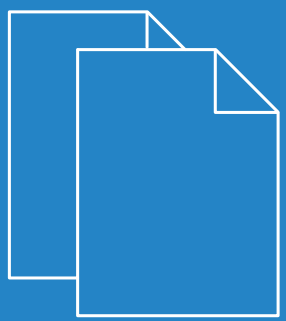
SECURE. NETWORKS.

LCOS 9.24

Addendum



LANCOM Systems

Contents

1 Addendum to LCOS version 9.24

This document describes the changes and enhancements in LCOS version 9.24 since the previous version.

2 Routing and WAN connections

2.1 Manually configuring VDSL/ADSL bandwidth

As of LCOS version 9.24, the bandwidth for devices with an integrated ADSL/VDSL modem can be set manually at the interface.

2.1.1 Configuring bandwidth with LANconfig

To configure the upstream and downstream transmission speeds in LANconfig, navigate to **Interfaces** > **WAN** and click the **Interface settings** button.

VDSL and ADSL interfaces

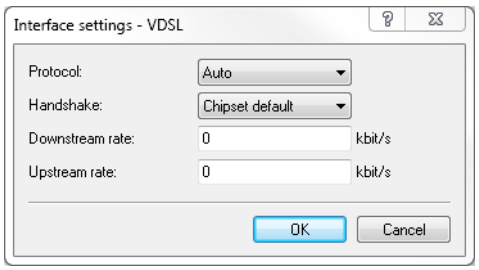
In order for Quality of Service to function properly, you need to know the actual bandwidth of the WAN connection. Sometimes, the bandwidth negotiated by the DSL modem may not agree with the actual data transfer rate. In this case, it is necessary to manually correct the speed of DSL connection to the actual value.

This only applies to devices with an integrated ADSL/VDSL modem.

Example:

The bandwidth negotiated during the DSL synchronization is 100 Mbps. In fact, the actual available bandwidth is a transmission speed of just 50 Mbps.

Settings for devices with an integrated VDSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode

VDSL2 (G.993.2)

Operating mode VDSL2 for transmission rates of up to 100 Mbps upstream and downstream.

ADSL

Operating mode ADSL with up to 8 Mbps downstream and 0.6 Mbps upstream

ADSL2+ (G.992.5)

Operating mode ADSL2+ with up to 24 Mbps downstream and 1 Mbps upstream

ADSL2 (G.992.3)

Operating mode ADSL2 with up to 12 Mbps downstream and 1.2 Mbps upstream

ADSL1 (G.992.1/G.DMT)

Operating mode ADSL (G.DMT) with up to 8 Mbps downstream and 1 Mbps upstream

ADSL2+ (Annex J)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.5 Mbps upstream

ADSL2 (Annex J)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.5 Mbps upstream

Off

The interface is not active.

Handshake

Select from the following handshake methods for this interface:

Chipset-default

The handshake is carried out according to the default for the chipset in the device.

V43 if needed

The V43 carrier set is used for the handshake if required.

V43 enabled

The carrier set V43 is enabled for the handshake.

V43 disabled

The carrier set V43 is disabled for the handshake.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

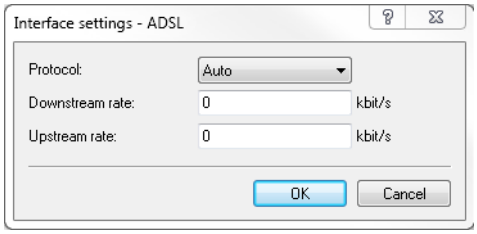
If the default value is "0", the value used is negotiated automatically.

Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

Settings for devices with an integrated ADSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode

ADSL1 (autom. Annex A/B)

Operating mode ADSL over POTS/ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (autom. Annex A/B)

Operating mode ADSL2 over POTS/ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (autom. Annex A/B)

Operating mode ADSL2+ over POTS/ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

Auto-POTS (autom. Annex A/I/L/M)

Operating mode ADSL over POTS for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex A)

Operating mode ADSL over POTS for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex A)

Operating mode ADSL2 over POTS with up to 12 Mbps downstream and 1 Mbps upstream

ADSL2+ (Annex A)

Operating mode ADSL2+ over POTS with up to 24 Mbps downstream and 1 Mbps upstream

ADSL2 (Annex I)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.2 Mbps upstream

ADSL2+ (Annex I)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.2 Mbps upstream

ADSL2 (Annex L)

Operating mode RE-ADSL2 with up to 6 Mbps downstream and 1.2 Mbps upstream

ADSL2 (Annex M)

Operating mode ADSL2 with up to 24 Mbps downstream and 3.5 Mbps upstream

ADSL2+ (Annex M)

Operating mode ADSL2+ with up to 24 Mbps downstream and 3.7 Mbps upstream

Auto-ISDN (autom. Annex B/J)

Operating mode ADSL over ISDN for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 3.5 Mbps upstream.

ADSL2+ (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 3.5 Mbps upstream.

Off

The interface is not active.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

2.1.2 Additions to the Setup menu

Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

SNMP ID:

2.23.6.16

Telnet path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

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

Default:

0

Special values:

0

The value used is negotiated automatically.

Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

SNMP ID:

2.23.6.18

Telnet path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

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

Default:

0

Special values:

0

The value used is negotiated automatically.

Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

SNMP ID:

2.23.8.16

Telnet path:

Setup > **Interfaces** > **VDSL**

Possible values:

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

Default:

0

Special values:

0

The value used is negotiated automatically.

Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

SNMP ID:

2.23.8.18

Telnet path:

Setup > **Interfaces** > **VDSL**

Possible values:

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

Default:

0

Special values:

0

The value used is negotiated automatically.

3 WLAN

3.1 Support for AiRISTA Flow Blink Mode (former Ekahau Blink Mode)

As of LCOS version 9.24, devices with at least one 11n Wi-Fi module support the AiRISTA Flow Blink Mode.

3.1.1 AiRISTA Flow Blink Mode

Ekahau and their "Real Time Location System" (RTLS) allow you to determine the location of objects and persons within a wireless LAN. This works with special Wi-Fi transmitters known as "Wi-Fi tags" that are located on the device or person's body and which send specially coded Wi-Fi packets. APs located nearby receive these packets, enrich them with additional information (e.g. RSSI), encapsulate them in the "TaZmen Sniffer Protocol" (TZSP) and forward this information to the "Ekahau RTLS Controller" (ERC) installed on the network. The ERC analyzes this data to determine the position of the Wi-Fi tag.

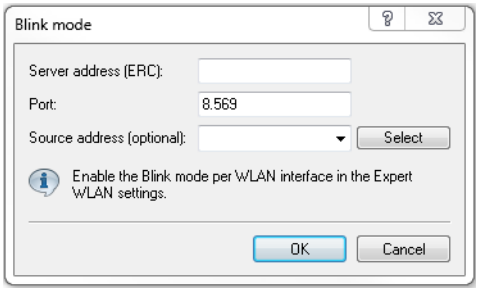
The Wi-Fi tags support three modes for sending the Wi-Fi packets:

- **Associated mode**: In "associated mode" the Wi-Fi tag functions like a Wi-Fi client. It associates with a nearby AP and stays in constant contact with it. While this provides seamless positioning, this mode consumes more power and the battery life of the Wi-Fi tag is reduced. In "associated mode" the Wi-Fi tags use the Ekahau Location Protocol (ELP).
- **Blink mode**: In "blink mode", the Wi-Fi tag transmits short Wi-Fi packets but does not connect to an AP. In "blink mode" the Wi-Fi tags use the "Ekahau Blink Protocol" (EBP).
- **Mixed mode**: In "Mixed mode", the Wi-Fi tags use EBP to send the RSSI and ELP to send status messages to the ERC.

Configuring the AiRISTA Flow Blink Mode with LANconfig

The blink mode only works with 802.11n WLAN modules, not with 802.11ac WLAN modules. Correspondingly, it is not possible to activate the 'blink mode' for 802.11ac WLAN modules in LANconfig. The option is permanently disabled for devices of this type.

To configure access to the RTLS Server (ERC) with LANconfig, open the view **Wireless LAN** > **General** and click the button **Blink mode**.



Server address (ERC)

Enter the address of the ERC. You can enter an IP address or a host name.

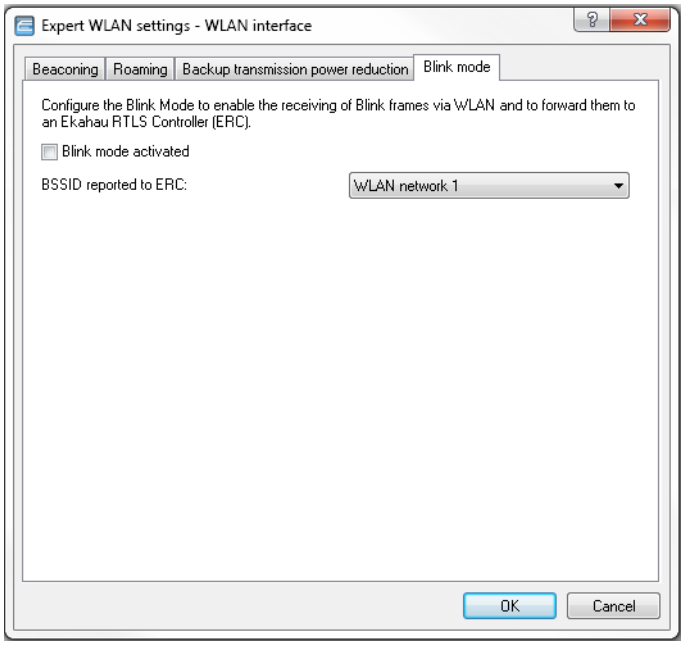
Port

Contains the default UDP port (8569) for communication with the ERC. Change this value only in exceptional cases.

Source address (optional)

Optionally, specify a source address.

To configure the blink mode for each physical WLAN interface, navigate to **Wireless LAN** > **General** and click the button **Expert WLAN settings**. If applicable, select the desired WLAN interface from the drop-down list and switch to the **Blink mode** tab.



Blink mode activated

Enable or disable the blink mode for this interface here.

BSSID reported to ERC

Here you select the logical WLAN interface that the device reports to the ERC.

The ERC "maps" this BSSID to a particular location. For example, if this location were a server room, the ERC knows that Wi-Fi tag "A" is located in the server room as long as the "blink" arrives from the BSSID belonging to the corresponding APs.

3.1.2 Additions to the Setup menu

Blink mode

This menu contains the settings for communications with the RTLS server (Ekahau RTLS Controller, ERC).

SNMP ID:

2.12.131

Telnet path:

Setup > **WLAN**

Server address

Contains the IP address or the DNS name of the RTLS server.

SNMP ID:

2.12.131.1

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

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

Default:

empty

Server port

Contains the UDP port number of the RTLS server.

SNMP ID:

2.12.131.2

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

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

Default:

8569

Loopback address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

SNMP ID:

2.12.131.3

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

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

Special values:

Name of the IP networks whose address should be used
"INT"
for the address of the first intranet
"DMZ"
for the address of the first DMZ
LB0 to LBF
for the 16 loopback addresses
Any valid IP address

Default:

empty

Blink mode

In this table, you configure the blink mode for the physical WLAN interfaces.

SNMP ID:

2.23.20.26

Telnet path:

Setup > **Interfaces**

Ifc

Contains the name of the physical WLAN interface.

SNMP ID:

2.23.20.26.1

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

WLAN-1
WLAN-2

Operating

Activates or deactivates the blink mode for this physical interface.

SNMP ID:

2.23.20.26.2

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

Yes
No

Default:

No

Network

Here you select the logical WLAN interface that the device reports to the ERC.

SNMP ID:

2.23.20.26.3

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

List of the available logical WLAN interfaces 'WLAN-1' to 'WLAN-x'

3.1.3 Additions to the Status menu

Packet transport

This entry contains the packet transport status values.

SNMP ID:

1.3.53

Telnet path:

Status > **WLAN**

4 Public Spot

4.1 Additional memory locations for your own Public Spot template images

As of LCOS version 9.24, additional memory locations are available for your own Public Spot template images.

4.1.1 Embedding graphics in user-created template pages

Images for your vouchers can now be uploaded into the device because a further five images slots (voucher image 1 to voucher image 5) are now available for your pages. These images are permanently stored in the flash memory of the device.

How to transfer the images into the device is described in the section *Custom header images for variable screen widths*. When uploading, set the **Certificate type** to "Public Spot - voucher image 1" to "Public Spot - voucher image 5".

Modify the HTML template of the relevant voucher (e.g. with a text editor such as Notepad++) and reference the uploaded images by including the following in the template: `<img src="/images/voucherimg1">` to `<img src="/images/voucherimg5">`. How to set up a custom template page is described in the section *Setting up a customized template page*.

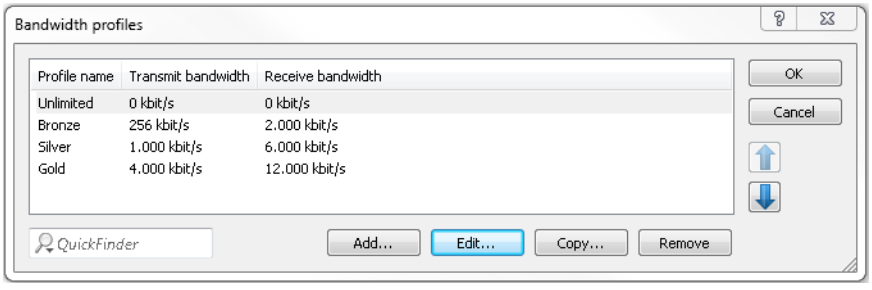
4.2 Predefined bandwidth profiles

As of LCOS version 9.24 you have the option of using predefined bandwidth profiles in the wizard **Create Public Spot account**.

Using the window **Public-Spot** > **Wizard** > **Bandwidth profiles**, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. You can select a predefined profile or create your own bandwidth profiles that meet your needs. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Create Public Spot account** in WEBconfig.

Integrating predefined bandwidth profiles

From the four predefined profiles, select the bandwidth profile that closest meets your requirements:



Unlimited

No restriction in the transmit and receive bandwidth.

These values refer to the transmit bandwidth (TX) and receive bandwidth (RX) from the perspective of the client.

Bronze

The transmit (TX) bandwidth is 256 kbps, the receive (RX) bandwidth is 2 Mbps.

Silver

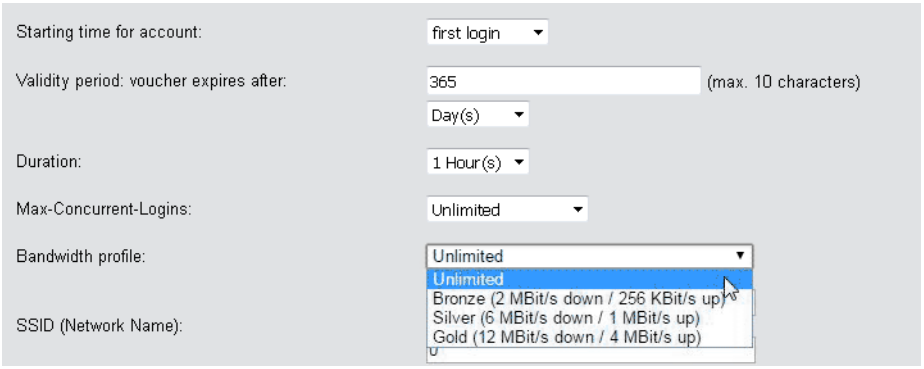
The transmit (TX) bandwidth is 1 Mbps, the receive (RX) bandwidth is 6 Mbps.

Gold

The transmit (TX) bandwidth is 4 Mbps, the receive (RX) bandwidth is 12 Mbps.

You have the option of customizing the predefined entries to meet your requirements. Select the profile for editing and click the button **Edit**. Alternatively, you can create your own profiles.

The selection dialog in WEBconfig has changed as follows:

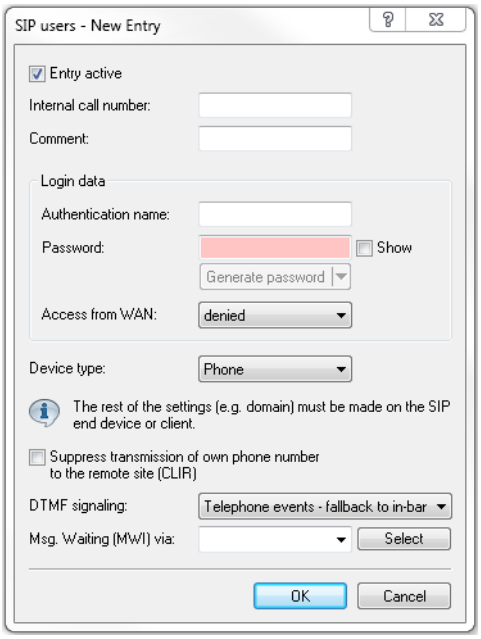


5 Voice over IP – VoIP

5.1 Message Waiting Indication

As of LCOS version 9.24, you can optionally enable the signaling of new messages on SIP phones.

The LANconfig dialog under **Voice Call Manager** > **Users** > **SIP users** has been modified as follows:



Msg. Waiting (MWI) via

The presence of voice messages left on your provider's online mailbox are signaled by notifications on the device. Signaling occurs in different ways depending on the terminal type. Select the line for which this function should be enabled from the list of configured SIP lines under **Voice Call Manager** > **Users** > **SIP users**.

Notification only occurs if the provider supports this function.

5.1.1 Additions to the Setup menu

MWI target line

Voice and messages left on your provider mailbox are signaled by notifications on the device. For the configured SIP users, select the line that is to be enabled for this function.

Notification only occurs if the provider supports this function.

SNMP ID:

2.33.3.1.1.21

Telnet path:

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

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]"{|}%<>[]`

Default:

empty

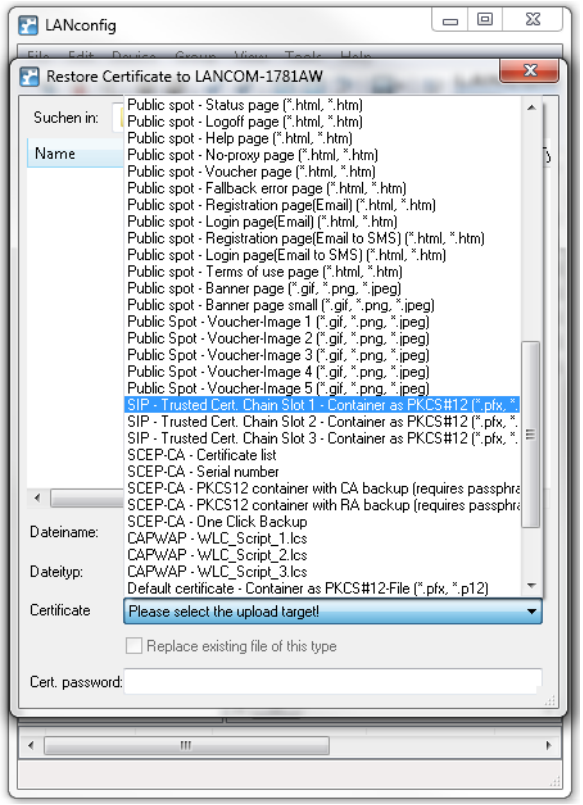
5.2 Certificate upload for encrypted telephony

As of LCOS version 9.24, you have the option to upload certificates for encrypted telephony onto your device and to check the existing certificate.

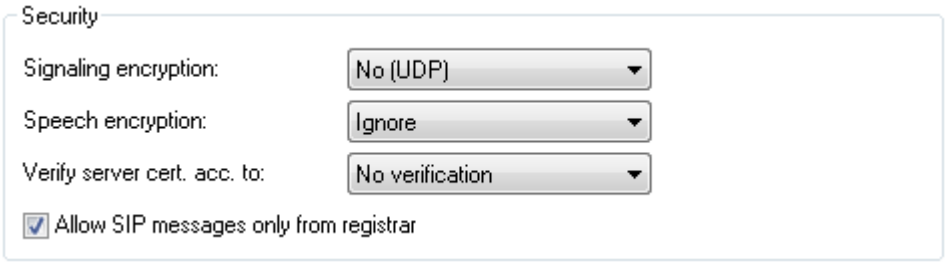
5.2.1 Certificate for encrypted telephony

You have the option to upload certificates for encrypted telephony onto your device and to check whether the existing certificate used by the SIP server to establish a TLS connection should be classified as trustworthy and accepted.

Upload the required certificate to your device with LANconfig by navigating to **Device, Configuration management** > **Upload certificate or file** .



In LANconfig under **Voice Call Manager** > **Lines** > **SIP lines** select in section "Security", whereupon the SIP certificate should be checked:



Verify server cert. acc. to:

With this setting, you specify whether the certificate of the SIP server is verified against certain Certificate Authorities (CAs). The CA certificates from globally known certificate chains are updated with LCOS updates.

Server certificate	
No verification	The server certificate is not verified. All valid server certificates are accepted, whichever CA they were signed by. This setting is useful for accepting self-signed certificates.
All trusted CAs	The server certificate is verified against all CAs known to the LANCOM. These include all CAs that LCOS "knows" to be trusted and also those from the SIP certificate slots 1 to 3. The encrypted connection is only established if one of these certificates is validated successfully.
SIP cert. slot 1	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 1 of the VoIP certificates.
SIP cert. slot 2	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 2 of the VoIP certificates.
SIP cert. slot 3	A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 3 of the VoIP certificates.
Telekom-Shared-Business-CA4	With this setting, the device only accepts server certificates signed by the Telekom Shared Business CA4 CA. Use this setting for SIP trunk connections from Deutsche Telekom AG.

5.2.2 Additions to the Setup menu

Verify server certificate

With this setting you specify whether the certificate produced by the SIP server when establishing the TLS connection is to be classified as trustworthy and accepted.

SNMP ID:

2.33.1.1.32

Telnet path:

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

Possible values:

No verification

The server certificate is not verified. All valid server certificates are accepted, whichever CA they were signed by. This setting is useful for accepting self-signed certificates.

Accept trusted

The server certificate is verified against all CAs known to the LANCOM. These include all CAs that LCOS "knows" to be trusted and also those from the SIP certificate slots 1 to 3.

The encrypted connection is only established if one of these certificates is validated successfully.

SIP-Trusted-CA-Slot-1

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 1 of the SIP certificates.

SIP-Trusted-CA-Slot-2

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 2 of the SIP certificates.

SIP-Trusted-CA-Slot-3

A check is made to see whether the server certificate was signed by the CA whose certificate was uploaded to slot 3 of the SIP certificates.

Telekom-Shared-Business-CA4

With this setting, the device only accepts server certificates signed by the Telekom Shared Business CA4 CA.

Use this setting for SIP trunk connections from Deutsche Telekom AG.

Default:

No verification

5.3 Auto provisioning LANCOM DECT 510 IP

The base station LANCOM DECT 510 IP is the ideal solution for integrating Gigaset DECT handsets at small and medium-sized enterprises.

LCOS version 9.24 facilitates the automatic installation and configuration of the base station with up to 6 DECT handsets. When connected to a LANCOM router, the LANCOM DECT 510 IP makes it easy to register the handsets and to assign the individual phone numbers.

The LANCOM DECT 510 IP base station can be configured via WEBconfig. This is not strictly required. If provisioning is enabled (**Setup** > **Provisioning-Server** > **Operating** set to "Yes"), your LANCOM router configures the base station automatically.

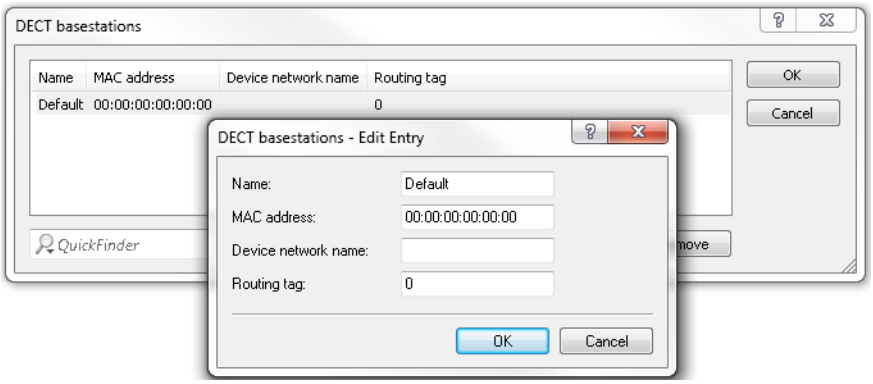
Requirements for the automatic configuration of the LANCOM DECT 510 IP are that the base station is connected to your LANCOM router and the handsets are registered with the station.

You also have the option to configure the base station by means of the All-IP Wizard. Simply follow the instructions provided by the Wizard.

5.3.1 Configuring DECT base stations and handsets with LANconfig

To configure the DECT base station in LANconfig, go to **Voice Call Manager** > **Users** > **DECT base stations** and add a new entry to the table.

If every LANCOM DECT 510 IP connected to the network should be configured in the same way by auto provisioning, no additional entries are required in this table. The default entry takes care of everything.



Name

Specify a unique name for this base station here.

MAC address

Enter the MAC address of the base station.

If you wish to permit communications with any MAC address, enter `00:00:00:00:00:00` (default).

Network name

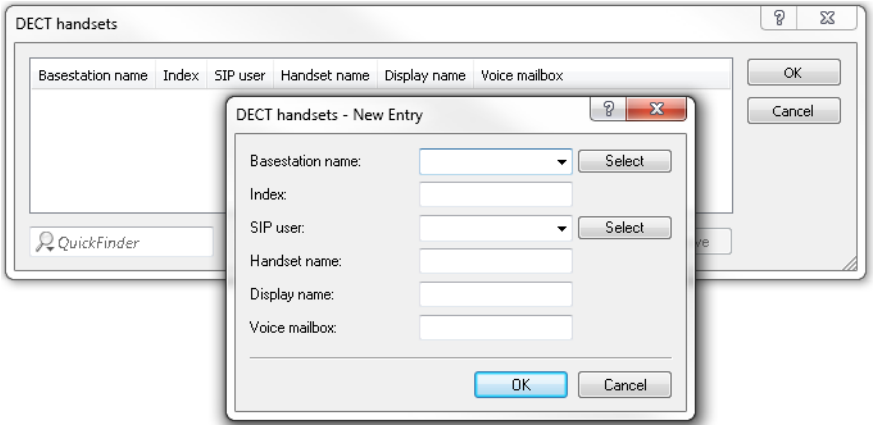
Here you optionally specify a network name that is displayed with the base station in the network.

Routing tag

The interface tag allows you to restrict the auto-provisioning of LANCOM DECT base stations to a specific network. This is particularly useful if your network contains IP addresses that are open to the public (e.g. via a Public Spot or DMZ). This restriction prevents SIP access credentials for the DECT base station from being unintentionally transmitted to third-party devices.

If you wish to use this service for all networks, enter the routing tag "0" here.

To configure the DECT handsets in LANconfig, go to **Voice Call Manager** > **Users** > **DECT handsets** and add a new entry to the table.



Base station name

Here you select the base station where the corresponding handset is registered.

Index

Enter here the number of the corresponding handset (e.g. "0" for handset 1, "1" for handset 2, etc.).

SIP user

Select the phone number of the handset here.

Handset name

Here you set the name to be shown in the display of the handset.

Display name

Here you set the name to be sent to a caller.

Voice mailbox

Enter the phone number of your voice mailbox here. This phone number is dialed by pressing and holding the button "1" on the handset.

Additions to the Setup menu

DECT

This menu contains the configuration options for DECT base stations and DECT handsets.

SNMP ID:

2.33.10

Telnet path:

Setup > **Voice-Call-Manager**

Base stations

This entry is used to configure your DECT base stations.

SNMP ID:

2.33.10.1

Telnet path:

Setup > **Voice-Call-Manager** > **DECT**

Name

Specify a unique name for this base station here.

SNMP ID:

2.33.10.1.1

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Max. 15 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

MAC address

Enter the MAC address of the base station.

If you wish to permit communications with any MAC address, enter `00:00:00:00:00:00`.

SNMP ID:

2.33.10.1.2

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

Max. 17 characters from `[A-F][a-f][0-9]`

Default:

ffffffffffff

Network name

Here you optionally specify a network name that is displayed with the base station in the network.

SNMP ID:

2.33.10.1.3

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

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

Default:

empty

Routing tag

This entry shows the routing tag used.

SNMP ID:

2.33.10.1.4

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Basestations**

Possible values:

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

Default:

0

Handsets

This entry is used to configure your DECT handsets.

SNMP ID:

2.33.10.2

Telnet path:

Setup > **Voice-Call-Manager** > **DECT**

Base station name

Here you select the base station where the corresponding handset is registered.

SNMP ID:

2.33.10.2.1

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 15 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

DEFAULT

Index

Enter here the number of the corresponding handset (e.g. "0" for handset 1, "1" for handset 2).

SNMP ID:

2.33.10.2.2

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

0 … 6

Default:

0

SIP user

Select the phone number of the handset here.

SNMP ID:

2.33.10.2.3

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 20 characters from `[0-9]+-`

Default:

empty

Handset name

Here you set the name to be shown in the display of the handset.

SNMP ID:

2.33.10.2.4

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 10 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Display name

Here you set the name to be sent to a caller.

SNMP ID:

2.33.10.2.5

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

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

Default:

empty

Voice mailbox

Enter the phone number of your voice mailbox here. This phone number is dialed by pressing and holding the button "1" on the handset.

SNMP ID:

2.33.10.2.6

Telnet path:

Setup > **Voice-Call-Manager** > **DECT** > **Handsets**

Possible values:

Max. 20 characters from `[0-9]+-`

Default:

empty

6 RADIUS

6.1 Dynamic authorization by RADIUS CoA (Change of Authorization)

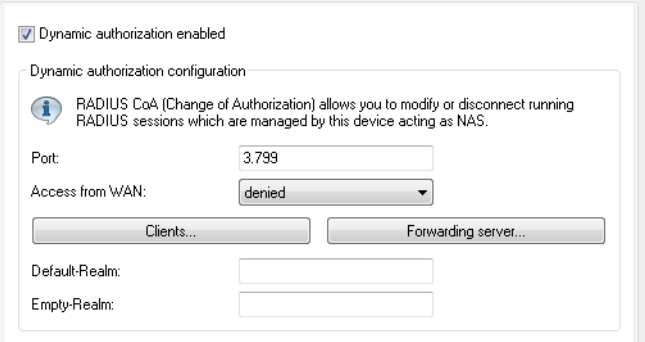
As of LCOS version 9.24, it is possible to use CoA messages to modify current RADIUS sessions.

If you operate an external hotspot server, it is possible to change the attributes of Public Spot sessions after the user has authenticated. This is achieved with dynamic authorization by means of RADIUS CoA (Change of Authorization). See also the section "Dynamic authorization by RADIUS CoA (Change of Authorization)" in the RADIUS chapter.

In LCOS version 9.24, this function is implemented for the Public Spot only.

6.1.1 Configuring dynamic authorization with LANconfig

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.

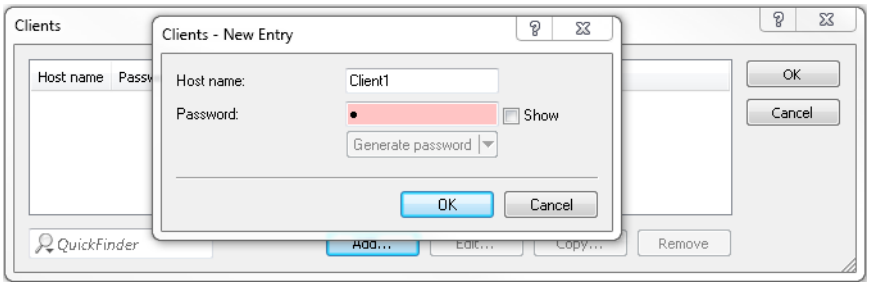
Default realm

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

Empty realm

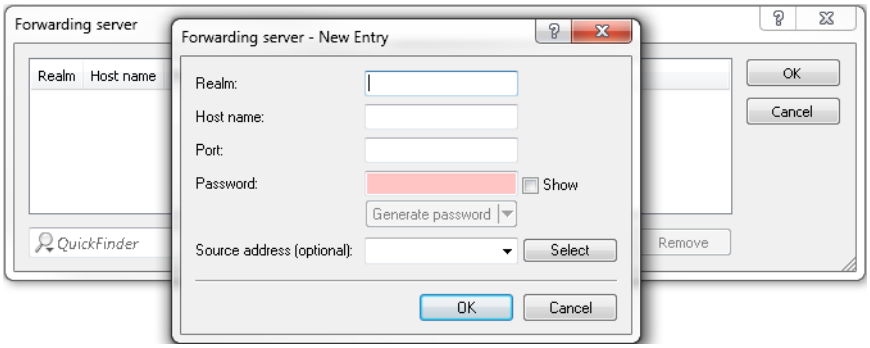
This realm is used when the specified username does not contain a realm.

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.

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**