path:

Setup > **Layer-7-App-Detection**

Port

This entry contains the name of the port selected from the table.

SNMP ID:

2.101.4.2

Telnet path:

Setup > **Layer-7-App-Detection** > **Port-Table**

Traffic tracking

This entry is used to enable or disable the tracking of traffic for this port.

SNMP ID:

2.101.4.3

Telnet path:

Setup > **Layer-7-App-Detection** > **Port-Table**

Possible values:

No
Yes

Default:

No

Status-Update-In-Minute

This entry sets an interval in minutes when the usage statistics are updated.

SNMP ID:

2.101.5

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

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

Default:

60

Max queue length

This entry specifies the maximum queue length for the usage statistics.

SNMP ID:

2.101.6

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

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

Default:

10000

Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

SNMP ID:

2.101.7

Telnet path:

Setup > **Layer-7-App-Detection**

HTTP-HTTPS tracking

In this menu, specify the entries for the tracking of HTTP / HTTPS connections.

SNMP ID:

2.101.8

Telnet path:

Setup > **Layer-7-App-Detection**

Application name

Name for the tracking of HTTP / HTTPS connections (e.g. youtube).

SNMP ID:

2.101.8.1

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

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

Default:

empty

Targets

Here you specify the targets for the tracking of HTTP / HTTPS connections (e.g. youtube).

Specify multiple targets in a comma-separated list (e.g. youtube, googlevideo, ytimg)

SNMP ID:

2.101.8.2

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

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

Default:

empty

Prio

Set the priority of HTTP/HTTPS tracking by the layer-7 application detection.

SNMP ID:

2.101.8.3

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

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

Default:

0

VLAN

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

SNMP ID:

2.101.11

Telnet path:

Setup > **Layer-7-App-Detection**

VLAN-ID

Use this entry to specify a VLAN ID.

SNMP ID:

2.101.11.1

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

0 … 65535

Default:

0

Track user

With this entry you enable or disable the collection of user-specific data (user or client name and MAC address).

SNMP ID:

2.101.11.2

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

Tracking active

This entry is used to enable or disable the collection of general or application-specific data.

SNMP ID:

2.101.11.3

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

Save-In-Min

Specify the interval in minutes for storing the usage statistics of the layer-7 application detection.

SNMP ID:

2.101.12

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

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

Default:

3600

9.1.3 Additions to the Status menu

Layer-7 app detection

This menu gives you information about the applications being tracked by the layer-7 application detection.

SNMP ID:

1.95

Telnet path:

Status

Applications

This table displays how much traffic each client generated to/from a service. The content of this table is regularly saved boot-persistent.

The table shows the name of the user or client in as far as this can be detected. The first attempt is to set the "User name" to the 802.1X user name. If 802.1X is not used, the client host name identified using DHCP snooping will be shown.

In addition, the column "PSpot-Users" shows the user name of the logged-on Public Spot users.

Public Spot user names are only displayed if the Public Spot module is active on the same device as that running the layer-7 application detection.

SNMP ID:

1.95.1

Telnet path:

Status > **Layer-7-App-Detection**

Total traffic per application

This table displays the traffic as grouped by application.

SNMP ID:

1.95.2

Telnet path:

Status > **Layer-7-App-Detection**

Total traffic per user

This table displays the traffic as grouped by user.

The table shows the name of the user or client in as far as this can be detected. The first attempt is to set the "User name" to the 802.1X user name. If 802.1X is not used, the client host name identified using DHCP snooping will be shown.

In addition, the column "PSpot-Users" shows the user name of the logged-on Public Spot users.

Public Spot user names are only displayed if the Public Spot module is active on the same device as that running the layer-7 application detection.

SNMP ID:

1.95.3

Telnet path:

Status > **Layer-7-App-Detection**

HTTP-HTTPS hit list

This table displays the hits for the HTTP/HTTPS connection tracking.

SNMP ID:

1.95.4

Telnet path:

Status > **Layer-7-App-Detection**

Operating

This entry indicates whether the layer-7 application detection is enabled or disabled.

SNMP ID:

1.95.5

Telnet path:

Status > **Layer-7-App-Detection**

Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

SNMP ID:

1.95.6

Telnet path:

Status > **Layer-7-App-Detection**