

■ connecting your business



Addendum

LCOS 8.84

Inhalt

1 Addendum to LCOS version 8.84.....	5
2 Configuration.....	6
2.1 Default Rollout Wizard.....	6
2.1.1 Additions to the Setup menu.....	6
2.2 Automatic generation of device-specific SSH keys.....	8
2.3 Suppress the security prompts during SSH key generation.....	8
2.4 Setting up multiple SNMP communities.....	9
2.4.1 Additions to the Setup menu.....	9
3 LCMS.....	11
3.1 Enhancements to LANconfig.....	11
3.1.1 Quick Rollback.....	11
3.1.2 Release firmware via the context menu.....	12
3.1.3 Exporting key fingerprints when commissioning CC devices	12
3.1.4 TLS/STARTTLS support and additional authentication methods with SMTP servers.....	12
3.1.5 Submitting an SNMP community to external programs.....	15
3.2 Enhancements to LANmonitor.....	16
3.2.1 Accessing devices through SNMP communities.....	16
4 Diagnosis.....	17
4.1 Documenting events on the xDSL interface.....	17
4.2 SYSLOG: Extended status display of the login to the cellular network.....	18
4.2.1 Extended status display of the login to the cellular network.....	18
5 Routing and WAN connections.....	21
5.1 Volume budget.....	21
5.1.1 Data volumes on the WAN interface.....	21
5.1.2 Additions to the Setup menu.....	23
5.1.3 Additions to the Status menu.....	28
5.1.4 Enhancements to LANconfig.....	30
5.1.5 Enhancements to LANmonitor.....	32
5.2 Script variable for dynamic IPv6 addresses.....	33
5.3 Assign actions from the action table of a WAN connection.....	34
5.3.1 Configuration.....	34
5.3.2 Additions to the Setup menu.....	36
5.4 Selecting frequency bands in LTE cellular networks.....	36
5.4.1 Enhancements to LANconfig.....	37
5.4.2 Additions to the Setup menu.....	37
5.5 Forwarding data packets from LAN via X.25 (ISDN).....	38
5.5.1 Additions to the Status menu.....	39
5.5.2 Additions to the Setup menu.....	44
5.6 HNAT tracing.....	50

6 IPv6.....	51
6.1 IPv6 prefix delegation from the WWAN to the LAN.....	51
6.1.1 Enhancements to LANconfig.....	51
6.1.2 Additions to the Setup menu.....	52
7 Certificate Management.....	53
7.1 Using internal LCOS variables in the SCEP client.....	53
8 WLAN.....	54
8.1 LANCOM Active Radio Control (ARC).....	54
8.2 Maximum EIRP value depends on the transmission standard.....	54
8.3 Adjusting the maximum transmit rate for multicasts and broadcasts.....	55
8.3.1 Automatic adjustment of multicast and broadcast transmission rates.....	55
8.3.2 Additions to the Setup menu.....	55
8.3.3 Additions to the Status menu.....	55
8.4 IGMP snooping in auto mode.....	56
8.4.1 General settings.....	57
8.4.2 Port settings	59
8.4.3 Static members.....	59
8.4.4 Simulated queriers.....	60
8.4.5 Additions to the Setup menu.....	61
8.5 Converting DHCP responses from broadcast into unicast	62
8.5.1 Additions to the Setup menu.....	62
8.6 Adaptive noise immunity to reduce interference on the WLAN.....	63
8.6.1 Enhancements to LANconfig.....	63
8.6.2 Additions to the Setup menu.....	64
8.6.3 Additions to the Status menu.....	64
8.7 Opportunistic key caching.....	66
8.7.1 Opportunistic key caching (OKC).....	66
8.7.2 Enhancements to LANconfig.....	67
8.7.3 Additions to the Setup menu.....	71
8.7.4 Additions to the Status menu.....	72
8.8 Feature enhancement of the WLC tunnel interface.....	73
8.9 Support for 802.11u/HotSpot 2.0 on WLAN controllers.....	74
8.9.1 Additions to the Status menu.....	74
8.9.2 Additions to the Setup menu.....	83
9 Public Spot.....	106
9.1 Any phone number format for Smart Ticket.....	106
9.2 Sending login data via a GSM-capable device (Smart Ticket).....	106
9.2.1 Configuring SMS authentication.....	106
9.2.2 Additions to the Setup menu.....	108
9.3 Terms of use when authenticating with name, password (and MAC address).....	110
9.3.1 Additions to the Setup menu.....	111
9.4 Advanced configuration of user templates with LANconfig.....	111
9.4.1 Setting default values for the Public Spot wizard.....	111

9.4.2 Setting default values for the user templates.....	113
9.5 Multi-lingual login and text messaging.....	114
9.5.1 Customizing text message content.....	114
9.5.2 Additions to the Setup menu.....	116
9.6 New URL placeholders (template variables).....	122
9.7 User-dependent HTML output on the voucher.....	123
9.8 Show/hide the LANCOM logo and header image in the voucher.....	123
9.8.1 Additions to the Setup menu.....	123
9.9 Additional languages for the authentication pages.....	124
9.10 Special template pages for Smart Ticket.....	124
9.10.1 Login pages depending on the login mode.....	124
9.11 Error page in case of WAN connection failure.....	125
9.11.1 Additions to the Setup menu.....	125
9.12 Template caching.....	126
9.12.1 Additions to the Status menu.....	127
9.12.2 Additions to the Setup menu.....	127
9.13 Quick link to the session information window.....	128
9.13.1 Additions to the Setup menu.....	128
10 RADIUS.....	129
10.1 Targeted (de-)activation of RADIUS user accounts.....	129
10.1.1 Additions to the Setup menu.....	129
10.2 Login to the LCOS administration interface via RADIUS.....	130
10.2.1 Login to the LCOS administration interface via RADIUS.....	130
10.2.2 Additions to the Setup menu.....	130
10.2.3 Enhancements to LANconfig.....	135
10.3 Separate RADIUS accounting server for each SSID	138
10.3.1 Additions to the Setup menu.....	138
11 Sending and receiving SMS text messages.....	141
11.1 Receiving SMS text messages.....	141
11.2 Basic configuration of the SMS module.....	141
11.3 Managing SMS text messages with LANmonitor.....	142
11.4 Sending SMS text messages with LANmonitor.....	143
11.5 URL placeholder for sending SMS text messages.....	143
11.6 Character set for sending SMS.....	144
11.7 Additions to the Status menu.....	145
11.7.1 SMS.....	145
11.8 Additions to the Setup menu.....	148
11.8.1 SMS.....	148
11.9 Enhancements to command-line commands	151
11.9.1 SMS send command.....	151

1 Addendum to LCOS version 8.84

This document describes the changes and enhancements in LCOS Version 8.84 since the previous version.

2 Configuration

This chapter gives you an overview of the ways and means by which you can access the device and adjust its settings. It contains descriptions for the following topics:

- Configuration tools
- Control and diagnostic functions of the device and software
- Backing up and restoring complete configurations
- Installing new firmware on the device

2.1 Default Rollout Wizard

Your device is supplied with a preconfigured Rollout Wizard, which allows you to retrieve a configuration from a *LANCOM Large Scale Rollout & Management (LSR)* server with just a few clicks. The **Default Rollout Wizard** runs if you have enabled the Rollout Wizard in LCOS but have not set up a customized Rollout Wizard.

The Default Rollout Wizard asks you for all the information that it needs to connect to the LSR. This includes:

- The protocol used for the connection (HTTP or HTTPS);
- The IP address or the DNS name of the LSR server;
- The user name and password for authentication against the LSR;
- The name or number of the rollout project;
- The device ID (optional); and
- The rollout TAN for the device.

 This process can be partially or even fully automated if you enter the relevant information into the device permanently. The table for this is located in the Setup menu under **HTTP > Rollout-Wizard > Presets**. Standard presets are the port and the loopback address used by the Wizard.

 If your device has a USB port, its automatic upload feature allows a USB stick to supply an unconfigured device with the basic information required by the Rollout Wizard.

Before the device starts processing the rollout, the wizard displays a summary of the connection data used. Also, the device uses an ICMP echo request (ping) to determine whether the specified server is available. If this test fails, you have the option to re-configure the wizard or to continue the rollout process anyway. The host is available, the device begins with the retrieval of a configuration from the LSR.

 If the LSR server can be accessed via the Internet, but you are running the Rollout Wizard on a device without an Internet connection, you must first execute the Internet Setup Wizard.

2.1.1 Additions to the Setup menu

Presets

This table enables you to predefine the values for all of the parameters that are requested by the Default Rollout Wizard. Parameters configured in this way are no longer queried when you run the Default Rollout Wizard.

 A 'blank' predefined value for **Port** and for **Source loopback address** will be interpreted by the device as the entry 'Auto'. In this case, the Default Rollout Wizard uses the corresponding HTTP(S) standard port and, as the

loopback address, the address of your device that matches to the target. If you are working with different ARF networks, you must use the loopback address to specify the ARF where the LSR server is located.

SNMP ID:

2.21.20.9

Telnet path:**Setup > HTTP > Rollout-Wizard****Name**

This entry shows the name of the parameter to be filled out with preset values.

SNMP ID:

2.21.20.9.1

Telnet path:**Setup > HTTP > Rollout-Wizard > Presets****Preset**

For the corresponding parameter, this entry shows the preset value to be used by the Rollout Wizard.

SNMP ID:

2.21.20.9.2

Telnet path:**Setup > HTTP > Rollout-Wizard > Presets****Possible values:**

Any string, max. 127 characters from

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

Default:**Use preset**

This entry defines whether the parameter value configured here is to be used by the Rollout Wizard. If set to yes, the Rollout Wizard will no longer query this parameter.

SNMP ID:

2.21.20.9.2

Telnet path:**Setup > HTTP > Rollout-Wizard > Presets****Possible values:**

No

Yes

Default:

(Depends on the line)

Delete Wizard

This action is used when you want to delete a custom Rollout Wizard. The next time you start the Rollout Wizard, the device reverts to the standard internal LCOS wizard.

SNMP ID:

2.21.20.10

Telnet path:

Setup > HTTP > Rollout-Wizard

Possible parameters:

No parameters available

2.2 Automatic generation of device-specific SSH keys

Ex-factory, all LCOS-based devices with an LCOS version earlier than 8.84 are equipped with a default set of cryptographic keys that are represented by the following fingerprints:

SSH

```
ssh-dss 27:c5:1d:9f:be:27:3d:50:d7:bf:c1:68:0b:18:97:d7
ssh-rsa 03:56:e6:52:ee:d2:da:f0:73:b5:df:3d:09:08:54:b7
```

If you have a device with LCOS 8.84 or later and you have not uploaded an individual key to the device, the internal SSH server will try to compile its own device-specific SSH keys after a configuration reset followed directly by a system restart. These include

- an SSH-2 RSA key of 2048-bit length and
- an SSH-2 DSS key of 1024-bit length (as defined in FIPS 186-2),

which the device stores as **ssh_rsakey** and **ssh_dsakey** in its internal file system.

If key generation is successful, the entry **SSH: ... host key generated** is entered as a **note** in the SYSLOG; if it fails, an entry **SSH: host key generation failed, try later again with '...'** is made as an **alarm**. If key generation fails (e.g. insufficient entropy), the device falls back to its factory cryptographic key.



If you perform an update from an older version of LCOS to 8.84 or higher without a subsequent configuration reset, the device does not generate a device-specific SSH key. This is to maintain compatibility with existing installations. However, you can manually initiate the key generation. Enter the following commands in the console:

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
```

2.3 Suppress the security prompts during SSH key generation

As of LCOS 8.84, you can optionally suppress any security prompts during SSH key generation in LCOS:

```
sshkeygen [-?|-h] [-t (dsa|rsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-q

This parameter enables the 'quiet' mode for the key generation. If you set this parameter, LCOS overwrites any existing RSA or DSA keys without asking; there is no information about the progress of the operation. You can, for example, use this parameter in a script to suppress any security prompts for the users.

2.4 Setting up multiple SNMP communities

As of LCOS 8.84, you have the option to define multiple read-only communities for SNMP access. The entries in the table [2.9.22 Read-Only-Communities](#) on page 10 complement the existing parameters in [2.9.15 Read-Only-Community](#) on page 9. The device evaluates the stored entries with an equal priority.

2.4.1 Additions to the Setup menu

Password required for SNMP read access

This setting specifies whether a password is required to read SNMP messages with an SNMP agent (e.g. LANmonitor).

SNMP ID:

2.9.10

Telnet path:

Setup > SNMP

Possible values:

No

This setting allows information about the state of the device, current connections, reports, etc., to be read out publicly via SNMP ('public' ready-only community enabled).

Yes

This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device ('public' ready-only community disabled). The authorization can either use the access credentials of the administrator account or those of the individual SNMP community.

Default:

No

Read-Only-Community

This parameter specifies an individual SNMP community for read access. Either specify a master password or a username:password pair. Leave the field empty if you do not wish to use any read-only communities except for 'public' (if activated).

 Disabling the community 'public' has no effect on accessing with the community created here. An individual SNMP read-only community always has an alternative access key, which is not tied to an administrator account.

SNMP ID:

2.9.15

Telnet path:

Setup > SNMP

Possible values:

No direct dependency on other values. However, **Read-Only-Community** under **Setup > SNMP > Read-Only Communities** does add additional read-only communities to the parameters defined here.

Max. 31 characters from [A-Z][a-z][0-9]@{|}~!\$%&'()+-./:;<=>?[\]^_`~`

Default:

empty

Read-Only-Communities

In this table, you define further write-protected communities for SNMP access.

SNMP ID:

2.9.22

Telnet path:

Setup > SNMP

Read-Only-Community

This parameter specifies an additional individual SNMP community for read access. You can specify either a master password or a username:password pair.

 Disabling the community 'public' has no effect on accessing with the community created here. An individual SNMP read-only community always has an alternative access key, which is not tied to an administrator account.

SNMP ID:

2.9.22.1

Telnet path:

Setup > SNMP > Read-Only-Communities

Possible values:

No direct dependency on other values. However, this parameter does supplement the **Read-Only-Community** under **Setup > SNMP** with additional read-only communities.

Max. 31 characters from [A-Z][a-z][0-9]@{|}~!\$%&'()+-./:;<=>?[\]^_`~`

Default:

empty

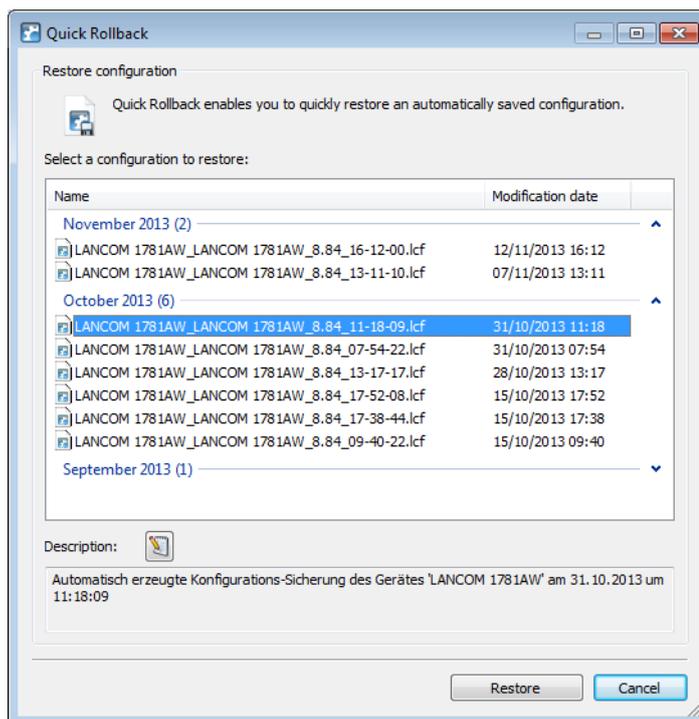
3 LCMS

3.1 Enhancements to LANconfig

3.1.1 Quick Rollback

As the counterpart to the automatic backup of device configurations, you can restore configuration backups with a single click. Just highlight the device and select **Device > Quick rollback**. LANconfig lists all of the device configurations that have been saved under the path for the automatic device-configuration backups. If LANconfig cannot find a backup file for the selected device, it cancels this action with a warning message.

 LANconfig allocates the configuration backup to the device by using the serial number stored in the meta data of the backup. As of LCOS 8.84 the serial number is automatically written to the backup; for older configuration backups without the serial number, you need to add these manually in order for Quick Rollback to recognize the files. Please also refer to [Advanced meta data for configuration files](#) on page 12.



To restore a configuration backup, select an entry and click on **Restore**.

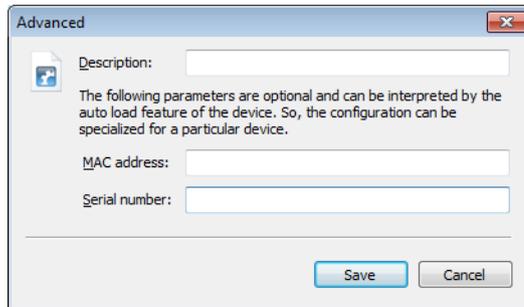
You also have the option to add comments to the configuration backups, or edit existing comments: The **Edit description** button  enables you to edit the field below it containing the comment text. Click on **Save description**  to write the text in the comment box back to the backup file.

 Quick Rollback is not available for LANCOM switches.

Advanced meta data for configuration files

If a device configuration is stored manually, LANconfig provides the option to save extra meta data in addition to the usual MAC address and/or device serial number in the configuration file (*.lcf). This extended meta-data can be taken into account, for example when performing a quick config rollback or when loading a device configuration via USB.

To include the additional meta data into a configuration file, click the **Advanced** button in the LANconfig save-file dialog and enter the data—if not entered already—into the respective fields.



Alternatively you can open a lcf/lcs file in a text editor and enter the advanced meta data by hand. Add to the line (`<Firmware>`) (`<Feature-Mask>;<Feature-IDs>;<Hardware-Mask>`) the following text with the brackets (`MAC:<MAC-Address>;SERIAL:<Serialnumber>`).

Example, any line breaks are due to the display formatting:

```
(Configuration of 'DEVICE-01' from 11/12/2013)
(8.84.0081) (0x0000c010,IDs:4,e,f,2b;0x0c000002) (MAC:00a0571d12fc;SERIAL:4002578718100036)
```

3.1.2 Release firmware via the context menu

With firmware running in test mode, you have the option of activating it using the firmware management in context menu of LANconfig. The firmware selection dialog was revised in LANconfig 8.84 for this purpose.

3.1.3 Exporting key fingerprints when commissioning CC devices

As of LANconfig 8.84, you have a convenient option to export the SSH key fingerprints when commissioning CC devices. While the CC Start-up Wizard is running, LANconfig creates the file **CCWizSummary.csv** containing the IP address of the device, the device name and its (SSH) key fingerprint. As an example, this list could be used by system administrators who need to be certain that they are connecting to the correct device, for instance when conducting remote maintenance or logging in to a device for the first time after a rollout.

By default, LANconfig saves this CSV file under `C:\Program files`

(`x86`)\LANCOM\LANconfig\Logging\ . You have also the option to change this path in the input field under **Tools > CC Start-up Wizard > Settings > Path**.

3.1.4 TLS/STARTTLS support and additional authentication methods with SMTP servers

As of LCOS 8.84, the device uses by default port 587 for connecting to SMTP servers. Also, connection establishment via STARTTLS is preferred. In addition to the PLAIN authentication method, a secure alternative is now available which enables the device to act according to the requirements of the SMTP server.

Setting up an e-mail address to send messages

A LANCOM device can send e-mail to a predefined address if certain events should occur. These events can include:

- Information about disconnections on a WAN interface
- Messages from the firewall or content filter
- Sending VPN profiles

You set up the e-mail address as follows:

In LANconfig you can configure an e-mail under **Log & Trace > SMTP account**.

With the Simple Mail Transfer Protocol (SMTP), your device can inform you about specific events (e.g. Denial of Service attacks).

General settings

This is the server to which the device will post email messages:

SMTP server:

SMTP port:

Encryption/TLS:

Sender email address:

Source address:

Authentication

You can specify the necessary SMTP account data here:

Authentication:

User name:

User password: Show

SMTP server: In this field, enter the IP address of the SMTP server.

SMTP port: By default, this is set to port 587 for transmitting unencrypted e-mails.

Encryption/TLS: Here you determine if and how the device encrypts the connection. The available values have the following meaning:

- **None:** No encryption. The device ignores any STARTTLS responses from the server.
- **Encrypted (SMTPS):** The device uses SMTPS, i.e. encryption is active from the connection establishment.
- **Preferred (STARTTLS):** The connection establishment is not encrypted. If the SMTP server offers STARTTLS, the device will use encryption. This is the default setting.
- **Required (STARTTLS):** The connection establishment is not encrypted. If the SMTP server does not offer STARTTLS, the device transmits no data.

Sender e-mail address: Enter a valid e-mail address for the LANCOM to use as the sender address. The specified SMTP server will message this address in case of delivery problems, for example. If this address is not specified or not valid, some SMTP servers may refuse to deliver any messages.

Source address: You can optionally set an alternative sender address here to be used by the LANCOM. If you have configured loopback addresses, you can specify them here as sender address. The field accepts various input formats:

- Name of the IP network (ARF network), whose address should be used by the device.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ. If there is an interface named "DMZ", then the device uses this address.
- "LB0" ... "LBF" for one of the 16 loopback addresses, or its name
- Any IP address in the form $x . x . x . x$.

Authentication: Here you determine if and how the device authenticates at the SMTP server. The available values have the following meaning:

- **None:** No authentication.
- **Preferred plain text:** Authentication takes place in plain text (PLAIN, LOGIN) if the server requires authentication. If you do not want plain-text authentication, the device uses a secure authentication method.
- **Preferred encrypted:** Secure authentication takes place, if possible. Otherwise the device uses either a plain text authentication or no authentication at all, depending on the server settings.
- **Encrypted:** If the server requires authentication, the password is sent in encrypted (e.g. CRAM-MD5). Plain text authentication does not occur.

Name: Enter the user name which the LANCOM uses to login to the SMTP server.

Password: Enter the password which the LANCOM uses to login to the SMTP server.

Additions to the Setup menu

SMTP port

Enter the number of the SMTP port of the aforementioned server for unencrypted e-mail transmission. The default value is 587.

SNMP ID:

2.27.2

Telnet path:

Setup > Mail

Possible values:

Max. 10 characters

Default:

587

SMTP-use-TLS

Here you determine if and how the device encrypts the connection. The available values have the following meaning:

- **No:** No encryption. The device ignores any STARTTLS responses from the server.
- **Yes:** The device uses SMTPS, i.e. encryption is active from the connection establishment.
- **Preferred:** The connection establishment is not encrypted. If the SMTP server offers STARTTLS, the device will use encryption. This is the default setting.
- **Required:** The connection establishment is not encrypted. If the SMTP server does not offer STARTTLS, the device transmits no data.

SNMP ID:

2.27.12

Telnet path:

Setup > Mail

Possible values:

No

Yes

Preferred

Required

Default:

Preferred

SMTP authentication

Here you specify if and how the device authenticates at the SMTP server. The device's behavior depends on the server settings: If the server does not require authentication, the login occurs in any case. Otherwise, the device reacts according to the settings described below:

SNMP ID:

2.27.13

Telnet path:

Setup > Mail

Possible values:

None

Basically no authentication.

Plain text preferred

The authentication preferably occurs in plain text (PLAIN, LOGIN), if the server requires authentication. If it does not accept plain text authentication, the device uses secure authentication.

Encrypted

The authentication is done without transmitting the password (e.g., CRAM-MD5), if the server requires authentication. Plain text authentication does not take place.

Preferably encrypted

The authentication is preferably encrypted (e.g., CRAM-MD5), if the server requires authentication. If it does not accept secure authentication, the device uses plain text authentication.

Default:

Preferably encrypted

3.1.5 Submitting an SNMP community to external programs

From LANconfig 8.84, you have the option of storing access credentials for calling external programs in the form of an SNMP community (**Device > Properties > Protocols & logins**). LANconfig then automatically sends the information when the relevant program is called.

Login information

Enter the access credentials for the external programs in this field. Click **New** to select one or more application(s) and enter the relevant access credentials.

Depending on your selection, the dialog window requests different access credentials. You always have the option of authenticating yourself with the username and password of your administrator login for the corresponding program. In the case of LANmonitor, you can alternatively specify a (custom) SNMP community for read-only access. For more information about read-only SNMP access see the Reference Manual

The screenshot shows a dialog box titled "Login information". It contains two input fields: "Administrator" and "Password". To the right of the "Password" field are "OK" and "Cancel" buttons. Below the input fields is a section labeled "Usage:" with four checkboxes: "LANmonitor (Read)", "LANmonitor (Write)", "LANtracer" (which is checked), and "Browser".

The screenshot shows a dialog box titled "Login information". It contains two input fields: "Administrator" and "Password/Community". To the right of the "Password/Community" field are "OK" and "Cancel" buttons. Below the input fields is a section labeled "Usage:" with four checkboxes: "LANmonitor (Read)" (which is checked), "LANmonitor (Write)", "LANtracer", and "Browser".

3.2 Enhancements to LANmonitor

3.2.1 Accessing devices through SNMP communities

As of LANmonitor 8.84, you have the option of storing the SNMP-access credentials in the form of an SNMP community (dialog **Device > Add > General** and also **Device > Properties > General**).

Authentication

In this section, choose how and with what credentials you authenticate yourself to the device. The setting you need depends on whether you have restricted the SNMP read-access to the device and have defined a community of your own. Learn more about this in the Reference Manual.

- **SNMP read-only community:** Use this setting if authentication at the device is handled by
 - the public community `public` or
 - your own community in the form of a master password or `username:password` pair
 . You then enter these into the **Community** field.
- **Administrator/Password:** Use this setting if authentication at the device is handled by
 - your own community in the form of a `username:password` pair or
 - the credentials of an administrator account
 . You then specify the user name in the **Administrator** field and the password in the **Password** field.

 Pay attention to the correct spelling/capitalization, because SNMP access to the device is blocked if the wrong data is entered.

You also have the option of saving the **access credentials for device actions (SNMP write community)** either for the current session or permanently in LANmonitor. This data is required for all device actions (such as deleting or resetting status values). If you do not store any credentials, the program prompts you for them the next time you attempt to execute an action.

 For read-only access, you should preferably specify a read-only community instead of an administrator account, as SNMP packets are transmitted in plain text with SNMPv2.

4 Diagnosis

4.1 Documenting events on the xDSL interface

As of LCOS 8.84, the device logs changes of state on the xDSL interfaces.

The device generates a SYSLOG entry for each of the following xDSL interface events:

Status	Meaning	SYSLOG severity
xDSL: Booting modem: ...	The modem is restarting.	NOTICE
xDSL: Set up line to <line mode>/<line type>	The xDSL module establishes the connection with the mode and type specified. The following values are possible: <ul style="list-style-type: none"> Line mode: Disabled, auto and all modes configured in Setup > Interfaces > ADSL or VDSL interface. Line type: POTS, ISDN 	INFORM
xDSL: Line is up. DS rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:	The modem connected successfully with the specified values.	NOTICE
xDSL: Line data update. DS rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. This can lead to a change in the line values. After one minute, the modem transmits the current line values.	NOTICE
xDSL: Line data update.	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. After one minute, the modem transmits this message if the line values do not change after the synchronization.	NOTICE
xDSL: Line disconnected due to	The connection was disconnected for the specified reason. The following values are possible: <ul style="list-style-type: none"> modem reboot retrain silence high line error rate protocol setting line type setting automode line type switch modem timeout VC parameter change 	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	The value between the required and measured signal-noise ratio (SNR) has changed by more than 1dB.	INFORM

4.2 SYSLOG: Extended status display of the login to the cellular network

As of LCOS version 8.84, the SYSLOG displays further information about the status of the login process on a cellular network (UMTS/3G+, GPRS, LTE/4G).

4.2.1 Extended status display of the login to the cellular network

In order to more quickly analyze connection problems in a cellular network, WWAN-capable LANCOM routers report all logon procedures to the SYSLOG. In this manner, the user can recognize if and why the cellular service provider rejected the connection, for example.

The device generates a SYSLOG entry for each of the following events:

Status	Meaning	SYSLOG severity
WWAN: Currently not searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Registered to home network	The modem has registered on its service provider's cellular network.	INFORM
WWAN: Registered to foreign network	The modem has successfully registered on the cellular network of the service provider's roaming partner.	INFORM
WWAN: Unknown registration	Initial value. The modem has not yet received a response from the radio module regarding the registration status.	INFORM
WWAN: Network registration denied	The cellular service provider has rejected the login on the cellular network.	ERROR
WWAN: Lost network registration	The modem lost the connection to the registered cellular network.	NOTICE
WWAN: Failed to set network	The modem has replied to the command to assign the network with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Failed to set network mode	The modem has replied to the command to assign the network mode with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using modem '...'	Displays the modem in use.	INFORM
WWAN: Modem is gone.	Modem no longer available.	INFORM
WWAN: Resetting modem.	Re-init by modem reset	WARNING
WWAN: Local disconnect.	D-channel disconnect	INFORM
WWAN: Local disconnect (Release).	D-channel release	INFORM
WWAN: Force 2G mode at ... dB.	Modem starts the 2G fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem ends the 2G fallback	INFO

Status	Meaning	SYSLOG severity
WWAN: Forced 2G mode disabled.	The 2G fallback mode is disabled.	INFO
WWAN: PIN missing in profile.	PIN is missing from the profile.	ERROR
WWAN: PUK required.	Modem requires the PUK.	ERROR
WWAN: Invalid PIN.	Incorrect PIN	ERROR
WWAN: Failed to set APN	Error when setting the APN The modem has replied to the command to assign the APNs with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using profile '...'	Name of the profile in use.	NOTICE
WWAN: Cannot find profile '...'	Profile not available.	ERROR
WWAN: Disconnected.	Physical connection is terminated.	INFORM
WWAN: Connected: '...'	The modem has established a data connection and can now transmit data over the cellular network.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Cell ID and country code.	INFORM
WWAN: Current Network is '...'	Network (text)	INFORM
WWAN: Current Network is	Network (number)	INFORM
WWAN: Mode ..., Band '...'	Display of network mode and band	INFORM
WWAN: Mode ..., Band '...', Bandwidth in MHz: ..., Channel (Rx/Tx): .../....	Display of network mode, band, bandwidth and channel (transmit and receive direction).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Display of network mode, band and channel (transmit and receive direction).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Current QoS data rate (down/upstream)	INFORM
WWAN: Network mode is '...'	Current mode. Possible values are: <ul style="list-style-type: none"> ■ GPRS ■ EDGE ■ UMTS ■ HSPA ■ LTE 	INFORM
WWAN: Signal strength is ... dBm.	Current signal strength	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Access point currently being used in the network.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Change of network access point	INFORM
WWAN: Temperature is ...°C.	Current temperature of the module	INFORM
WWAN: Temperature status: '...'	Current temperature status of the module. Possible values are: <ul style="list-style-type: none"> ■ Normal ■ High warning ■ High critical ■ Low critical 	INFORM (normal), WARNING (high warning), CRITICAL (high critical, low critical)

Status	Meaning	SYSLOG severity
WWAN: Closing device: '...'. WWAN: Hangup: '...'. WWAN: Error in modem init: '____'.	The device running the connection to the WAN is shutting down. The modem terminates the network connection. An error has occurred when initializing the modem.	INFORM INFORM ERROR

5 Routing and WAN connections

5.1 Volume budget

As of LCOS 8.84 the device records the volume of data sent and received over all WAN interfaces. This may be useful if you wish to react to throttled data rates, for example.

5.1.1 Data volumes on the WAN interface

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. The device captures the amount of data sent over each WAN interface, archives the values for up to 12 months, and can perform actions when a specified threshold is reached. The budgets also apply to VPN, PPTP, or all other kinds of connection.

At the change of the month, the device archives the data for the previous month and resets the counter to zero for the current month. You can view the current data volume and the archived information in LANmonitor or in the WEBconfig status menu. The archive contains data from the last 12 months. In the 13th month, the device automatically overwrites the archive data of the 1st month.

ⓘ Currently, this feature is only available for the following device types and series:

- LANCOM L-45x series
- LANCOM 1781 series
- LANCOM 1780EW-3G, 1780EW-4G
- LANCOM WLC-4006+, WLC-4025+, WLC-4100
- LANCOM 7100 VPN, 7100+ VPN, 9100 VPN, 9100+ VPN
- LANCOM IAP-321, IAP-321-3G, IAP-3G
- LANCOM OAP-322, OAP-321, OAP-321-3G, OAP-3G

Configuring data volume budgets

The following section describes how you can use LANconfig to manage the data volumes exchanged with remote stations.

1. Start LANconfig with **Start > Programs > LANCOM > LANconfig** and open the configuration of the device for which you want capture the data volumes.
For information on configuring devices with LANconfig refer to the LCMS section of the Reference Manual.
2. In the configuration dialog, navigate to the item **Management > Budget**.

Budget monitoring

Via budget monitoring data volume can be captured per WAN connection and actions can be configured when exceeding limits.

Specify the networks per WAN connection which data volume should not be captured.

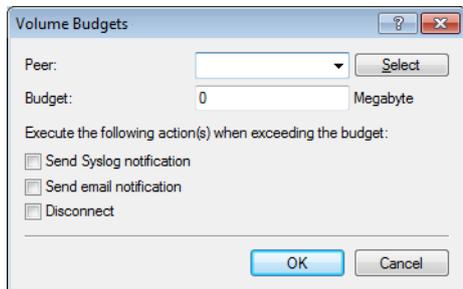
Specify the time for resetting the captured data volume.

Specify an email address for sending messages when actions are executed.

email Address:

If the device should send an e-mail when your data volume is exceeded, you can enter the required address into the field **E-mail address**.

3. Click on **Volume budgets** and then on **Add**.



The item **Peer** lets you select the remote station which requires a volume budget. With **Select** you can choose from the available remote stations or manage new ones.

Specify the data volume in the **Budget** field. In most cases this value is the permitted data volume specified by the provider before the data rate is throttled.

Further, you can specify actions that the device should perform when the budget is reached:

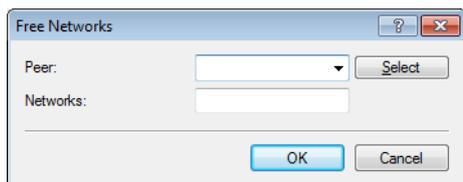
- **Send SYSLOG notification:** The device stores a SYSLOG message (with the flag "Critical") that you can analyze with LANmonitor or a special SYSLOG client.
- **Send e-mail notification:** The device sends a message to the e-mail address that you specified above.
- **Disconnect:** The device disconnects from the remote station.



The **disconnect** action activates the charge limiter. The device can no longer connect to this remote until the end of the month unless you increase the volume budget for this remote site.

You can also specify that the device should perform multiple actions. If they include the action **disconnect**, the device performs this action as the last one.

4. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.
5. If data transfer to certain networks does not affect the volume budget for a remote site, you can exclude these networks from the budgeting. To do this, click on **Free networks** and then on **Add**.



The item **Peer** lets you select the remote station which is to be excluded. With **Select** you can choose from the available remote stations or manage new ones.



You can make multiple entries for each remote by suffixing the name of the remote station with the # character and adding a number (e.g. "INTERNET", "INTERNET#1", "INTERNET#2", etc.). This is useful if you explicitly wish to define an exception that is only temporarily active. When this exception is no longer valid, you delete only the entry with the correspondingly numbered remote station.

In the **Networks** field you can specify IPv4 and IPv6 addresses and also whole networks in prefix notation (for example "192.168.1.0/24"). Separate each entry with a comma. Here too you can add the # character and a digit to the remote station name.

6. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.
7. You can set the day and time when the device should start each monthly billing period under **Billing period**.

8. If you want to change the preset values, select the line containing the peer named "*" and click on **Edit**; otherwise click on **Add**.

The screenshot shows a dialog box titled "Billing period". It has a "Peer:" label followed by a dropdown menu and a "Select" button. Below this is the instruction "Specify the time for a monthly reset of the captured data volume." followed by three input fields: "Day:" with the value "1", "Hour:" with the value "0", and "Minute:" with the value "0". At the bottom of the dialog are "OK" and "Cancel" buttons.

The item **Peer** lets you select the remote station for which you want to set the time when the period starts. With **Select** you can choose from the available remote stations or manage new ones.

- ! You can use wildcards for the names of the remote stations. The wild card "*" in this case applies for all remote stations.

In the fields **Day**, **Hour** and **Minute** you set the day of the month and the time at which the device resets the budget for this peer.

- ! By default the device resets the budget for all peers on the first day of the month at 00:00h.

- ! If you enter the value "31" in the field **Day**, the device does not reset the budget in months with fewer days (e.g. February or November).

9. Click **OK** to add this entry to the table, and then click **OK** to add the entries to the configuration of the device.
10. Finally click on **OK** to load the configuration into the device.

5.1.2 Additions to the Setup menu

Reset budgets

You can manually reset units, time and volume budgets.

Enter the name of the WAN connection as the parameter. You can reset all volume budgets with the parameter '*'. If you do not specify a parameter, you reset only the unit- and time counters.

- ! By resetting the current budget, you remove any charge limiter that may be in effect.

SNMP ID:

2.3.12

Telnet path:

Setup > Charges

Activate additional budget

Some providers allow you an additional data volume or time limit if your budget is reached. This action can be used to increase the volume- or time budget by an appropriate amount.

Specify the name of the WAN connection as well as the amount of the budget in MB as additional parameters. If you do not specify a budget, you approve the full amount of the budget specified for this WAN connection.

- ! By activating an additional budget, you remove any charge limiter that may be in effect.

SNMP ID:

2.3.16

Telnet path:**Setup > Charges****Volume budgets**

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. This directory allows you to set a data volume for each remote station, and also to define an action for the device to perform when this limit is exhausted.

SNMP ID:

2.3.17

Telnet path:**Setup > Charges****Peer**

Name of the remote station for which this data volume applies.

SNMP ID:

2.3.17.1

Telnet path:**Setup > Charges > Volume-budgets****Possible values:**

Select from the list of defined peers.

Max. 16 characters

Default:

Blank

Limit-MB

Data volume in megabytes that applies to the specified remote station.

SNMP ID:

2.3.17.2

Telnet path:**Setup > Charges > Volume-budgets****Possible values:**

0 - 4294967295 MB

Max. 10 characters

Special values:

0: No monitoring of data volume

Default:

0

Action

Action to be executed by the device when the budget is exhausted. Possible actions are:

- **syslog**: The device stores a SYSLOG message (with the flag "Critical") that you can analyze with LANmonitor or a special SYSLOG client.
- **mail**: The device sends a message to the e-mail address that you specified in **Setup > Charges > Charging-Email**.
- **disconnect**: The device disconnects from the remote station.



The **disconnect** action activates the charge limiter. The device can no longer connect to this remote until the end of the month unless you increase the volume budget for this remote site.

You can also specify that the device should perform multiple actions. If they include the action **disconnect**, the device performs this action as the last one.

SNMP ID:

2.3.17.3

Telnet path:**Setup > Charges > Volume-budgets****Possible values:**

SYSLOG

Mail

Disconnect

Default:

Blank

Free networks

If data transfer to certain networks does not affect the volume budget for a remote site, you can exclude these networks from the budgeting.

SNMP ID:

2.3.18

Telnet path:**Setup > Charges****Peer**

Name of the remote station for which this exception applies.



You can make multiple entries for each remote by suffixing the name of the remote station with the # character and adding a number (e.g. "INTERNET", "INTERNET#1", "INTERNET#2", etc.). This is useful if you explicitly wish to define an exception that is only temporarily active. When this exception is no longer valid, you delete only the entry with the correspondingly numbered remote station.

SNMP ID:

2.3.18.1

Telnet path:**Setup > Charges > Free -Networks****Possible values:**

Select from the list of defined peers.

Max. 20 characters

Default:

Blank

Free networks

This parameter allows you to specify individual IPv4- and IPv6 addresses, or even entire networks (using prefix notation, for example "192.168.1.0/24"), which are exempt from the budget.

SNMP ID:

2.3.18.2

Telnet path:**Setup > Charges > Free -Networks****Possible values:**

Valid IPv4- and IPv6 address(es), max. 100 characters. Multiple values can be provided in a comma-separated list.

Default:

Blank

Budget control

This table defines when the monthly recordings should begin.

SNMP ID:

2.3.19

Telnet path:**Setup > Charges****Peer**

Name of the remote station for which this time applies.



You can use wildcards for the names of the remote stations. The wild card "*" in this case applies for all remote stations.

SNMP ID:

2.3.19.1

Telnet path:**Setup > Charges > Budget-Control**

Possible values:

Select from the list of defined peers.

Max. 16 characters

Default:

Blank

Day

Day of the month for resetting the data-volume budget.

SNMP ID:

2.3.19.2

Telnet path:

Setup > Charges > Budget-Control

Possible values:

1 - 31

Default:

1

Hour

Hour of the day for resetting the data-volume budget.

SNMP ID:

2.3.19.3

Telnet path:

Setup > Charges > Budget-Control

Possible values:

0 - 23

Default:

0

Minute

Minute of the hour for resetting the data-volume budget.

SNMP ID:

2.3.19.4

Telnet path:

Setup > Charges > Budget-Control

Possible values:

0 - 59

Default:

0

Charging e-mail

If the device is to send an e-mail when the data volume is exhausted, you specify the e-mail address here.

SNMP ID:

2.3.20

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

Valid e-mail address with a maximum of 255 characters.

Default:

Blank

5.1.3 Additions to the Status menu

Delete values

This action deletes all values in the charging statistics.



By resetting the current budget, you remove any charge limiter that may be in effect.



The archive table for recording the data volumes remains unaffected. Use the separate action **Clear archive** to delete the contents of this table.

SNMP ID:

1.24.3

Telnet path:**Status > Charging****Volume budgets**

This table stores the volume of data used for each remote station in the current time interval.

SNMP ID:

1.24.12

Telnet path:**Status > Charging****Peer**

Name of the remote device

Data-MB

Data volume exchanged with the peer to date, in MB.

Data-KB

Data volume exchanged with the peer to date, in kB.

Limit-MB

Data budget for exchanging data with the peer in the current time interval.

Percent

Budget consumed at the current time in percent.

Flags

Note when the set limit is exhausted. The following values are possible:

- Alarm not acknowledged: This indicates that LANmonitor has not yet acknowledged the alarm.
- Limit exceeded: The data budget for this connection has been exceeded. The connection remains intact, however.
- Charge limiter: The data budget for this connection has been exceeded and the connection is interrupted until the beginning of the next billing period.

Month

Month of the current recording interval.

Year

Year of the current recording interval.

Archive

This table stores the budget data saved over the last 12 months. In the 13th month, the device automatically overwrites the archive data of the 1st month.

SNMP ID:

1.24.13

Telnet path:

Status > Charging

Peer

Name of the remote device

curr-Month

Displays the volume of data transmitted in the current month.

curr-Year

Displays the volume of data transmitted in the current year.

curr-Limit

Displays the data budget for the current time interval.

curr-Flags

Displays a notice when the data volume with the peer has been exceeded for the current recording period.

MB-<Month>

Displays the data volume recorded for the corresponding month in MB.

KB<Month>

Displays the data volume recorded for the corresponding month in kB.

Clear archive

This action deletes all entries in the archive.

SNMP ID:

1.24.14

Telnet path:

Status > Charging

Activate additional budget

Some providers allow you an additional data volume if your budget is reached. This action can be used to increase the budget by an appropriate amount.

Specify the name of the WAN connection as well as the amount of the budget in MB as additional parameters. If you do not specify a budget, you approve the full amount of the budget specified for this WAN connection.

 By activating an additional budget, you remove any charge limiter that may be in effect.

SNMP ID:

1.24.14

Telnet path:

Status > Charging

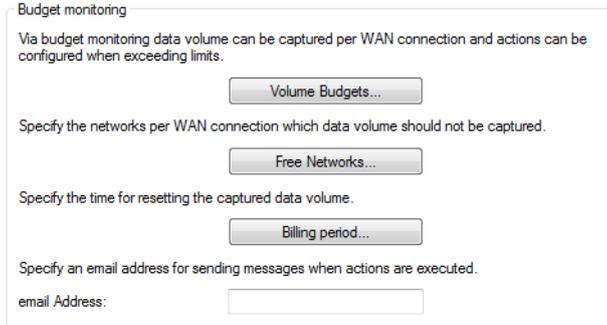
5.1.4 Enhancements to LANconfig

Budget monitoring

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. The device captures the amount of data sent over each WAN interface, archives the values for up to 12 months, and can perform actions when a specified threshold is reached. The budgets also apply to VPN, PPTP, or all other kinds of connection.

At the change of the month, the device archives the data for the previous month and resets the counter to zero for the current month. You can view the current data volume and the archived information in LANmonitor or in the WEBconfig status menu. The archive contains data from the last 12 months. In the 13th month, the device automatically overwrites the archive data of the 1st month.

You can configure budget monitoring under **Management > Budget**.



Budget monitoring

Via budget monitoring data volume can be captured per WAN connection and actions can be configured when exceeding limits.

Specify the networks per WAN connection which data volume should not be captured.

Specify the time for resetting the captured data volume.

Specify an email address for sending messages when actions are executed.

email Address:

If the device should send an e-mail when your data volume is exceeded, you can enter the required address into the field **E-mail address**.

Volume budgets

To set a data volume for communications with a remote site, click on **Volume budgets** and then **Add**.

The item **Peer** lets you select the remote station which requires a volume budget. With **Select** you can choose from the available remote stations or manage new ones.

Specify the data volume in the **Budget** field. In most cases this value is the permitted data volume specified by the provider before the data rate is throttled.

Further, you can specify actions that the device should perform when the budget is reached:

- **Send SYSLOG notification:** The device stores a SYSLOG message (with the flag "Critical") that you can analyze with LANmonitor or a special SYSLOG client.
- **Send e-mail notification:** The device sends a message to the e-mail address that you specified above.
- **Disconnect:** The device disconnects from the remote station.



The **disconnect** action activates the charge limiter. The device can no longer connect to this remote until the end of the month unless you increase the volume budget for this remote site.

You can also specify that the device should perform multiple actions. If they include the action **disconnect**, the device performs this action as the last one.

Free networks

If data transfer to certain networks does not affect the volume budget for a remote site, you can exclude these networks from the budgeting. To do this, click on **Free networks** and then on **Add**.

The item **Peer** lets you select the remote station which is to be excluded. With **Select** you can choose from the available remote stations or manage new ones.

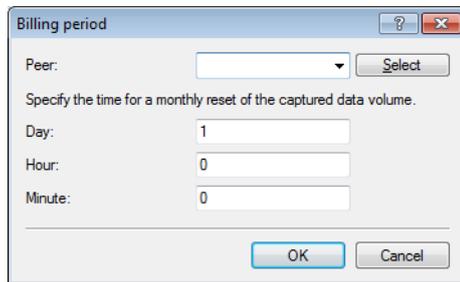


You can make multiple entries for each remote by suffixing the name of the remote station with the # character and adding a number (e.g. "INTERNET", "INTERNET#1", "INTERNET#2", etc.). This is useful if you explicitly wish to define an exception that is only temporarily active. When this exception is no longer valid, you delete only the entry with the correspondingly numbered remote station.

In the **Networks** field you can specify IPv4 and IPv6 addresses and also whole networks in prefix notation (for example "192.168.1.0/24"). Separate each entry with a comma. Here too you can add the # character and a digit to the remote station name.

Billing period

You can set the day and time when the device should start each monthly billing period under **Billing period**.



The item **Peer** selects the remote station for which you want to set the time when the period starts. The **Select** button lets you choose from the available peers or manage new peers.

! You can use wildcards for the names of the remote stations. The wild card "*" in this case applies for all remote stations.

In the fields **Day**, **Hour** and **Minute** you set the day of the month and the time at which the device resets the budget for this peer.

! By default the device resets the budget for all peers on the first day of the month at 00:00h.

! If you enter the value "31" in the field **Day**, the device does not reset the budget in months with fewer days (e.g. February or November).

5.1.5 Enhancements to LANmonitor

Show volume budget archive

Displays the volume budget archive of all WAN interfaces.

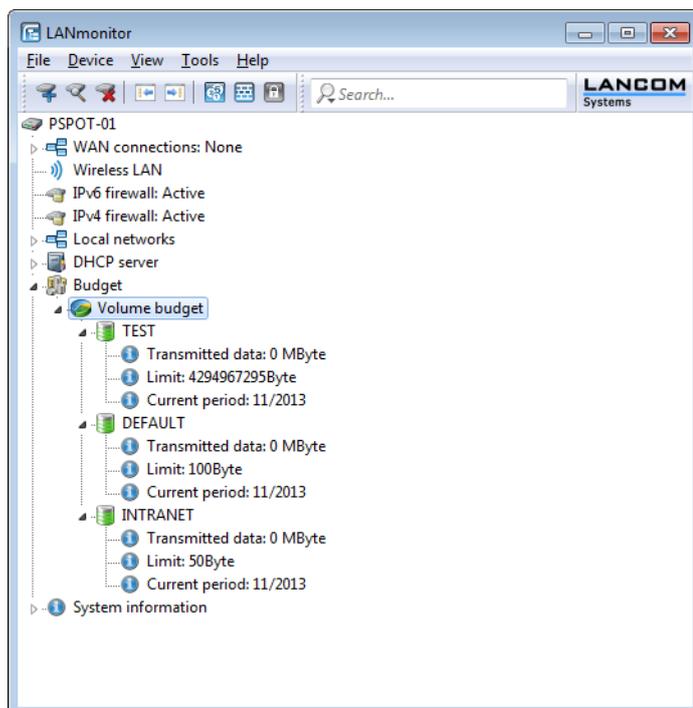
Peer (MByte)	Dec 12	Jan 13	Feb 13	Mar 13	Apr 13	May 13	Jun 13	Jul 13	Aug 13	Sep 13
TEST	0	0	0	0	0	0	0	0	0	0
DEFAULT	0	0	0	0	0	0	0	0	0	0
INTRANET	0	0	0	0	0	0	0	0	0	0

Budget analysis

Depending on your tariff plan, mobile or landline operators may activate bandwidth throttling if a certain data volume is exceeded, also for flatrate plans. The device captures the amount of data sent over each WAN interface, archives the values for up to 12 months, and can perform actions when a specified threshold is reached. The budgets also apply to VPN, PPTP, and all other types of connection.

At the change of the month, the device archives the data for the previous month and resets the counter to zero for the current month. You can view the current data volume and the archived information in LANmonitor or in the WEBconfig

status menu. The archive contains data from the last 12 months. In the 13th month, the device automatically overwrites the archive data of the 1st month.



By clicking with the right mouse button on **Volume budget** you can reset all of the displayed volume budgets or display the volume budget archive.

Peer (MByte)	Dec 12	Jan 13	Feb 13	Mar 13	Apr 13	May 13	Jun 13	Jul 13	Aug 13	Sep 13
TEST	0	0	0	0	0	0	0	0	0	0
DEFAULT	0	0	0	0	0	0	0	0	0	0
INTRANET	0	0	0	0	0	0	0	0	0	0

By clicking with the right mouse button on a WAN interface, you can reset the budget for the corresponding interface or assign an additional volume budget.

5.2 Script variable for dynamic IPv6 addresses

As of LCOS version 8.84, the variable %a for dynamic IPv4 addresses in DynDNS scripts or action-table scripts is now complemented by the variable %z for dynamic IPv6 addresses.

ⓘ Using the variable %z requires that you specify the IPv6 address. If you do not supply an address, the device will not execute the script.

New in the action table is the action prefix `dnscheck6 :`, with which you initiate an IPv6 DNS name resolution. For example, the action `dnscheck6 :myserver.dyndns.org` requests the IPv6 address of the indicated server.

5.3 Assign actions from the action table of a WAN connection

As of LCOS 8.84, actions in the action table can be executed on certain types of WAN connections from the LANCOM. Thus makes it possible, for example, for each WAN connection to use its own DynDNS provider.

5.3.1 Configuration

With the action table you can define actions that the LANCOM is to execute when the status of a WAN connection changes.

In LANconfig, the action table is located under **Communication > General > Action table**

- **Entry active:** Activates or deactivates this entry.
- **Name:** Action name. This name can be referenced with the wildcard %h (hostname) in the fields **Action** and **Result check**.
- **Remote site:** A change in status of this remote site triggers the action defined in this entry.
- **Routing tag:** You can use the routing tag to specify which remote site is used when the action is applied. Of course, this site must be equipped with the appropriate routing tag.
- **Lock time:** Prevents this action from being repeated within the period defined here in seconds (max. 10 characters).
- **Condition:** Various changes in WAN-connection status can be set here, and the action is triggered when this condition occurs. Possible values are:
 - Establish – the action triggers if the device has successfully established the connection.
 - Disconnect without failure – the action triggers if the device itself terminates the connection (e.g. through manual disconnection or expiry of a holding time).
 - End (disconnect or broken) – the action triggers as soon as the connection terminates (regardless of the reason).
 - Broken with failure – this action is triggered on disconnects that were not initiated or expected by the device.
 - Establish failure – the action triggers if connection establishment was unsuccessful.
 - Volume budget exhausted – this action executes when the specified volume is reached.

- Volume budget released – this action occurs after a state change from 'Volume exceeded' to 'Volume no longer exceeded', e.g. when you reset an exceeded volume or when the device enters a new billing period. If the volume has not been exceeded at the time of the reset, no action takes place.
- **Action:** This item describes the action to be executed by the device when there is a change in the status of the WAN connection. You can specify only one action per entry (max. 250 characters). For each of the following values, the colon (:) is part of the action value. Possible values are:
 - `exec` : – This prefix initiates any command as you would enter it at the Telnet console. For example, the action `exec : do /o/m/d` terminates all current connections.
 - `dnscheck` : – This prefix initiates an IPv4 DSN name resolution. For example, the action `dnscheck : myserver . dyndns . org` requests the IPv4 address of the indicated server.
 - `dnscheck6` : – This prefix initiates an IPv6 DSN name resolution. For example, the action `dnscheck6 : myserver . dyndns . org` requests the IPv6 address of the indicated server.
 - `http` : – This prefix initiates an HTTP-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org:

```
http://username:password@members.dyndns.org/nic/update?
system=dyndns&hostname=%h&myip=%a
```

The meaning of the place holders %h and %a is described below.

- `https` : – Like `http` : , except that the connection is encrypted.
- `gnudip` : – This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the GnuDIP protocol to execute a DynDNS update at a DynDNS provider:


```
gnudip://gnudipserver?method=top&user=myserver&domain=mydomain.org&pass=password&req=0&addr=%a
```

 The meaning of the place holder %a is described below.
- `repeat` : – This prefix together with a time in seconds repeats all actions with the condition "Establish" as soon as the connection has been established. For example, the action `repeat 300` causes all of the establish actions to be repeated every 5 minutes.
- `mailto` : – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator as soon as a connection is terminated:


```
mailto:admin@mycompany.com?subject=VPN connection broken at
?t?body=VPN connection to branch office 1 was broken.
```

Optional variables for the actions:

- %a – WAN IPv4 address of the WAN connection relating to the action.



Using the variable %z requires that you specify the IPv6 address. If you do not supply an address, the device will not execute the script.

- %z – WAN IPv6 address of the WAN connection relating to the action.
- %H – Host name of the WAN connection relating to the action.
- %h – Like %H, except the hostname is in small letters.
- %c – Connection name of the WAN connection relating to the action.
- %n – Device name
- %s – Device serial number
- %m – Device MAC address (as in Sysinfo)
- %t – Time and date in the format YYYY-MM-DD hh:mm:ss
- %e – Description of the error that was reported when connection establishment failed.

You can inspect the outcome of the actions in the field **Result check**.

- **Result check:** You can evaluate the result of the action here to determine the number of lines to be skipped in the processing of the action table. Possible values for the actions (max. 50 characters):
 - `contains=` – This prefix checks if the result of the action contains the defined string.
 - `isequal=` – This prefix checks if the result of the action is exactly equal to the defined string.

- `?skipiftrue=` – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is TRUE.
- `?skipiffalse=` – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is FALSE.

The optional variables for the actions are the same as for the actions above.

Example: A DNS check queries the IP address of an address in the form "myserver.dyndns.org". The check `contains=%a?skipiftrue=2` allows you to skip the two following entries in the action table if the IP address found by the DNS check agrees with the current IP address (%a) of the device.

- **Owner:** Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the device cannot execute the action.

5.3.2 Additions to the Setup menu

Routing tag

A routing tag is used to map actions in the action table to a specific WAN connection. The LANCOM performs the action over the connection indicated by this routing tag.

SNMP ID:

2.2.25.10

Telnet path:

Setup > WAN > Action-Table

Possible values:

Max. 5 characters from 0123456789

Default:

0

5.4 Selecting frequency bands in LTE cellular networks

As of LCOS 8.84, you can set the frequency bands to be used by a LANCOM 4G router for data transmissions in the LTE mobile network.

5.4.1 Enhancements to LANconfig

Selecting frequency bands in LTE cellular networks

Mobile profiles enable you to set which frequency bands the LTE/4G modem should use. Navigate to **Interfaces > WAN > Mobile settings**, .

If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result.

The selection under **LTE bands** allows you to control which frequency bands the mobile router can or should use. The following frequency bands are available:

- **2100 MHz (B1)**: 2.1GHz band is enabled.
- **1800 MHz (B3)**: 1.8GHz band is enabled.
- **2600 MHz (B7)**: 2.6GHz band is enabled.
- **900 MHz (B8)**: 900MHz band is enabled.
- **800 MHz (B20)**: 800MHz band is enabled.
- **All**: All frequency bands are enabled.

! This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

5.4.2 Additions to the Setup menu

LTE bands

If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result. This selection allows you to control which frequency bands the mobile router can or should use. The following frequency bands are available:

- **B1_2100**: 2.1GHz band is enabled.
- **B3_1800**: 1.8GHz band is enabled.
- **B7_2600**: 2.6GHz band is enabled.
- **B8_900**: 900MHz band is enabled.
- **B20_800**: 800MHz band is enabled.
- **All**: All frequency bands are enabled.

 This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

SNMP ID:

2.23.41.1.10

Telnet path:**Setup > Interfaces > Mobile > Profiles****Possible values:**

All

B1_2100

B3_1800

B7_2600

B8_900

B20_800

Default:

All

5.5 Forwarding data packets from LAN via X.25 (ISDN)

The TCP-X.25 bridge integrated in LCOS allows you to forward (and receive) data from a TCP/IP network via ISDN to an X.25 network. This gives you the option of setting up a backup connection in an X.25 network in case of disruption of the WAN connection.

The following steps show you how you configure the TCP-X.25 bridge on your device for these scenarios. This example is based on modern debit/credit card terminals which now commonly use only TCP/IP to communicate with a centralized server or network and in which at least two different IP addresses can be configured. On your terminal, enter your destination network or the destination server in the usual manner as the primary IP address and port. As the second IP address and port, enter the LANCOM where the terminal sends its data packets in the case that the primary destination is not available.

The LANCOM uses the settings stored in LCOS to check whether the respective data should be forwarded. If so, the device establishes a connection to the configured destination address via the ISDN interface and transparently forwards the TCP/IP data packets via X.25. The respective remote site must also be available via ISDN and support X.25.

 The number of logical connections via the TCP-X.25 bridge is currently limited to one. If the device receives another connection request while it already has an established connection, it will be ignored. In this case, the respective terminal must repeat its TCP connection requests until the other X.25 connection is disconnected.

1. Go to the console or open the table **WAN > X.25-Bridge > Outgoing calls** in the setup menu in WEBconfig.
2. Add a new data record and add the following basic information to the default settings. Please find further information about the parameters in the CLI guide or Menu Reference Guide.
 - **Name**
 - **Terminal-Port**
 - **Local-Port**
 - **Remote-ISDN**
 - **Local-ISDN**
 - **X.25-Remote**

- **X.25-Local**

! The **Terminal IP** and **Loopback address** are optional, but highly recommended for configurations with multiple local networks.

! For connections to some providers (e.g., **TeleCash**), it is also necessary to enter the **Protocol ID** and the **User data**.

That's it! This concludes the basic configuration of the TCP-X.25 bridge.

5.5.1 Additions to the Status menu

X.25 bridge

This menu contains the status values for the TCP-X.25 bridge.

SNMP ID:

1.4.45

Telnet path:

Status > WAN

connections

This table shows the list of all active connections via the TCP-X.25 bridge. This list shows the current states of the TCP, ISDN and X.25 components for a connection, as well as their connection parameters.

SNMP ID:

1.4.45.2

Telnet path:

Status > WAN > X.25-Bridge

Index

Number of the table entry.

SNMP ID:

1.4.45.2.1

Telnet path:

Status > WAN > X.25-Bridge > Connections

Direction

This displays the direction in which the connection over the TCP-X.25 bridge was established.

SNMP ID:

1.4.45.2.2

Telnet path:

Status > WAN > X.25-Bridge > Connections

Possible values:

Outgoing

Outgoing connection

TCP status

This displays the status of the TCP connection from your device to a LAN remote site (e.g., a terminal).

SNMP ID:

1.4.45.2.3

Telnet path:

Status > WAN > X.25-Bridge > Connections

Possible values:

Establish

Connected

Disconnect

Not connected

ISDN status

This displays the status of the ISDN connection from your device to the X.25 remote site (or its ISDN service).

SNMP ID:

1.4.45.2.4

Telnet path:

Status > WAN > X.25-Bridge > Connections

Possible values:

Establish

Connected

Disconnect

Not connected

X.25 status

This displays the status of the X.25 connection from your device to the X.25 remote site.

SNMP ID:

1.4.45.2.5

Telnet path:

Status > WAN > X.25-Bridge > Connections

Possible values:

Establish
Connected
Disconnect
Not connected

Terminal-IP

This displays the IP address of the LAN remote site (e.g., a terminal).

SNMP ID:

1.4.45.2.6

Telnet path:

Status > WAN > X.25-Bridge > Connections

Terminal-Port

This displays the port of the LAN remote site (e.g., of a terminal) used for the TCP connection.

SNMP ID:

1.4.45.2.7

Telnet path:

Status > WAN > X.25-Bridge > Connections

Local IP

This displays the LAN IP address of your device used to accept and send data packets via the TCP-X.25 bridge.

SNMP ID:

1.4.45.2.8

Telnet path:

Status > WAN > X.25-Bridge > Connections

Local-Port

It displays the port on your device where the TCP connection to the LAN remote site is located.

SNMP ID:

1.4.45.2.9

Telnet path:

Status > WAN > X.25-Bridge > Connections

Routing tag

This displays the source tag (expected interface or routing tag) of the ARF context of the respective connection.

SNMP ID:

1.4.45.2.10

Telnet path:

Status > WAN > X.25-Bridge > Connections

ISDN-Remote

This displays the ISDN phone number of the X.25 remote site (or its ISDN service).

SNMP ID:

1.4.45.2.11

Telnet path:

Status > WAN > X.25-Bridge > Connections

ISDN-Local

This displays the ISDN phone number of your device.

SNMP ID:

1.4.45.2.12

Telnet path:

Status > WAN > X.25-Bridge > Connections

X.25-Remote

It displays the X.25 address of the X.25 remote site.

SNMP ID:

1.4.45.2.13

Telnet path:

Status > WAN > X.25-Bridge > Connections

X.25-Local

This displays the X.25 address of your device.

SNMP ID:

1.4.45.2.14

Telnet path:

Status > WAN > X.25-Bridge > Connections

Protocol-ID

This displays the X.25 protocol number that was configured for this connection. For outgoing connections, this is the protocol number that is stored in LCOS.

SNMP ID:

1.4.45.2.15

Telnet path:**Status > WAN > X.25-Bridge > Connections****User data**

This displays the X.25 user data transmitted for this connection. For outgoing connections, this is the user data that is stored in LCOS.

SNMP ID:

1.4.45.2.16

Telnet path:**Status > WAN > X.25-Bridge > Connections****Payload-Size**

This displays the size of the X.25 payload negotiated for this connection.

When establishing the connection, the device initially transmits the size configured in LCOS. The remote site can change the value. If it makes changes, the status value shows the modified payload, otherwise it shows the one configured in LCOS.



The X.25 standard makes it possible to specify different sizes for sent and received packets. The status value only shows the size of the packets that were sent by the device.

SNMP ID:

1.4.45.2.17

Telnet path:**Status > WAN > X.25-Bridge > Connections****TCP ports**

This table shows the list of all local ports that your device checks for incoming TCP connections for the TCP-X.25 bridge (TCP Listener). If the table contains a valid configuration line for a port, [2.2.45.2 Outgoing-Calls](#) on page 44 the device accepts the TCP connection; otherwise it rejects the connection request via the TCP X.25 bridge.

SNMP ID:

1.4.45.3

Telnet path:**Status > WAN > X.25-Bridge****Local-Port**

Number of the port that your device checks for incoming TCP connections for the TCP-X.25 bridge (TCP Listener).

SNMP ID:

1.4.45.3.1

Telnet path:**Status > WAN > X.25-Bridge > TCP-Ports****Disconnect**

With this action you trigger the immediate disconnection of the X.25 connection and close the associated ISDN channels.

SNMP ID:

1.4.45.4

Telnet path:**Status > WAN > X.25-Bridge****Possible arguments:***none*

5.5.2 Additions to the Setup menu

X.25 bridge

This menu contains the settings for the TCP-X.25 bridge.

SNMP ID:

2.2.45

Telnet path:**Setup > WAN**

Outgoing-Calls

This table contains the settings for the incoming TCP connections (of the LAN remote site) and outgoing X.25 connections (for the X.25 remote site).

SNMP ID:

2.2.45.2

Telnet path:**Setup > WAN > X.25-Bridge****Name**

Enter a name for the table entry or the X.25 connection that has to be configured.

SNMP ID:

2.2.45.2.1

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

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

Default:

DEFAULT

Prio

Specify the priority of the selected X.25 connection. The lower the value, the higher the priority.

 LCOS sorts the displayed table entries in descending order according to the priorities.

SNMP ID:

2.2.45.2.2

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

0 ... 65535

Default:

0

Terminal-IP

Enter the IPv4 address of the remote site in your LAN to be used to send data packets over the selected X.25 connection.

SNMP ID:

2.2.45.2.3

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

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

Special values:**0.0.0.0**

The TCP-X.25 bridge can be used for all remote sites, not only those in your LAN but also those from the WAN.

Default:

0.0.0.0

Terminal-Port

Enter the port of the remote site in your LAN that the remote site can use to send data packets.

SNMP ID:

2.2.45.2.4

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls**

Possible values:

0 ... 65535

Special values:

0

The TCP-X.25 bridge allows connections using any port.

Default:

0

Loopback address

Specify the IPv4 address, which has an ARF context used by your device to receive connections from the terminal. The loopback address replaces the entries for IP address and routing tag. The device selects the routing tag and its local address based on the loopback address. If the loopback address is empty, the device accepts connections on any address (even the WAN!).

SNMP ID:

2.2.45.2.5

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

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

Default:*empty***Local-Port**

Enter the TCP port which your device uses to make a connection to the X.25 remote site.

SNMP ID:

2.2.45.2.6

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

1 ... 65535

Default:

1998

ISDN-Remote

Enter the ISDN phone number of the X.25 remote site.

SNMP ID:

2.2.45.2.7

Telnet path:

Setup > WAN > X.25-Bridge > Outgoing-Calls

Possible values:

Max. 21 characters [0–9]

Default:

0

ISDN-Local

Enter the ISDN phone number that your device uses as its outgoing number.

SNMP ID:

2.2.45.2.8

Telnet path:

Setup > WAN > X.25-Bridge > Outgoing-Calls

Possible values:

Max. 21 characters [0–9]

Default:

empty

X.25-Remote

Enter the X.25 address of the X.25 remote site.

SNMP ID:

2.2.45.2.9

Telnet path:

Setup > WAN > X.25-Bridge > Outgoing-Calls

Possible values:

Max. 14 characters [0–9]

Default:

empty

X.25-Local

Enter the X.25 address of the device.

SNMP ID:

2.2.45.2.10

Telnet path:

Setup > WAN > X.25-Bridge > Outgoing-Calls

Possible values:

Max. 14 characters [0–9]

Default:*empty***Protocol-ID**Enter the X.25 protocol number. Your device enters this ID as bytes 0 to 3 in the X.25 *User data* .**SNMP ID:**

2.2.45.2.11

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

Max. 8 characters [0–9] [a–f]

Default:

00000000

User data

You can store additional information in the X.25 data packets that your device transmits to the X.25 remote site.

SNMP ID:

2.2.45.2.12

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls****Possible values:**

Max. 8 characters [A–Z] [a–z] [0–9] @ { | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ . ` #

Default:*empty***Payload-Size**

Specify the size of the X.25 payload. Valid values are powers of two between 16 and 1024.



The X.-25 standard allows different settings for the sizes of sent and received packets. The configuration relates to both directions.

SNMP ID:

2.2.45.2.13

Telnet path:**Setup > WAN > X.25-Bridge > Outgoing-Calls**

Possible values:

16 ... 1024 Bytes

Default:

128

Data trace

This parameter enables and disables the tracing of data packets that pass the X.25 bridge. The trace is output on the console where you enabled the trace.

SNMP ID:

2.2.45.5

Telnet path:**Setup > WAN > X.25-Bridge****Possible values:****Off**

The device does not output any traces.

On

The device does not output any trace data in the direction of the transmission and the number of the data bytes. Example of a data trace:

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.
```

Advanced

Identical to **On**, although the device additionally outputs the data as a dump. Example for a data trace with added dump output (excerpt):

```
[X.25-Bridge] 2014/01/15 13:55:39,331
Receiving 256 bytes of data from X.25.

Adr:= 04394380
Len:= 00000100
00000000: C2 79 .. 46 60 50 8C .. E3 B7 | .6y..GF` P.....
00000010: 2D AE .. 24 5D E9 B6 .. 40 59 | -.0..U$] ..l..g@Y
00000030: A5 36 .. 3C 6B 01 21 .. 9D 14 | .6.M..<k !H..u..
00000040: 94 38 .. 89 AA 54 22 .. 81 F7 | .8..2m.. T".=....
00000050: E0 7C .. F3 28 B6 E8 .. 74 2F | .|.....( ..a]b.t/
[...]
```

Default:

Off

Disconnect delay

Using these parameters you define the time that the device waits after establishing the X.25 connection before it disconnects the ISDN connection. Within this time period no other X.25 connections can be established without completely re-establishing the ISDN connection.

SNMP ID:

2.2.45.4

Telnet path:**Setup > WAN > X.25-Bridge****Possible values:**

0 ... 99 Seconds

Special values:**0**

This parameter disables the waiting period. The device disconnects ISDN connections in conjunction with the X.25 connection.

Default:

5

5.6 HNAT tracing

As of LCOS 8.84 a new trace command is available for troubleshooting on devices with hardware NAT (HNAT):

Table 1: Overview of all possible traces

This parametercauses the following message in the trace:
hnat	Information on hardware NAT

The current status information about HNAT can be displayed with the command `show eth hnat`.

6 IPv6

6.1 IPv6 prefix delegation from the WWAN to the LAN

As of LCOS 8.84, the WWAN router can communicate an IPv6/64 prefix to the LAN by means of DHCPv6 or router advertising.

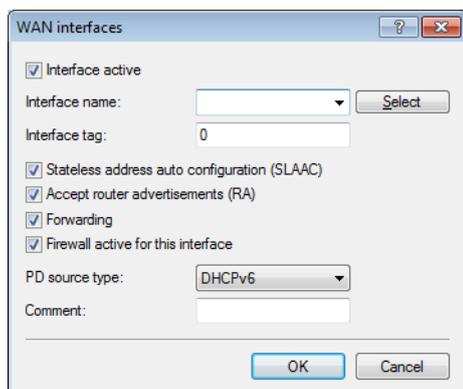
6.1.1 Enhancements to LANconfig

IPv6 prefix delegation from the WWAN to the LAN

For cellular networks with IPv6 support, the support of DHCPv6 prefix delegation is only expected to be provided with 3GPP Release 10. So for cellular networks earlier than Release 10, the only way to assign just one /64 prefix to a terminal device is, for example, by using router advertisements. In the case of smartphones or laptops, this method allows IPv6 support to be implemented relatively simply. However, each IPv6 router needs at least one additional prefix that it can propagate to clients on the LAN.

IPv6 prefix delegation from the WWAN into the LAN makes it possible for clients to use the /64 prefix, as assigned on the WAN cellular network side, to be used on the LAN. This makes it possible to operate a router in an IPv6 cellular network without DHCPv6 prefix delegation and neighbor discovery proxy (ND proxy). The router announces the assigned /64 prefix by router advertisement on the LAN, rather than adding it at the WAN interface. Clients can then generate an address from this prefix and use it for IPv6 communication.

To do this, you configure the IPv6 Internet access in the normal way. Additionally you should go to **IPv6 > General > IPv6 interfaces > WAN interface** and, for the corresponding WAN interface, switch the parameter **PD source type** from "DHCPv6" to "Router advertisement".



The following restrictions apply:

- You can only use the feature on point-to-point connections (such as PPP), whereby the remote station automatically sends all traffic to the router because there is no ND proxy.
- You can create only one IPv6 network in the LAN, because only one /64 prefix is available.
- This feature is not suitable for scenarios where an interim router cannot or does not perform prefix delegation, with the exception of point-to-point connections.
- The automatically generated IPv6 address on the WAN interface cannot be reached from clients on the LAN, because there is no ND proxy.

6.1.2 Additions to the Setup menu

PD mode

For cellular networks with IPv6 support, the support of DHCPv6 prefix delegation is only expected to be provided with 3GPP Release 10. So for cellular networks earlier than Release 10, the only way to assign just one /64 prefix to a terminal device is, for example, by using router advertisements. In the case of smartphones or laptops, this method allows IPv6 support to be implemented relatively simply. However, each IPv6 router needs at least one additional prefix that it can propagate to clients on the LAN.

IPv6 prefix delegation from the WWAN into the LAN makes it possible for clients to use the /64 prefix, as assigned on the WAN cellular network side, to be used on the LAN. This makes it possible to operate a router in an IPv6 cellular network without DHCPv6 prefix delegation and neighbor discovery proxy (ND proxy). The router announces the assigned /64 prefix by router advertisement on the LAN, rather than adding it at the WAN interface. Clients can then generate an address from this prefix and use it for IPv6 communication.

This option allows you to set the way in which the router performs the prefix delegation:

- DHCPv6: Prefix delegation via DHCPv6
- Router advertisement: Prefix delegation via router advertisement, in which case the DHCPv6 client is not activated.

Telnet path:

Setup > IPv6 > WAN-Interfaces

Possible values:

DHCPv6

Router advertisement

Default:

DHCPv6

7 Certificate Management

7.1 Using internal LCOS variables in the SCEP client

As of LCOS version 8.84, the SCEP client can also use these internal LCOS variables:

- %% inserts a percent sign.
- %f inserts the version and the date of the firmware currently active in the device.
- %r inserts the hardware release of the device.
- %v inserts the version of the loader currently active in the device.
- %m inserts the MAC address of the device.
- %s inserts the serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

8 WLAN

8.1 LANCOM Active Radio Control (ARC)

The intelligent WLAN optimization concept behind **LANCOM Active Radio Control (ARC)** helps you to sustainably optimize your radio field and proactively avoid sources of interference on the WLAN. Active Radio Control consists of numerous complementary functions in the LANCOM operating system LCOS, which combine to significantly improve the performance of your WLAN. All of the features in Active Radio Control are included for free in the LANCOM operating system LCOS and they are easy to operate with the appropriate management tools.

RF optimization

Automatic selection of optimum WLAN channels: WLAN clients benefit from improved throughput thanks to reduced channel overlap. In controller-based WLAN installations, the optimal channels are selected automatically for managed access points.

For more information about RF optimization, see the relevant section of the Reference Manual.

Band steering

Make optimal use of your WLAN's bandwidth: Automatically controlled by the access point, clients steered to the 5-GHz frequency band can effectively double the WLAN performance because only here are sufficient channels available for channel bundling.

For more information about band steering, see the relevant section of the Reference Manual.

Adaptive noise immunity

Better WLAN throughput thanks to immunity to interfering signals: WLAN clients benefit from significantly improved data throughput thanks to interference-free signal coverage. Enabling the adaptive noise immunity allows an access point to block out interfering signals and to focus exclusively on WLAN clients with sufficient signal strength.

For more information about adaptive noise immunity, [see the relevant section](#) of the Reference Manual.

Spectral scan

Check your WLAN radio spectrum for sources of interference: With LANCOM Spectral Scan, you have a professional tool for efficient WLAN troubleshooting. A scan of the entire radio spectrum identifies sources of interference from outside the WLAN and allows a graphical representation.

For more information about spectral scanning, see the relevant section of the Reference Manual.

8.2 Maximum EIRP value depends on the transmission standard

In order to comply with the maximum transmission power density defined by the 802.11b transmission standard, the maximum available EIRP value is 18dBm. For the 802.11gn transmission standard, the EIRP value may not exceed 20dBm. As of LCOS 8.84, the maximum EIRP value for any WLAN-enabled device from LANCOM automatically concurs with the applicable transmission standard.

8.3 Adjusting the maximum transmit rate for multicasts and broadcasts

As of LCOS 8.84, the LANCOM can automatically adjust the broadcast and multicast transmission rates to that of the access point with the lowest transmission rate.

8.3.1 Automatic adjustment of multicast and broadcast transmission rates

Whereas with unicast broadcasts the access point and client can negotiate the optimum transfer rate between them, multicast and broadcast transmissions communicate in just one direction: From the access point to the client. The clients cannot report back the access point with their actual maximum transmission speeds.

The access point has two options for setting the transmission rate for multicast and broadcast transmissions:

- **Fixed bit rate:** The transfer rate is set so that the slowest client in the WLAN can receive error-free transmissions even under unfavorable conditions. This can lead to the situation that the LANCOM transmits at a lower rate than environmental conditions and the clients would actually allow. As a result, the access point slows down the communications in the WLAN unnecessarily.
- **Automatic bit rate:** By setting the transmission rate to auto, the access point collects information about the transmission rates of the various WLAN clients. Clients automatically notify the access point of this rate with each unicast communication. The access point takes the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

8.3.2 Additions to the Setup menu

Basic rate

The basic rate is the transmission rate used by the LANCOM to send multicast and broadcast packets.

The rate defined here should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached at this speed.

If you choose "Auto", the device automatically matches the transmission rate to the slowest WLAN client on your network.

SNMP ID:

2.23.20.2.4

Telnet path:

Setup > Interfaces > WLAN > Transmission

Possible values:

Auto

Select from the available speeds between 1Mbps and 54Mbps

Default:

2Mbps

8.3.3 Additions to the Status menu

Networks

Displays information about the WLAN interfaces of the device.

SNMP ID:

1.3.56

Telnet path:**Status > WLAN****Ifc**

The name of the interface

Operating

Indicates whether the interface is enabled.

Network name

Displays the name of the network (SSID)

BSSID

MAC address of the access point for this WLAN

Radio mode

Displays the data transfer standard being used by the access point.

VLAN ID

Displays the VLAN ID of the interface.

Num. stations

Indicates how many stations are currently logged on to the access point.

MCast-Pwr-Save

Indicates whether the power-save mode is enabled.

APSD

Indicates whether APSD is activated or deactivated for the respective WLAN (SSID). APSD is only indicated as active if it is activated in the settings for the logical WLAN and also if the general QoS module is activated.

Alarm state

Displays the alarm state of the interface.

Basic rate

Indicates the transmission rate for multicast and broadcast transmissions.

MAC filter

Indicates whether the MAC filter is enabled.

Access mode

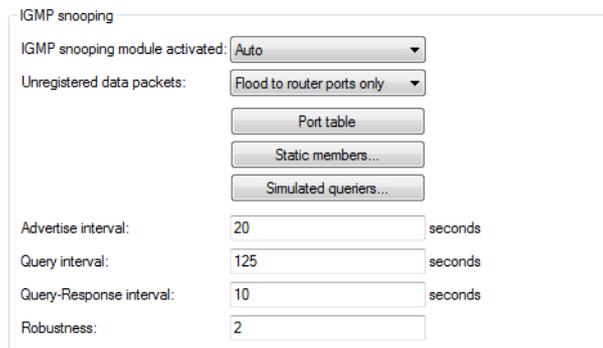
Indicates whether the access point blocks or approves the stations entered in the access list.

8.4 IGMP snooping in auto mode

As of LCOS version 8.84, the bridge can automatically detect whether there is at least one querier in the network. Only then can it learn the multicast-group memberships and forward the multicasts accordingly.

8.4.1 General settings

The configuration of the IGMP snooping in LANconfig is located under **Interfaces > IGMP snooping**



IGMP snooping

IGMP snooping module activated: Auto

Unregistered data packets: Flood to router ports only

Port table

Static members...

Simulated queriers...

Advertise interval: 20 seconds

Query interval: 125 seconds

Query-Response interval: 10 seconds

Robustness: 2

IGMP snooping module activated

Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

Possible values:

- Yes
- No
- Automatic

Default:

- Automatic

With the setting **Auto**, the bridge only activates the IGMP snooping when there are also queriers in the network.



If this function is deactivated, the bridge sends all IP multicast packets on all ports. If there is a change of operating state, the bridge completely resets the IGMP snooping function, i.e. it clears all dynamically learned values (memberships, router port properties).

Unregistered data packets

This setting defines the handling of multicast data packets with a destination address outside the 224 . 0 . 0 . x range and for which neither static memberships were defined nor were dynamic memberships learned.

Possible values:

- Flood to router ports only: Sends these packets to all router ports.
- Flood to all ports: Sends these packets to all ports.
- Drop: Drops these packets.

Default:

- Router ports only

Advertise interval

The interval in seconds in which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries.

Possible values:

- 4 to 180 seconds

Default:

- 20

Query interval

Interval in seconds in which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224 . 0 . 0 . 1, so prompting the stations to transmit return messages about multicast group memberships. These regular queries influence the time in which the bridge ages, expires, and are deletes the multicast group memberships.

- After the startup phase, the querier sends IGMP queries in this interval.
- A querier returns to the querier status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".
- A port loses its router-port status after a time equal to "Robustness*Query-Interval+(Query-Response-Interval/2)".

Possible values:

- 10-figure number greater than 0.

Default:

- 125



The query interval must be greater than the query response interval.

Query response interval

Interval in seconds influencing the timing between IGMP queries and router-port aging and/or memberships.

Interval in seconds in which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which multicast group memberships are "aged" and then deleted.

Possible values:

- 10-figure number greater than 0.

Default:

- 10



The query response interval must be less than the query interval.

Robustness

This value defined the robustness of the IGMP protocol. This option tolerates packet losses of IGMP queries with respect to Join messages.

Possible values:

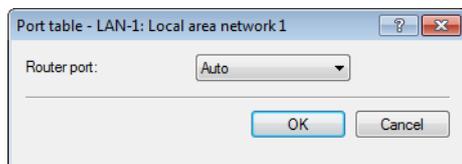
- 10-figure number greater than 0.

Default:

- 2

8.4.2 Port settings

This table is used to define the port-related settings for IGMP snooping.



Port

The port for which the settings apply.

Possible values:

- Selects a port from the list of those available in the device.

Default:

- N/A

Router port

This option defines the port's behavior.

Possible values:

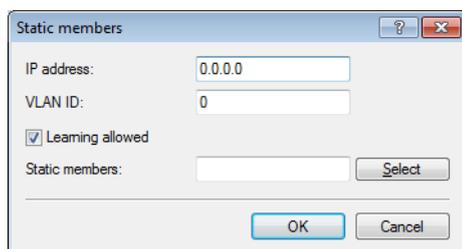
- Yes: This port will always work as a router port, irrespective of IGMP queries or router messages that the bridge receives at this port.
- No: This port will never work as a router port, irrespective of IGMP queries or router messages that the bridge receives at this port.
- Automatic: This port will work as a router port if IGMP queries or router messages are received. The port loses this status if the bridge receives no packets for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

Default:

- Automatic

8.4.3 Static members

This table enables members to be defined manually, for example if they cannot or should not be learned automatically.



IP address

The IP address of the manually defined multicast group.

Possible values:

- Valid IP multicast address.

Default:

- 0.0.0.0

VLAN-ID

The VLAN ID to which the bridge applies this static membership. You can enter multiple entries with different VLAN IDs for each IP multicast address.

Possible values:

- 0 to 4096.

Default:

- 0

Special values:

- If "0" is selected as VLAN, the IGMP queries are sent without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

Learning allowed

This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, the bridge only sends packets via the ports which have been manually defined for the multicast group.

Possible values:

- Activated
- Deactivated

Default:

- Activated

Static members

The bridge will always send packets with the corresponding IP multicast address to these ports, irrespective of any Join messages received.

Possible values:

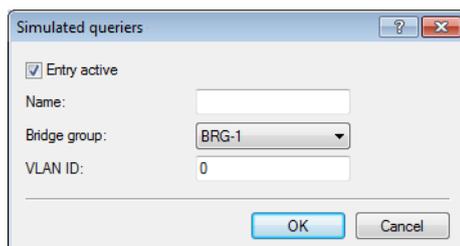
- Comma-separated list of the desired ports, max. 215 alphanumerical characters.

Default:

- Blank

8.4.4 Simulated queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP snooping functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs if you define multiple independent queriers to support the corresponding VLAN IDs.



Entry active

Activates or deactivates the querier instance

Possible values:

- Activated
- Deactivated

Default:

- Activated

Name

Name of the querier instance

Possible values:

- 8 alphanumerical characters.

Default:

- Blank

Bridge group

Limits the querier instance to a certain bridge group.

Possible values:

- Select from the list of available bridge groups.
- None

Default:

- BRG-1

Special values:

- If bridge group is set to "none", the bridge sends all IGMP queries via all bridge groups.

VLAN-ID

Limits the querier instance to a certain VLAN.

Possible values:

- 0 to 4096

Default:

- 0

Special values:

- If the VLAN ID is set to "0", the bridge sends the IGMP requests without a VLAN tag. For this reason, this value only makes sense when VLAN is deactivated in general.

8.4.5 Additions to the Setup menu

Operating

Activates or deactivates IGMP snooping in the device and all of the defined querier instances. Without IGMP snooping the bridge functions like a simple switch and forwards all multicasts to all ports.

 If this function is deactivated, the bridge sends all IP multicast packets on all ports. If there is a change of operating state, the device completely resets the IGMP snooping function, i.e. it clears all dynamically learned values (memberships, router port properties).

SNMP ID:

2.20.30.1

Telnet path:**Setup > LAN-Bridge > IGMP-Snooping****Possible values:**

No

Yes

Auto

Default:

No

8.5 Converting DHCP responses from broadcast into unicast

To deliver DHCP responses in the WLAN more reliably, LCOS 8.84 and later gives you the option of converting data packets sent from the device as a broadcast (which have no specific addressee, no optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and a low data rate) into unicast packets.

In LANconfig, the setting **Convert broadcast DHCP responses to unicast** is available in the dialog **Wireless LAN > General > Logical WLAN settings > WLAN network [...] > Transmission**.

 This function is already an integral part of the setting **Only transmit unicasts, suppress broadcast and multicasts** and does not need to be activated explicitly.

8.5.1 Additions to the Setup menu

Convert to unicast

Using this parameter you specify which type of data packets, which have been sent as a broadcast, are automatically converted into unicast by the device within a WLAN network.

SNMP ID:

2.23.20.2.25

Telnet path:**Setup > Interfaces > WLAN > Transmission****Possible values:**

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

Default:

DHCP

8.6 Adaptive noise immunity to reduce interference on the WLAN

As of LCOS version 8.84, LANCOM access points are equipped with adaptive noise immunity (ANI), which compensates for various types of interference on the wireless network.

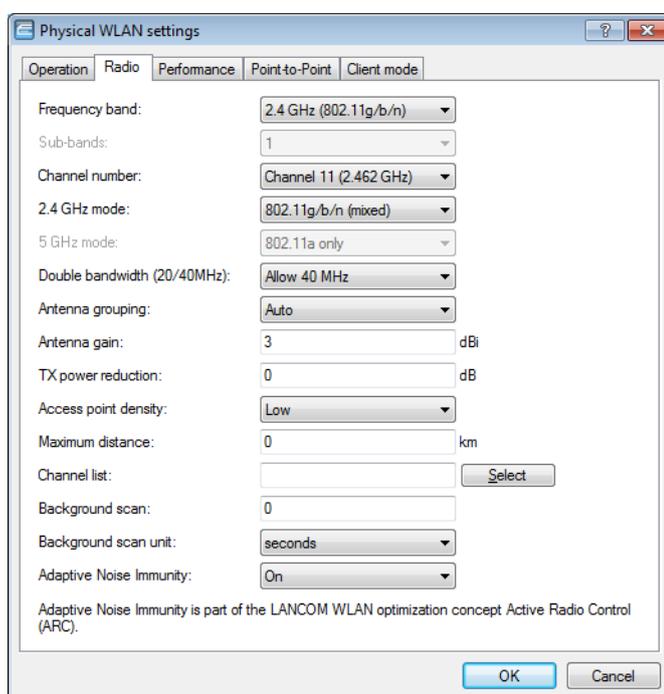
8.6.1 Enhancements to LANconfig

Adaptive noise immunity for reducing interference on the WLAN

A wireless LAN can be subjected to interference from various sources. Devices such as microwave ovens or cordless phones interfere with data transmission, and even the network devices themselves can emit interference and hinder communications. Each type of interference has its own characteristics. Adaptive noise immunity (ANI) enables the access point to use different error conditions to determine the best way to compensate for the interference. By automatically increasing noise immunity, the size of the radio cell can be reduced to mitigate the impact of interference on the data transfer.

The current values and any previous actions are to be found in WEBconfig under **Status > WLAN > Noise-Immunity**.

You can enable adaptive noise immunity in LANconfig under **Wireless LAN > General > Interfaces > Physical WLAN settings > Radio**.



To enable the adaptive noise immunity function, go to the Radio tab and set the value in the selection field **Adaptive noise immunity** to "On".

! Adaptive noise immunity is a component of [LANCOM Active Radio Control \(ARC\)](#)

8.6.2 Additions to the Setup menu

Adaptive noise immunity

A wireless LAN can be subjected to interference from various sources. Devices such as microwave ovens or cordless phones interfere with data transmission, and even the network devices themselves can emit interference and hinder communications. Each type of interference has its own characteristics. Adaptive noise immunity (ANI) enables the access point to use different error conditions to determine the best way to compensate for the interference. By automatically increasing noise immunity, the size of the radio cell can be reduced to mitigate the impact of interference on the data transfer.

The current values and any previous actions are to be found under **Status > WLAN > Noise-Immunity**.

SNMP ID:

2.23.20.8.23

Telnet path:**Setup > Interfaces > WLAN > Radio-settings****Possible values:**

No

Yes

Default:

Yes

8.6.3 Additions to the Status menu

Noise immunity

This directory contains current measurements of the WLAN values and the records of past events.

SNMP ID:

1.3.63

Telnet path:**Status > WLAN**

Current parameters

This table shows the current ANI parameters for all bands and radio channels.



If adaptive noise immunity is disabled, the table contains either the default values after the initialization of the WLAN interface or the manually preset values.

SNMP ID:

1.3.63.1

Telnet path:**Status > WLAN > Noise-immunity****Band**

Indicates the radio band on which the access point is measuring the current parameters. Possible values are:

- 2.4 GHz
- 5 GHz

Radio channel

Displays the radio channels available in the corresponding band.

Interface

Indicates the WLAN interface on which the access point is measuring the current parameters.

Age

Indicates the age of the measurement.

Noise immunity level

Shows the level of noise immunity. The higher the value, the more "immune" the access point is to interference. The range of values depends on the radio module being used.

Spurious immunity level

Parameter for internal use by the WLAN module.

Fir step level

Parameter for internal use by the WLAN module.

OFDM weak signal detection

Parameter for internal use by the WLAN module.

CCK weak signal detection threshold

Parameter for internal use by the WLAN module.

MRC-CCK

Parameter for internal use by the WLAN module.

The range of values for the individual measurements depends on the radio module being used. Information about which radio module is installed in your device is displayed in the status menu **WLAN > Interfaces > Card ID**.

Radio module chipset	Noise immunity	OFDM weak signal detection	CCK weak signal detection threshold	Fir step level	Spurious immunity	MRC-CCK
AR5212/5213/2414/5414	0 to 4	0, 1	0, 1	0 to 3	0 to 7	Blank
AR9160/9280	0 to 4	0, 1	0, 1	0 to 3	0 to 7	Blank
AR9380/9382/9390	Blank	0, 1	0, 1	0 to 8	0 to 7	0, 1

Log table

This table shows the recorded ANI events per band, channel and WLAN interface.

Under extreme conditions (very strong or very weak interference) the parameters can reach their maximum values. Even if the interference levels change within these extremes, the access point writes this maximum value to the table just once.

SNMP ID:

1.3.63.2

Telnet path:

Status > WLAN > Noise-immunity

Index

Contains the sequential number of the entry

Time

The time of the log entry.

Interface

Displays the WLAN interface where the event or action occurred.

Band

Shows the band that the event applied to.

Radio channel

Shows the radio channel that the event applied to.

Event

Displays the changes to the ANI parameters. Possible values are:

- Min. immunity:
- Value change:

Parameters

Parameter for internal use by the WLAN module.

Value

Parameter for internal use by the WLAN module.

8.7 Opportunistic key caching

As of version 8.84, LCOS uses opportunistic key caching to facilitate WPA2-Enterprise encryption and speed up WLAN roaming.

8.7.1 Opportunistic key caching (OKC)

Authentication of wireless clients using EAP and 802.11X has become standard in corporate networks, and these methods are becoming even more widespread with the integration of the Hotspot 2.0 specification for public Internet access. The disadvantage of 802.11X authentication is the significantly longer time between login and connection, because up to twelve data packets have to be exchanged between the WLAN client and the access point. For most applications, which are all about data exchange, this may not be particularly important. However, for time-critical applications such as Voice over IP, it is important that the authentication at neighboring WLAN radio cells does not affect communication.

To counteract this, authentication strategies such as PMK caching and pre-authentication have become established, although pre-authentication does not fix all of the problems. On the one hand, there is no guarantee that the WLAN client can recognize whether the access point can perform pre-authentication. On the other hand, pre-authentication causes considerable load on the RADIUS server, which needs to handle the authentication of all clients and all access points in the WLAN.

Opportunistic key caching delegates the key management to a WLAN controller, or to a central switch, which manages all of the access points in the network. If a client logs on to an access point, the WLAN controller behind it works as an authenticator to manage the keys and send the PMK to the access point, which is ultimately received by the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID. It then send this to the new access point in the hope that OKC is enabled there (therefore "opportunistic"). If the access point cannot handle the PMKID, then it negotiates an 802.11X authentication with the client in the usual manner.

A LANCOM access point can even perform OKC if the WLAN controller is temporarily unavailable. In this case, it stores the PMK and sends this to the WLAN controller when it becomes available again. Ultimately it sends the PMK to all of the access points in the network, which allows clients to use OKC to login after a change of radio cell.

8.7.2 Enhancements to LANconfig

Logical WLAN networks

Under **WLAN Controller > Profiles > Logical WLAN networks** you can set the logical WLAN network parameters, which the WLAN controller is to assign to the access points. The following parameters can be defined for each logical WLAN network:

Logical WLAN network activated

Enable the logical WLAN network by clicking on this option.

Name

Here, specify a name which uniquely identifies the logical WLAN network.

Inheritance

If you wish to create entries that differ only slightly from existing ones, you can choose a "parent" entry here and select the parameters which are to be applied each time it is used.

! A "parent" entry itself can contain inherited entries. Try to ensure that the structure of inherited entries is not too complex, otherwise they may be difficult to understand and configure.

Network name (SSID)

Enter the SSID of the WLAN network here. All stations that belong to this WLAN network must use the same SSID.

SSID connect to

Here you select which of the access point's logical interfaces is to be associated with the SSID, i.e. where the access point sends the data packets for this SSID.

- "LAN": The access point forwards the data packets locally into the LAN (LAN-1) by default. It must be configured appropriately to do this.
- "WLC-Tunnel-x": The SSID is connected to a WLC bridge layer-3 tunnel. The access point sends all data packets to this tunnel and thus to the WLC. This tunnel must be configured on the WLC.

 Note that although forwarding all data packets to the WLC allows you to define routes and filters centrally, this creates a heavy load on the WLAN controller. This model demands a correspondingly high bandwidth in order to transfer all of the data traffic of this and any other SSIDs that are connected to this WLAN controller via WLC tunnel.

VLAN mode

This item sets the access point VLAN mode for packets belonging to this WLAN network (SSID). VLAN IDs are used if the VLAN module is enabled in the physical WLAN parameters of the access point. Otherwise the access point ignores all VLAN settings in the logical networks. Even with VLAN activated, it is possible to operate the network untagged.

- "Untagged": The access point does not tag data packets from this SSID with a VLAN ID.

 Even with VLAN activated, it is possible to operate a WLAN network untagged. The VLAN ID '1' is reserved internally for this.

- "Tagged": The access point marks the data packets with the VLAN ID specified as follows.

VLAN-ID

VLAN ID for this logical WLAN network

 Please note that to use VLAN IDs in a logical WLAN network, you must set up a management VLAN ID (see physical WLAN parameters).

Encryption

This item sets the encryption method or, in the case of WEP, the key length for packet encryption in this WLAN.

Key 1/passphrase

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "0x". The following character string lengths result for the formats used:

- WPA-PSK: 8 to 63 ASCII characters
- WEP128 (104 bit): 13 ASCII or 26 hex characters
- WEP64 (40 bit): 5 ASCII or 10 hex characters

RADIUS profile

Specify which RADIUS profile the access point should receive for this network, so that it can connect directly to the RADIUS server if necessary. Leave this field blank if the WLAN controller is to handle RADIUS requests.

 You configure the RADIUS profiles in the corresponding table.

Allowed frequency bands

Here you set the frequency band used by network participants for transmitting data on the wireless network. You can select the 2.4-GHz band, the 5-GHz band, or both bands.

AP standalone time

The time in minutes that a managed-mode access point continues to operate in its current configuration.

The configuration is provided to the access point by the WLAN controller and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN

controller be interrupted, the access point will continue to operate with the configuration stored in flash for the time period entered here. The access point can also continue to work with this flash configuration after a local power outage.

If there is no connection to the WLAN controller after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLAN controller is available, the WLAN controller transmits the configuration to the access point again.

This represents an effective measure against theft as the access point deletes all security-related configuration parameters after this time has expired.

 If the access point establishes a backup connection to a secondary WLAN controller, then the countdown to the expiry of standalone operation is halted. The access point and its WLAN networks remain active as long as it has a connection to a WLAN controller.

 Please note that the access point only deletes the configuration in flash memory after the time for standalone operation has expired, and not when the power is lost!

802.11u network profile

Select the Hotspot 2.0 profile from the list.

OKC activated

This option enables the opportunistic key caching. OKC makes it easy for WLAN clients to quickly and conveniently roam between WLAN cells in wireless environments with WPA2-Enterprise encryption.

MAC check activated

The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (**Wireless LAN > Stations > Stations**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

Suppress SSID broadcast

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

- **No:** The access point publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes:** The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID.
- **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond.

 Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

RADIUS accounting activated

Select this option if you want to enable the RADIUS accounting in this logical WLAN network.

Allow traffic between stations of this SSID

Check this option if all stations logged on to this SSID are to be able to communicate with one another.

WPA version

Here you select which WPA version the access point is to offer to the WLAN clients for encryption.

- WPA1: WPA2 only
- WPA2: WPA2 only
- WPA1/2: WPA1 and WPA2 in one SSID (radio cell)

WPA1 session key type

If you use "802.11i (WPA)-PSK" for encryption, the method for generating a WPA1 session or group key can be selected here:

- AES: The access point uses the AES method.
- TKIP: The access point uses the TKIP method.
- AES/TKIP: The access point uses the AES method. If the client hardware does not support the AES method, the access point will change to the TKIP method.

WPA2 session key type

The method for generating a WPA2 session or group key can be selected here.

Basis rate

The defined basis rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster". By setting the transmission rate to auto, the access point collects information about the transmission rates of the various WLAN clients. Clients automatically notify the access point of this rate with each unicast communication. The access point takes the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

Client-bridge support.

Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ().



The client-bridge mode operates between two LANCOM devices only.

Maximum count of clients

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

Minimum client signal strength

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

Use long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

Max. spatial streams

The spatial multiplexing function allows the access point to transmit multiple data streams over separate antennas in order to increase the data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

 In the 'Auto' setting, the access point uses all of the spatial streams supported by this WLAN module.

Allow short guard interval

This option is used to reduce the transmission pause between two signals from 0.8 μ s (default) to 0.4 μ s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

Use frame aggregation

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This procedure reduces the overhead of the packets to increase the throughput.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

STBC (space time block coding) activated

Activate the space time block coding here.

The function 'STBC' additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

LDPC (low density parity check) activated

Activate the low density parity check here.

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

8.7.3 Additions to the Setup menu

OKC

Opportunistic key caching delegates the management of the WLAN client keys to a WLAN controller, or to a central switch, which manages all of the access points in the network. If a client logs on to an access point, the WLAN controller behind it works as an authenticator to manage the keys and send the PMK to the access point, which is ultimately received by the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID. It then send this to the new access point in the hope that OKC is enabled there (therefore "opportunistic"). If the access point cannot handle the PMKID, then it negotiates an 802.11X authentication with the client in the usual manner.

A LANCOM access point can even perform OKC if the WLAN controller is temporarily unavailable. In this case, it stores the PMK and sends this to the WLAN controller when it becomes available again. Ultimately it sends the PMK to all of the access points in the network, which allows clients to use OKC to login after a change of radio cell.

This setting enables OKC on the access point that is being managed by the WLAN controller.

SNMP ID:

2.37.1.1.40

Telnet path:**Setup > WLAN-Management > AP-Configuration > Network-Profiles****Possible values:**

Yes

No

Default:

Yes

8.7.4 Additions to the Status menu

Contents

This table contains all entries of the PMK caches.

SNMP ID:

1.3.60.2

Telnet path:**Status > WLAN > PMK-Caching > Content****Authenticator**

This entry contains the MAC address of the authenticating access points.

Supplicant

This entry contains the MAC address of the authenticating WLAN client.

Source

This entry indicates how the WLAN client obtained the PMK:

- **Unknown:** The source is unknown. This entry should not occur in normal operation.
- **Authentication:** PMK is the result of a normal 802.1x-authentication between WLAN client and access point.
- **Pre-authentication:** PMK is the result of a normal 802.1x-pre-authentication between the WLAN client and another access point.

OKC: The PMK results from opportunistic key caching.

User name

This entry contains the user name, which the RADIUS server sends to the access point for access permission.



If the RADIUS server does not transmit a user name, this field is left blank.

VLAN ID

This entry contains the VLAN-ID, which the RADIUS server sends to the access point for access permission.



If the RADIUS server does not transmit a VLAN-ID, this field is left blank.

Lifetime

This entry contains the lifetime of the PMKs in seconds. It is calculated from the validity of the session, which the RADIUS server transmitted with the access permission.

The value is 0 seconds if the RADIUS server did not transmit a duration or the PMK does not have a validity period.

Expired

This entry shows whether a PMK has expired. If this is the case, the access point no longer accepts PMK-caching or authentication attempts with this PMK. Instead, it will launch a new 802.1x authentication.

Encryption

This table contains information about the encryption on each interface.

SNMP ID:

1.3.64

Telnet path:

Status > WLAN

Interface

Name of interface

Encryption

Displays whether encryption is enabled for this interface.

Method

Displays the encryption method. If encryption is not enabled, this column contains the value "None"

WPA version

Displays the WPA encryption version.

WPA1 session key types

Displays the log for the WPA1 session key.

WPA2 session key types

Displays the log for the WPA2 session key.

PMK caching

Indicates whether the PMK caching (pairwise master key storage) is enabled on the interface.

Pre-authentication

Indicates whether pre-authentication is enabled on this interface.

OKC

Indicates whether the opportunistic key caching is enabled on this interface.

8.8 Feature enhancement of the WLC tunnel interface

WLC tunnel interfaces provide "virtual" Ethernet interfaces, which so far had some limitations in comparison with physical Ethernet interfaces. As of LCOS version 8.84, WLC tunnel interfaces additionally support the following features:

- You can set a bandwidth limit per user.
- VRRP works (entry of additional MAC addresses)
- You can set a VLAN-ID for each user.

8.9 Support for 802.11u/HotSpot 2.0 on WLAN controllers

With LCOS 8.84, WLAN controllers gain the IEEE 802.11u/Hotspot 2.0 functions that were introduced for access points with LCOS 8.82. Controllers use profiles to configure and assign these functions to the access points managed by them. The options in the settings correspond to those of the access points.

8.9.1 Additions to the Status menu

IEEE802.11u

This menu shows the full range of IEEE802.11u or Hotspot-2.0 settings assigned to the device by the WLC.

SNMP ID:

1.59.108

Telnet path:

Setup > WLAN-Management

Network profiles

This table shows the network profile or 802.11u profile that has been assigned to the device by the WLC.

SNMP ID:

1.59.108.1

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the network profile or 802.11u profile

Operating

Indicates whether support for IEEE 802.11u connections is enabled for this profile

Hotspot2.0

Indicates whether support for Hotspot2.0 connections is enabled for this profile

Internet

Indicates whether the Internet bit is set for this profile

Network type

The type of network that the logical WLAN network most closely characterizes (e.g. private, public, access with or without authorization, etc.)

Asra

Indicates whether the Asra bit is set for this profile

HESSID type

Indicates the source of the MAC address for the HESSID. Possible values are:

- **Auto:** Automatic calculation of the HESSID by the WLC
- **User:** Manual allocation of HESSID by the network administrator
- **None:** No HESSID available

HESSID-MAC

MAC address of the HESSID

ANQP profile

ANQP profile used on the WLC for the 802.11u profile

HS20 profile

Hotspot2.0 or SH20 profile used on the WLC for the 802.11u profile

ANQP profiles

This table shows the ANQP profile assigned to the device by the WLC.

SNMP ID:

1.59.108.2

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the ANQP profile

Include in beacon OUI

Organizationally unique identifier (abbreviated as OUI and simplified to OI) broadcast by an access point in its beacons

Additional OUI

OI(s) additionally broadcast by an access point after a GAS request from a station

Domain list

List of domains which a hotspot belongs to

NAI realm list

Allocated NAI realm profile

Cellular list

Assigned cellular network profile

Network auth type list

Assigned authentication parameters

Hotspot2.0 profiles

This table shows the Hotspot-2.0 profile assigned to the device by the WLC.

SNMP ID:

1.59.108.3

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the Hotspot2.0 profile

Operator name

Assigned profile list for hotspot operators

Connection capabilities

Assigned connection capabilities

Operating class

Code for the global operating class of the managed access points

Network authentication type

This table shows the network authentication type profile assigned to the device by the WLC for the ANQP profile.

SNMP ID:

1.59.108.4

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the network authentication type profile

Network auth type

Context to which the redirect applies

Redirect URL

Address to which the device redirects stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners.

Cellular network information list

This table shows the cellular network profile assigned to the device by the WLC for the ANQP profile.

SNMP ID:

1.59.108.5

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the cellular network profile

Country code

Assigned mobile country code (MCC) of the hotspot operator or its roaming partners

Network code

Assigned mobile network code (MNC) of the hotspot operator or its roaming partners

Venue name

This table shows the venue name profile (used to manage information about the location of the access point) assigned to the device by the WLC.

SNMP ID:

1.59.108.6

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the venue name profile

Language

Language in which the site information is stored

Venue name

Description of the location of the device

NAI realms

This table shows the NAI realm profile assigned to the device by the WLC for the ANQP profile.

SNMP ID:

1.59.108.7

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the NAI realm profile

NAI realm

Assigned realm for the WLAN network

EAP method

Assigned authentication method for the NAI realm

Auth parameter list

Assigned authentication parameters for the EAP method

Operator list

This table shows the operator profile assigned to the device by the WLC for the Hotspot2.0 profile.

SNMP ID:

1.59.108.8

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the operator profile

Language

Assigned language for hotspot operators

Operator name

Assigned plain text name of the hotspot operator

General

This table shows the location profile assigned to the device by the WLC.

SNMP ID:

1.59.108.9

Telnet path:

Setup > WLAN-Management > IEEE802.11u

Name

Name of the location profile

Link status

Internet connectivity status of the managed access point

Downlink speed

Nominal value of the downlink bandwidth

Uplink speed

Nominal value of the uplink bandwidth

IPv4 addr type

Information for an IEEE 802.11u-capable station about the availability of IPv4 address space

IPv6 addr type

Information for an IEEE 802.11u-capable station about the availability of IPv6 address space

Venue group

Assigned venue group

Venue type

Assigned venue type code

Venue name

Assigned venue name profile (used to manage information about the location of the access point)

IEEE802.11u

This menu shows the IEEE802.11u or Hotspot-2.0 settings that are currently assigned by the device to the managed access points.

SNMP ID:

1.73.2.17

Telnet path:

Setup > WLAN-Management > AP-Configuration

Network profiles

This table shows the different network profiles currently assigned by the device to the managed access points for the logical WLAN networks, by means of the 802.11u profile.

SNMP ID:

1.73.2.17.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the network or 802.11u profile

Operating

Indicates whether IEEE 802.11u connection support is enabled for this profile

Hotspot2.0

Indicates whether Hotspot-2.0 connection support is enabled for this profile

Internet

Indicates whether the Internet bit is set for this profile

Network type

Type that most closely characterizes the logical WLAN network (e.g. private, public, access with or without authorization, etc.)

Asra

Indicates whether the Asra bit is set for this profile

HESSID type

Indicates the source of the MAC address for the HESSID. Possible values are:

- `Auto`: Automatic calculation of the HESSID by the WLC
- `User`: Manual allocation of HESSID by the network administrator
- `None`: No HESSID available

HESSID-MAC

MAC address of the HESSID

ANQP profile

ANQP profile used for the 802.11u profile

HS20 profile

Hotspot-2.0 or HS20 profile used for the 802.11u profile

ANQP profiles

This table shows the different ANQP profiles currently assigned by the device to the managed access points for the logical WLAN networks, by means of the network- or 802.11u profile.

SNMP ID:

1.73.2.17.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the ANQP profile

Include in beacon OUI

Organizationally unique identifier (abbreviated as OUI and simplified to OI) broadcast by an access point in its beacons

Additional OUI

OI(s) additionally broadcast by an access point after a GAS request from a station

Domain list

List of domains which a hotspot belongs to

NAI realm list

Allocated NAI realm profile

Cellular list

Assigned cellular network profile

Network auth type list

Assigned authentication parameters

Hotspot2.0 profiles

This table shows the different Hotspot2.0 profiles currently assigned by the device to the managed access points for the logical WLAN networks, by means of the network- or 802.11u profile.

SNMP ID:

1.73.2.17.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the Hotspot2.0 profile

Operator name

Assigned profile list for hotspot operators

Connection capabilities

Assigned connection capabilities

Operating class

Code for the global operating class of the managed access points

Network authentication type

This table shows the individual network authentication type profiles that are currently used by the device for one or more ANQP profiles.

SNMP ID:

1.73.2.17.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the network authentication type profile

Network auth type

Context to which the redirect applies

Redirect URL

Address to which the device redirects stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners.

Cellular network information list

This table shows the cellular network profiles that are currently used by the device for one or more ANQP profiles.

SNMP ID:

1.73.2.17.5

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the cellular network profile

Country code

Assigned mobile country code (MCC) of the hotspot operator or its roaming partners

Network code

Assigned mobile network code (MNC) of the hotspot operator or its roaming partners

Venue-Name

This table shows the venue name profiles (used to manage information about the location of the access point) used by the device for one or more venue profiles.

SNMP ID:

1.73.2.17.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Name of the venue name profile

Language

Language in which the site information is stored

Venue name

Description of the location of the device

NAI-Realms

This table shows the individual NAI profiles that are currently used by the device for one or more ANQP profiles.

SNMP ID:

1.73.2.17.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Name of the NAI realm profile

NAI realm

Assigned realm for the WLAN network

EAP method

Assigned authentication method for the NAI realm

Auth parameter list

Assigned authentication parameters for the EAP method

Operator-List

This table shows the individual operator profiles that are currently used by the device for one or more Hotspot2.0 profiles.

SNMP ID:

1.73.2.17.8

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Name of the operator profile

Language

Assigned language for hotspot operators

Operator name

Assigned plain text name of the hotspot operator

General

This table shows the individual venue profiles that are currently used by the device for one or more WLAN profiles.

SNMP ID:

1.73.2.17.9

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Name of the location profile

Link status

Internet connectivity status of the managed access point

Downlink speed

Nominal value of the downlink bandwidth

Uplink speed

Nominal value of the uplink bandwidth

IPv4 addr type

Information for an IEEE 802.11u-capable station about the availability of IPv4 address space

IPv6 addr type

Information for an IEEE 802.11u-capable station about the availability of IPv6 address space

Venue group

Assigned venue group

Venue type

Assigned venue type code

Venue name

Assigned venue name profile (used to manage information about the location of the access point)

8.9.2 Additions to the Setup menu

IEEE802.11u

The tables and parameters in this menu are used to make all settings for connections according to IEEE 802.11u and Hotspot 2.0. With the use of profiles, these settings can be assigned to the access points connected to the WLAN controller.

SNMP ID:

2.37.1.17

Telnet path:

Setup > WLAN-Management > AP-Configuration

ANQP profiles

Using this table you manage the profile lists for IEEE802.11u and ANQP. IEEE802.11u profiles offers you the ability to group certain ANQP elements and to independently assign logical WLAN interfaces in the table **Network profiles**. These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.

SNMP ID:

2.37.1.17.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Assign a name for the ANQP 2.0 profile here. You specify this name later in the table **Network profiles** under **ANQP profile**.

SNMP ID:

2.37.1.17.2.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles

Possible values:

String, max. 32 characters

Default:**Include-in-Beacon-OUI**

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.



This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional-OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

SNMP ID:

2.37.1.17.2.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles

Possible values:

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

Default:**Additional-OUI**

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.

SNMP ID:

2.37.1.17.2.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles

Possible values:

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

Default:**Domain-List**

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org`, `provx-mobile.com`, `wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., `providerX.org`, this domain is also assigned to access points with the domain name `wi-fi.providerX.org`.

When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

SNMP ID:

2.37.1.17.2.4

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles****Possible values:**

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

Default:**NAI-Realm-List**

Enter a valid NAI realm profile in this field.

SNMP ID:

2.37.1.17.2.5

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles****Possible values:****Name** from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > NIA-Realms**, max. 65 characters Multiple names can be provided in a comma-separated list.**Default:****Cellular-List**

Enter a valid cellular network profile in this field.

SNMP ID:

2.37.1.17.2.6

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles****Possible values:****Name** from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Cellular-Network-Information-List**, max. 65 characters Multiple names can be provided in a comma-separated list.**Default:****Network-Auth-Type-List**

Enter one or more valid authentication parameters in this field.

SNMP ID:

2.37.1.17.2.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles**

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Authentication-Type**, max. 65 characters Multiple names can be provided in a comma-separated list.

Default:**Auth-Parameter**

This table contains a set list of possible authentication parameters for the NAI realms, as referenced by a comma-separated list in the table **NAI realms** in the input field **Auth parameter**.

Table 2: Overview of possible authentication parameters

Parameters	Sub-parameters	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password
None	No credentials required	
TunnelEAPCredentials.*		
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
Anonymous*	Anonymous login	

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

SNMP ID:

2.37.1.17.10

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

This entry displays the name of the authentication parameters that you referenced as a comma-separated list in the table **NAI-Realms** in the input field **Auth-Parameter**.

SNMP ID:

2.37.1.17.10.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Auth-Parameter****Cellular network information list**

Using this table, you manage the profile lists for the cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.

In the setup menu you use the **ANQP-Profiles** table to assign this list to an ANQP profile.

SNMP ID:

2.37.1.17.5

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Assign a name for the cellular network profile, such as an abbreviation of the network operator in combination with the cellular network standard used. You specify this name later in the table **ANQP profiles** under **Cellular-List**.

SNMP ID:

2.37.1.17.5.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Cellular-Network-Information-List****Possible values:**

String, max. 32 characters

Default:**Country-Code**

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., 262 for Germany.

SNMP ID:

2.37.1.17.5.2

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Cellular-Network-Information-List****Possible values:**

Valid MCC, max. 3 characters

Default:**Network-Code**

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

SNMP ID:

2.37.1.17.5.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Cellular-Network-Information-List****Possible values:**

Valid MNC, max. 32 characters

Default:**Connection capability**

This table contains a set list of possible connection capabilities, as referenced by a comma-separated list in the table **Hotspot2.0 profiles** in the input field **Connection-Capabilities**. Possible status values for each of these services are 'closed' (-C), 'Open' (-O) or 'unknown' (-U):

SNMP ID:

2.37.1.17.11

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

This entry displays the name of the connection capability that you referenced as a comma-separated list in the table **Hotspot2.0-Profiles** in the input field **Connection-Capabilities**.

SNMP ID:

2.37.1.17.11.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Connection-Capability****General**

This table is used to manage the general settings for IEEE 802.11u/Hotspot 2.0.

On a standalone access point, these settings exist in the form of separate parameters. On a WLAN controller, these parameters are summarized into tables, which are subsequently assigned to the managed access points by means of the WLAN profile (the **Common profiles** table).

SNMP ID:

2.37.1.17.9

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Assign a name for the general settings profile here. You specify this name later in the table **Setup > WLAN-Management > AP-Configuration > Common-Profiles** under **Hotspot2.0-General** an.

SNMP ID:

2.37.1.17.9.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:**

String, max. 32 characters

Default:**Link-Status**

Using this entry, you specify the connectivity status of your device to the Internet.

SNMP ID:

2.37.1.17.9.2

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:**

- **Auto**: The device determines the status value for this parameter automatically
- **Link-Up**: The connection to the Internet is established.
- **Link-Down**: The connection to the Internet is interrupted.
- **Link-Test**: The connection to the Internet is being established or is being checked.

Default:

Auto

Downlink-Speed

Using this entry, you enter the nominal value for the maximum receiving bandwidth (downlink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

SNMP ID:

2.37.1.17.9.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:**

0 to 4294967295, in Kbit/s

Default:

0

Uplink-Speed

Using this entry you can enter the nominal value for the maximum transmission bandwidth (uplink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

SNMP ID:

2.37.1.17.9.4

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:**

0 to 4294967295, in Kbit/s

Default:

0

IPv4-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv4.

SNMP ID:

2.37.1.17.9.5

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:****Not-Available**

IPv4 address type is not available.

Public-Addr-Available

Public IPv4 address is available.

Port-Restr-Addr-Avail

Port-restricted IPv4 address is available.

Single-Nat-Priv-Addr-Avail

Private, single NAT-masked IPv4 address is available.

Double-Nat-Priv-Addr-Avail

Private, double NAT-masked IPv4 address is available.

Port-Restr-Single-Nat-Addr-Avail

Port-restricted IPv4 address and single NAT-masked IPv4 address is available.

Port-Restr-Double-Nat-Addr-Avail

Port-restricted IPv4 address and double NAT-masked IPv4 address is available.

Availability-not-known

The availability of an IPv4 address type is unknown.

Default:

Single-Nat-Priv-Addr-Avail

IPv6-Addr-Type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv6.

SNMP ID:

2.37.1.17.9.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General

Possible values:**Not-Available**

IPv6 address type is not available.

Available

IPv6 address type is available.

Availability-not-known

The availability of an IPv6 address type is unknown.

Default:

Not-Available

Venue-Group

The venue group describes the environment where you set up the access point. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

SNMP ID:

2.37.1.17.9.7

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General

Possible values:

- Unspecified: Unspecified
- Assembly: Assembly
- Business: Business
- Educational: Educational:
- Factory-and-Industry: Factory and industry
- Institutional: Institutional
- Mercantile: Commerce
- Residential: Residence hall
- Storage: Warehouse
- Utility-and-Miscellaneous: Utility and miscellaneous
- Vehicular: Vehicular
- Outdoor: Outdoor

Default:

Unspecified

Venue-Type

Using the location type code (venue type), you have the option to specify details for the location group. These values are also specified by the standard. The possible type codes can be found in the following table.

SNMP ID:

2.37.1.17.9.8

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General****Possible values:****Table 3: Overview of possible values for venue groups and types**

Venue group	Code = Venue type code
Unspecified	
Assembly	<ul style="list-style-type: none"> ■ 0 = unspecified assembly ■ 1 = stage ■ 2 = stadium ■ 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) ■ 4 = amphitheater ■ 5 = amusement park ■ 6 = place of worship ■ 7 = convention center ■ 8 = library ■ 9 = museum ■ 10 = restaurant ■ 11 = theater ■ 12 = bar ■ 13 = café ■ 14 = zoo, aquarium ■ 15 = emergency control center
Business	<ul style="list-style-type: none"> ■ 0 = unspecified business ■ 1 = doctor's office ■ 2 = bank ■ 3 = fire station ■ 4 = police station ■ 6 = post office ■ 7 = office ■ 8 = research facility ■ 9 = law firm
Educational:	<ul style="list-style-type: none"> ■ 0 = unspecified education ■ 1 = primary school ■ 2 = secondary school ■ 3 = college
Factory and industry	<ul style="list-style-type: none"> ■ 0 = unspecified factory and industry ■ 1 = factory

Venue group	Code = Venue type code
Institutional	<ul style="list-style-type: none"> ■ 0 = unspecified institution ■ 1 = hospital ■ 2 = long-term care facility (e.g., nursing home, hospice) ■ 3 = rehabilitation clinic ■ 4 = organizational association ■ 5 = prison
Commerce	<ul style="list-style-type: none"> ■ 0 = unspecified commerce ■ 1 = retail store ■ 2 = food store ■ 3 = auto repair shop ■ 4 = shopping center ■ 5 = gas station
Halls of residence	<ul style="list-style-type: none"> ■ 0 = unspecified residence hall ■ 1 = private residence ■ 2 = hotel or motel ■ 3 = student housing ■ 4 = guesthouse
Warehouse	<ul style="list-style-type: none"> ■ 0 = unspecified warehouse
Utility and miscellaneous	<ul style="list-style-type: none"> ■ 0 = unspecified service and miscellaneous
Vehicular	<ul style="list-style-type: none"> ■ 0 = unspecified vehicle ■ 1 = passenger or transport vehicles ■ 2 = aircraft ■ 3 = bus ■ 4 = ferry ■ 5 = ship or boat ■ 6 = train ■ 7 = motorcycle
Outdoor	<ul style="list-style-type: none"> ■ 0 = unspecified outdoor ■ 1 = municipal Wi-Fi network (wireless mesh network) ■ 2 = city park ■ 3 = rest area ■ 4 = traffic control ■ 5 = bus stop ■ 6 = kiosk

Default:

0

Venue-Name

Use this field to specify one or more valid list entries from the table **Venue Name** in order to identify the location of the device. The parameter considers all list entries that match the venue name specified here.

SNMP ID:

2.37.1.17.9.9

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Venue-Name**, max. 32 characters Multiple names can be provided in a hash-separated (#) list.

Default:**Hotspot2.0 profiles**

Using this table you manage the profile lists for the Hotspot 2.0. Hotspot 2.0 profiles enable you to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign these to logical WLAN interfaces in the table **Network-Profiles** under **HS20-Profile**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.

SNMP ID:

2.37.1.17.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Assign a name for the Hotspot 2.0 profile here. You specify this name later in the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles** under **HS20-Profile**.

SNMP ID:

2.37.1.17.3.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Hotspot2.0-Profiles

Possible values:

String, max. 32 characters

Default:**Operator name**

Enter a valid profile for hotspot operators in this field.

SNMP ID:

2.37.1.17.3.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Hotspot2.0-Profiles

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Operator-List**, max. 65 characters

Default:**Connection capabilities**

Enter one or more valid entries for the connection capabilities in this field. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown".

SNMP ID:

2.37.1.17.3.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Hotspot2.0-Profiles****Possible values:****Name** from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Connection-Capability**, max. 250 characters Multiple names can be provided in a comma-separated list.**Default:****Operating class**

Enter the code for the global operating class of the managed access point. Using the operating class, you inform a station on which frequency bands and channels an access point is available. Example:

- 81: Operation at 2.4 GHz with channels 1-13
- 11.6: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to an access point: Global operating classes, available at standards.ieee.org.

SNMP ID:

2.37.1.17.3.4

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Hotspot2.0-Profiles****Possible values:**

Operating class code, max. 32 characters

Default:**NAI-Realms**

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.

In the setup menu you use the **ANQP-Profiles** table to assign this list to an ANQP profile.

SNMP ID:

2.37.1.17.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. You specify this name later in the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles** under **NAI-Realm-List**.

SNMP ID:

2.37.1.17.7.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > NAI-Realms

Possible values:

String, max. 32 characters

Default:**NAI-Realm**

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest case, is <username>@<realm>, for `user746@providerX.org`, and therefore the corresponding realm is `providerX.org`.

SNMP ID:

2.37.1.17.7.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > NAI-Realms

Possible values:

String, max. 32 characters

Default:**EAP-Method**

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication procedure

SNMP ID:

2.37.1.17.7.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > NAI-Realms

Possible values:

- **None:** Select this setting when the relevant NAI realm does not require authentication.
- **EAP-TLS:** Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate installed by the user.
- **EAP-SIM:** Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.
- **EAP-TTLS:** Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.
- **EAP-AKA:** Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

Default:

None

Auth-Parameter-List

In this field, enter the appropriate authentication parameters for the EAP method using a comma-separated list, e.g., for EAP-TLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` or for EAP-TLS `Credentials.Certificate`.

SNMP ID:

2.37.1.17.7.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > NAI-Realms

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Auth-Parameter**, max. 65 characters Multiple names can be provided in a comma-separated list.

Default:

Network authentication type

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

You specify the name for the Network Authentication Type Profile later in the table **ANQP profiles** under **Network-Auth-Type-List**.

SNMP ID:

2.37.1.17.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Assign a name for the table entry, e.g., `Accept Terms and Conditions`.

SNMP ID:

2.37.1.17.4.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Authentication-Type

Possible values:

String, max. 32 characters

Default:

Network-Auth-Type

Choose the context from the list, which applies before forwarding.

SNMP ID:

2.37.1.17.4.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Authentication-Type

Possible values:

- **Accept-Terms-Cond:** An additional authentication step is set up that requires the user to accept the terms of use.
- **Online-Enrollment:** An additional authentication step is set up that requires the user to register online first.
- **Http-Redirection:** An additional authentication step is set up to which the user is forwarded via HTTP.
- **DNS-Redirection:** An additional authentication step is set up to which the user is forwarded via DNS.

Default:

Accept-Terms-Cond

Redirect-URL

Enter the address to which the device forwards stations for additional authentication.

SNMP ID:

2.37.1.17.4.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Authentication-Type****Possible values:**

URL, max. 65 characters

Default:**Network profiles**

The table **Network profiles** is the highest administrative level for 802.11u and Hotspot 2.0. It gives you the option of turning the functions for every profile on or off, to assign child profile lists (such as those for ANQP or HS20), or to make general settings.

SNMP ID:

2.37.1.17.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

This parameter specifies the name of the 802.11u profile. You will subsequently assign this profile to a logical wireless network in the table **Setup > WLAN-Management > AP-Configuration > Network-profiles** under **802.11u network profile**.

SNMP ID:

2.37.1.17.1.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

String, max. 32 characters

Default:**Operating**

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

SNMP ID:

2.37.1.17.1.2

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-profiles****Possible values:**

Yes

No

Default:

No

Hotspot2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.



The prerequisite for this function is that support for connections according to IEEE 802.11u is enabled.

SNMP ID:

2.37.1.17.1.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

Yes

No

Default:

No

Internet

Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

SNMP ID:

2.37.1.17.1.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles

Possible values:

Yes

No

Default:

No

Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface.

SNMP ID:

2.37.1.17.1.5

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles

Possible values:

- **Private:** Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.
- **Private-GuestAcc:** Similar to **Private**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.
- **Public-Charge:** Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.
- **Public-Free:** Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.
- **Personal-Dev:** In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.
- **Emergency:** Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.
- **Experimental:** Describes networks that are set up for testing purposes or are still in the setup stage.
- **Wildcard:** Placeholder for previously undefined network types.

Default:

Private

Asra

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.



Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

SNMP ID:

2.37.1.17.1.6

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

Yes

No

Default:

No

HESSID type

Specify which HESSID is provided by the device to the access points for the homogeneous ESS.

A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point (its BSSID), or the MAC address of the WLC, serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT".

SNMP ID:

2.37.1.17.1.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

- **Auto:** Based on its own MAC address, the device generates a common HESSID for all access points that belong to the network profile.
- **User:** Manually assign an HESSID for all access points that belong to the network profile.
- **None:** The connected access points are not assigned an HESSID.

Default:

Auto

HESSID MAC

If you selected the setting `user` for the **HESSID-type**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. For the HESSID, select the BSSID for any access point in your homogeneous ESS, or the MAC address of your WLC, in capital letters and without separators, e.g., `008041AEFD7E` for the MAC address `00:80:41:ae:fd:7e`.



If an access point is not present in multiple homogeneous ESS's, the HESSID is identical for all of its interfaces.

SNMP ID:

2.37.1.17.1.8

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

MAC address in capital letters and without separators

Default:

000000000000

ANQP profile

Using this parameter, you specify a valid ANQP profile that you want to use for the 802.11u profile.

SNMP ID:

2.37.1.17.1.10

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > ANQP-Profiles**, max. 32 characters

Default:**HS20 profile**

Using this parameter, you specify a valid Hotspot 2.0 or HS20 profile that you want to use for the 802.11u profile.

SNMP ID:

2.37.1.17.1.10

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles****Possible values:**

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Hotspot2.0-Profiles**, max. 32 characters

Default:**Operator-List**

Using this table you manage the plain text name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.

SNMP ID:

2.37.1.17.8

Telnet path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****Name**

Assign a name for the entry, such as an index number or combination of operator-name and language.

SNMP ID:

2.37.1.17.8.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Operator-List

Possible values:

String, max. 32 characters

Default:**Language**

Select a language for the hotspot operator from the list.

SNMP ID:

2.37.1.17.8.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Operator-List

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabian

Default:

None

Operator name

Enter the plain text name of the hotspot operator.

SNMP ID:

2.37.1.17.8.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Operator-List

Possible values:

String, max. 65 characters

Default:**Venue-Name**

In this table, enter general information about the location of an access point.

In the event of a manual search, additional details on the Venue information help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

SNMP ID:

2.37.1.17.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u

Name

Enter a name for the list entry in the table. This name will be used to reference the site information from other tables.

SNMP ID:

2.37.1.17.6.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Venue-Name

Possible values:

String, max. 65 characters

Default:**Language**

Select the language in which you store information about the location.

SNMP ID:

2.37.1.17.6.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Venue-Name

Possible values:

None
English
Deutsch
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish

Portuguese

Polish

Czech

Arabic

Default:

None

Venue-Name

Enter a short description of the location of your device for the selected language.

SNMP ID:

2.37.1.17.6.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Venue-Name

Possible values:

String, max. 65 characters

Default:

IEEE802.11u network profile

This parameter specifies the name of 802.11u network profile which is to be assigned to the logical WLAN network.

SNMP ID:

2.37.1.1.39

Telnet path:

Setup > WLAN-Management > AP-Configuration > Network-Profiles

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > Network-Profiles**, max. 32 characters

Default:

IEEE802.11u-General

These parameters specify the name of the location profile that you want to apply for the WLAN profile (i.e. this common profile).

SNMP ID:

2.37.1.3.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > Commonprofiles

Possible values:

Name from the table **Setup > WLAN-Management > AP-Configuration > IEEE802.11u > General**, max. 32 characters

Default:

9 Public Spot

9.1 Any phone number format for Smart Ticket

As of LCOS 8.84, users of Smart Ticket who opt to receive login credentials via SMS can enter their phone number in any format (0049.../+49..., etc.). The device removes any leading zeros or '+' character automatically and saves the phone number in the RADIUS user table in a standard format (49...).

9.2 Sending login data via a GSM-capable device (Smart Ticket)

As of LCOS 8.84, you can activate the option **Login data will be sent via SMS (text message)**

- and make direct use of a device's own 3G/4G WWAN module, or
- the 3G/4G WWAN module of another device

instead of using an external E-Mail2SMS gateway.

9.2.1 Configuring SMS authentication

The settings for transmitting the login credentials as an SMS text message to the phone number specified by the user are adjusted in the dialog **Public Spot > SMS**. The choices available to you vary according to the device type:

- The credentials are sent as an SMS text message via the 3G/4G WWAN module in this device,
- The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device,
- The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

The following steps show you how to correctly configure the different variants of SMS authentication.

 In order to send login data as a text message via a 3G/4G WWAN-capable device, the internal SMS module of this device must be set up under **Log & Trace > SMS messages** (see [Basic configuration of the SMS module](#) on page 141).

 SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

 In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace > SMTP account** and **Log & Trace > SMTP options**.

In addition, you can specify individual text blocks used by the device to send the login credentials; see [Customizing text message content](#) on page 114. By default, the device inserts predefined text modules; for an overview of these see [Standard texts for e-mail sender, subject line and body](#) on page 115.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot > Authentication**.
3. Change the login mode to **Login data will be sent by SMS**.

4. Navigate to the menu item **Public Spot > SMS**.

The following settings are needed if you selected for 'Authentication' the sending of login data by SMS.

SMS

Send SMS via external email-to-SMS gateway
 Send SMS via GSM capable LANCOS (e.g. with 3G/4G modem)
 Send SMS via internal GSM modem

 Please remember to configure the corresponding section 'Log_Trace' -> 'SMTP' or 'SMS' for each selection.

Address of GSM device:
 Administrator:
 Password: Show

Gateway email address:
 Max. messages send: per hour
 Max. requests per MAC: per day
 Sender email address:

5. Specify how the device sends SMS text messages.

- In order to send the login credentials as an SMS text message via the internal 3G/4G WWAN module, select **Send SMS via internal GSM modem** and then continue with the next main step in the configuration.
- In order to send the login credentials as an SMS text message via the 3G/4G WWAN module of another device, you first carry out the steps in section [Operating devices with the 3G/4G WWAN module as an SMS gateway](#) on page 107 and then continue with the next main step in the configuration.
- In order to send the login credentials to an external E-Mail2SMS gateway, select the setting **Send SMS via external e-mail-to-SMS gateway** and then continue with the next main step in the configuration.
 - a) Under **Gateway e-mail address** you enter the IP address or the hostname of the gateway server, which converts the e-mail into SMS. If the provider expects to find the mobile phone number in the local part of the e-mail, you can use the variable `$PSpotUserMobileNo`.
 - b) Under **Sender e-mail address** enter the return address that your Public Spot users will see when the SMS is delivered, e.g. `support@providerX.org`.
- 6. Under **Max. messages send** you enter the maximum number of SMS text messages that the Public Spot module may send per hour to users authenticating via SMS. Lower the value to reduce the number of new users per hour.
- 7. Under **Max.requests per MAC** you specify how many different sets of credentials the device can provide to a MAC address within one day.
- 8. Under **Country codes** you enter the international code numbers that the Public Spot will accept when sending data via SMS.
Country codes can be entered directly or with a prefixed double-zero, for example for Germany 49 or 0049.

 This table acts as a whitelist. You must define country codes in order for the login data to be delivered.

9. You can write the configuration back to the device.

Operating devices with the 3G/4G WWAN module as an SMS gateway

When using Public Spot authentication via SMS (Smart Ticket), you have the option of sending access credentials via the 3G/4G WWAN module in a further device instead of using an external E-Mail2SMS gateway. To use this option, you must store the address and the access credentials for the 3G/4G device on the device that provides the Public Spot. In order to send the SMS, the Public Spot module logs on to the other device and uses a URL to initiate the transmission of the text message via the 3G/4G-WWAN module or SMS module in the other device.

This option is available on devices both with and without their own 3G/4G WWAN module. These options allow you to chain multiple devices together and to set up your own transmitting device if you operate multiple Public Spots or use a device without a 3G/4G WWAN module.

1. Start LANconfig and set up the SMS module on the 3G/4G device that is to serve as an SMS gateway (see [Basic configuration of the SMS module](#) on page 141). In addition, we recommended that you create an administrator without access rights (select **None**) and with just one function right, **Send SMS**.
2. Open the configuration dialog for the device that provides the Public Spot.
3. Navigate to the menu item **Public Spot > SMS**.

The following settings are needed if you selected for 'Authentication' the sending of login data by SMS.

4. Select the setting **Send SMS via GSM-capable LANCOM (e.g. with 3G/4G modem)**.
5. Enter the user name and password for the administrator on the other 3G/4G device under **Administrator** and **Password**.
6. In the field **Address of GSM device**, enter the IP address where the Public Spot is to reach the other 3G/4G device.

9.2.2 Additions to the Setup menu

Send SMS

This parameter specifies how the device sends SMS text messages. You have a variety of choices, depending on the device type.

! To successfully deliver login credentials as a text message via a 3G/4G WWAN-enabled device, its internal SMS module must be set under **Setup > SMS**.

! SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

! In order to send login credentials via e-mail, a valid SMTP account must be set under **Setup > E-mail**.

SNMP ID:

2.24.41.2.15

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication

Possible values:**Send directly**

The credentials are sent as an SMS text message via the 3G/4G WWAN module in this device.

HTTP2SMS

The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device

When registering with the Public Spot via SMS, you have the option of sending the access credentials via another LANCOM device equipped with a 3G/4G WWAN module. To use this option, you must store the address and the access data for the other device on the device that provides the Public Spot. In order to send the SMS, the Public Spot module logs on to the other device and uses a URL to initiate the transmission of the text message via the 3G/4G WWAN module in the other device.



Make sure that the SMS module on the other device is configured correctly. In addition, we recommended that you create an administrator without access rights (select **None**) and with just one function right, **Send SMS**.

SMS gateway

The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

Default:

SMS gateway

HTTP user name

With this parameter you specify the user name used by your device to authenticate at another LANCOM device.

SNMP ID:

2.24.41.2.16

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication

Possible values:

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

Default:

empty

HTTP password

With this parameter you specify the password for the user name used by your device to authenticate at another LANCOM device.

SNMP ID:

2.24.41.2.17

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication

Possible values:

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

Default:*empty***HTTP gateway address**

This parameter specifies the IP address of the other LANCOM device that is to be used for sending SMS.

SNMP ID:

2.24.41.2.18

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication

Possible values:

Valid IPv4/IPv6 address, max. 15 characters from [0-9][A-F][a-f]:./

Default:*empty*

9.3 Terms of use when authenticating with name, password (and MAC address)

With LCOS 8.84, the requirement for the user to agree to the terms and conditions of use, as previously used for Smart Ticket authentication, is now additionally available with the login modes **Authenticate with name and password** and **Authenticate with name, password and MAC address**. In this way, users who receive a voucher can also be required to confirm the terms and conditions of use before they can access the network via Public Spot.

In LANconfig you can enable or disable the confirmation of terms for the various login modes in the dialog **Public Spot > Authentication** under **User has to accept the terms of use**.

Authentication for network access

Authentication mode:

No authentication needed
 No credentials required (login via agreement)
 Authenticate with name and password
 Authenticate with name, password and MAC address
 Login data will be sent by email
 Login data will be sent by SMS
 User has to accept the terms of use

Protocol of login page

Login page is called via:

HTTPS - Data transmission is encrypted (recommended)
 HTTP - Data transmission is unencrypted

Login via agreement

Maximum request per hour: requests

Accounts per day: users

Username prefix:

Customization

Here you can optionally specify a personalized text that is displayed on the login page.

9.3.1 Additions to the Setup menu

User must accept GTC

By enabling this parameter, certain modes of authentication require the user to authenticate and also acknowledge the general terms and conditions of use. In this case, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering and/or authenticating. Users who explicitly do not agree to these terms and conditions cannot login to the Public Spot.

The following login modes can be combined with an acknowledgment of the terms and conditions:

- User+password
- MAC+user+password
- E-mail
- E-mail2SMS

 Remember to upload your custom page template to the device before you request a confirmation of the terms and conditions of use.

SNMP ID:

2.24.36

Telnet path:

Setup > Public-Spot-Module

Possible values:

No

Yes

Default:

No

9.4 Advanced configuration of user templates with LANconfig

As of LCOS 8.84, you have the option to

- configure user templates for self-sufficient user registration via e-mail/SMS, also known as Smart Ticket, and also
- to manage the max. concurrent logins table for the **Create Public Spot Account** Wizard)

directly in LANconfig under **Public Spot > Wizard**.

9.4.1 Setting default values for the Public Spot wizard

The following section describes how you define default values for the **New user wizard** (setup wizard **Create Public Spot account**) to meet your needs. Public Spot administrators can select the values defined here (e.g. for validity periods, bandwidth profiles, etc.) from selection lists when they are setting up new users and printing out vouchers.

 Exceptions to this are the values for User name pattern and Password length shown in the dialog below, which only serve as default values for the device.

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

2. Change the view to **Public Spot > Wizard**.

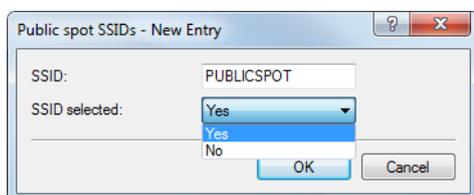
3. In **Default validity periods**, define which default validity periods for user accounts and vouchers are to be available by default.
The new-user wizard takes the shortest validity period as the default.

4. Under **Max. concurrent logins** you select the maximum number of devices that have access to the user account simultaneously.
The value 0 stands for 'unlimited'. Whether or not it is generally possible for a user to login with the multiple devices at the same time is determined by the Public Spot administrator with a separate setting in the wizard when creating a new user.

5. In **User name pattern** you specify the pattern used by the new user wizard to create usernames.
You can enter up to 19 characters, whereby the wizard will automatically create a unique number for every user if you enter "%n". The default description `user%n` will be shown later on the voucher, for example, as `user12345`.
6. Using **Password length** you specify the length of the passwords that the new user wizard generates for Public Spot access.

The default is 6 characters. If you would like to have longer passwords, keep in mind that guests can make mistakes when entering them, which can cause unnecessary problems and complaints.

7. Optional: Under **Bandwidth profiles** you set the uplink and downlink limits for each Public Spot user.
8. Public Spot via WLAN only: Using **Public Spot SSIDs** you specify the names of the Public Spot networks taken by default when you create new user accounts using the Create Public Spot account wizard.



The Create Public Spot account wizard automatically marks the specified network names as **SSID selected** when creating a new Public Spot user. If you employ an access point, WLAN controller or WLAN router, you can select several network names as default values in order to give users access to various different WLANs (e.g., for WLANs in the hotel lobby, the conference room, and floors where their rooms are located). When creating a new user and subsequently printing the voucher, these SSIDs are also printed out on the voucher.

Using the arrow buttons, you can change the order in which the SSIDs are displayed. In this way, the most popular SSIDs can be placed at the top of the list.

That's it! This concludes the configuration of the default values for the Public Spot wizard.

9.4.2 Setting default values for the user templates

The following section describes how you adjust the default values for the **User templates** to meet your needs. The device uses the values set here as defaults when creating new users in Smart Ticket and when users login after confirming the terms and conditions. If you have so opted to send the login credentials via e-mail/SMS or you have activated the login after confirming the terms and conditions, each new user account is equipped with the permissions and constraints as defined by the user template.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot > Wizard**.

Add user wizard

Public spot user accounts can be easily generated by the WEBconfig wizard. Both user name and password are generated automatically, and the next page offers to print out a page for the public spot user that contains all necessary data.

User name pattern:

Password length:

Print header and company emblem
 Print logout link

User template for email and SMS

Expiry type:

Relative expiry: seconds

Absolute expiry: days

Multiple login

Max. concurrent logins: *

Time budget: seconds

Volume budget: Megabyte

Comment:

3. Complete the input fields in the section **User template** according to your preferences:

- **Expiry type:** Using this entry you define how an automatically created Public Spot user account expires. You can specify whether the validity period of a user account is absolute (e.g. expires on a set date) and/or relative (elapsed time since the first successful login). If you select both values, the expiry time depends on which case occurs first.
 - **Relative expiry:** Using this entry you define the relative expiry time of an automatically created user account (in seconds). The **Expiry-type** that you chose must include `relative` in order for this setting to work. The validity of the account terminates after the time period specified in this field from the time of the first successful login of the user.
 - **Absolute expiry:** Using this entry you define the absolute expiry time of an automatically created user account (in days). The **Expiry-type** that you chose must include `absolute` in order for this setting to work. The validity of the account terminates at the time specified in this field, calculated from the day of the creation of the account.
 - **Multiple login:** This entry allows you to generally allow or prohibit users with an automatically created account to login to the Public Spot using the same credentials with multiple devices at the same time. The number of devices that can be logged on simultaneously is specified using the input field **Max. concurrent logins**.
 - **Maximum number:** Using this entry you set the maximum number of devices which can concurrently login to an automatically created account. The value 0 stands for "unlimited". In order for this setting to work, the parameter **Multiple login** must be enabled.
 - **Time budget:** Using this entry you define the time budget which automatically created users are assigned. A value of 0 disables the function.
 - **Volume budget:** Using this entry you define the volume budget which automatically created users are assigned. A value of 0 disables the function.
 - **Comment:** Using this entry you specify a comment or informational text which the RADIUS server adds to an automatically created user account.
4. Optional: If necessary, change the **User name pattern** and the **Password length**. In the authentication modes mentioned above, the device uses the relevant *New user wizard default values* to automatically generate a user name and a password.
 5. You can write the configuration back to the device.

9.5 Multi-lingual login and text messaging

As of LCOS 8.84, you can store selected texts in multiple languages. The following texts are now managed in language tables:

- The individual text on the login page (**Login text**; available in LANconfig under **Public Spot > Authentication**)
- The standard text for e-mail sender, subject and content as used for user registration via e-mail/SMS (**E-mail name of sender, E-mail subject, E-mail body**; available in LANconfig under **Public Spot > E-mail/SMS**)

The language tables complement the *template pages in various languages* and work on the same principle; the language selected by the device depends on the language set in the browser. Unless you specify custom text for e-mail sender, subject and content for a language, the Public Spot module uses the device's own standard texts in English (see *Standard texts for e-mail sender, subject line and body* on page 115). No standard texts have been implemented for the login text; in this case, the device refers to the individual login text in English (if available).

9.5.1 Customizing text message content

By default, the device uses predefined text modules as the content of the e-mails or SMS text messages. An overview of these standard texts is available under *Standard texts for e-mail sender, subject line and body* on page 115. You can also define your own texts.

 If you do not specify any text for a language, the device automatically enters the internal default text.

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

2. Depending on the selected authentication method, switch to the view **Public Spot > E-mail** or **SMS**.
3. Using the button **Name of sender**, enter a customized sender name for the e-mails or SMS text messages sent in the various languages, e.g. `Provider X`.
4. Use the **E-mail subject** button to enter a subject line for the e-mails sent in the various languages by the Public Spot module. Special control characters are available for this, described in more detail in the section [Variables and control characters](#) on page 115.
5. Use the **E-mail body** or **Message body** button to enter the content of the e-mails or SMS text messages sent in the various languages by the Public Spot module. Variables and special control characters are available for this, described in more detail in the section [Variables and control characters](#) on page 115.
6. Now write the configuration back to the device.

Variables and control characters

The message texts used for the Smart Ticket function can be customized with the use of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user or the SMS gateway.

Variables

The following variables are available in the input field **E-mail body**:

\$PSpotPasswd

Placeholder for user-specific password for the Public Spot access.

\$PSpotLogoutLink

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

Control characters

The following control characters may also be used in the text entered into the fields **E-mail subject** and **E-mail body**:

\n

CRLF (carriage return, line feed)

\t

Tabulator

\<ASCII>

ASCII code of the corresponding character



If the e-mail/SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Standard texts for e-mail sender, subject line and body

If you leave the dialogs **Public Spot > Email** or **SMS** blank, then the device automatically reverts to the standard texts in the corresponding language as stored in LCOS to generate the e-mail. The language used depends on the language setting of the browser used by the user for registration. If there are no default texts stored internally for a language, the device uses the English texts.

Table 4: Overview of the internal standard texts for authentication via e-mail/SMS

	Name of sender	E-mail subject	E-mail body
Deutsch	Public Spot	Your login credentials for the Public Spot	Your password for the LANCOM Public Spot: \$PSpotPasswd \$PSpotLogoutLink
English	Public Spot	Your Public Spot account	Your password for the LANCOM Public Spot: \$PSpotPasswd \$PSpotLogoutLink

9.5.2 Additions to the Setup menu

Name

This table is used to manage the different language variants for the sender names used by the Public Spot module in the e-mails containing the login credentials. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.1.20

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication

Language

This parameter shows the language variant for the sender name.

SNMP ID:

2.24.41.1.20.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Real-Name

Content

This parameter sets the sender name for the selected language.

SNMP ID:

2.24.41.1.20.2

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Real-Name

Possible values:

Any string, max. 251 characters from

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

Default:

Body

This table is used to manage the different language variants for the message text used by the Public Spot module for sending the login credentials via e-mail. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.1.21

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication****Language**

This parameter shows the language variant for the message text.

SNMP ID:

2.24.41.1.21.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Body****Content**

This parameter specifies the message text for the selected language. You can make use of a variety of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user.

The following **variables** are available:

\$PSpotPasswd

Placeholder for user-specific password for the Public Spot access.

\$PSpotLogoutLink

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

The following **control characters** are available:

\n

CRLF (carriage return, line feed)

\t

Tabulator

\<ASCII>

ASCII code of the corresponding character



If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

SNMP ID:

2.24.41.1.21.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Body**

Possible values:

Any string, max. 251 characters from

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

Default:**Subject**

This table is used to manage the different language variants for the subject line used by the Public Spot module in the e-mails containing the login credentials. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.1.22

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication

Language

This parameter shows the language variant for the subject line.

SNMP ID:

2.24.41.1.22.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Subject

Content

This parameter specifies the subject line for the selected language. You can make use of the following control characters.

\n

CRLF (carriage return, line feed)

\t

Tabulator

\<ASCII>

ASCII code of the corresponding character



If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

SNMP ID:

2.24.41.1.22.2

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail-Authentication > Subject

Possible values:

Any string, max. 251 characters from

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

Default:**Name**

This table is used to manage the different language variants for the sender names used by the Public Spot module for sending the login credentials via e-mail2MSM. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.2.23

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication****Language**

This parameter shows the language variant for the sender name.

SNMP ID:

2.24.41.2.23.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Real-Name****Content**

This parameter sets the sender name for the selected language.

SNMP ID:

2.24.41.2.23.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Real-Name****Possible values:**

Any string, max. 251 characters from

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

Default:**Body**

This table is used to manage the different language variants for the message text used by the Public Spot module for sending the login credentials via e-mail2MSM. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.2.24

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication**

Language

This parameter shows the language variant for the message text.

SNMP ID:

2.24.41.2.24.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Body

Content

This parameter specifies the message text for the selected language. You can make use of a variety of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the SMS gateway.

The following **variables** are available:

\$PSpotPasswd

Placeholder for user-specific password for the Public Spot access.

\$PSpotLogoutLink

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

The following **control characters** are available:

\n

CRLF (carriage return, line feed)

\t

Tabulator

\<ASCII>

ASCII code of the corresponding character



If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

SNMP ID:

2.24.41.2.24.2

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Body

Possible values:

Any string, max. 251 characters from

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

Default:**Subject**

This table is used to manage the different language variants for the subject line used by the Public Spot module for sending the login credentials via e-mail2MSM. If you do not specify any text for a language, the device automatically enters the internal default text.

SNMP ID:

2.24.41.2.25

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > E-mail2SMS-Authentication****Language**

This parameter shows the language variant for the subject line.

SNMP ID:

2.24.41.2.25.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Subject****Content**

This parameter specifies the subject line for the selected language. You can make use of the following control characters.

\n

CRLF (carriage return, line feed)

\t

Tabulator

\<ASCII>

ASCII code of the corresponding character



If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

SNMP ID:

2.24.41.2.25.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > E-mail2SMS-Authentication > Subject****Possible values:**

Any string, max. 251 characters from

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

Default:**Login text**

This table is used to manage the login text.

The Public Spot module gives you the option to specify customized text, which appears on the login page inside the box of the registration form. This **login text** is stored in multiple languages, and the language which is issued depends on the language settings of the user's Web browser. If you do not specify any individual login text for a language, the device falls back to the English login text (if available).

SNMP ID:

2.24.60

Telnet path:

Setup > Public-Spot-Module

Language

This parameter indicates the language for the login text.

SNMP ID:

2.24.60.1

Telnet path:

Setup > Public-Spot-Module > Login-Text

Content

This parameter specifies the login text for the selected language. To type umlauts, you should 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 fill out the form.</i>
```

SNMP ID:

2.24.60.2

Telnet path:

Setup > Public-Spot-Module > Login-Text

Possible values:

Any string, max. 254 characters from

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

Default:

9.6 New URL placeholders (template variables)

A Public Spot gives you the option to include variables in the URL to be sent to the templates, i.e. to control the web pages displayed by the Public Spot module to a user.

As of LCOS 8.84 you can choose from the following additional variables:

%c

Inserts the LAN MAC address of the LANCOM device as a hexadecimal string of length 12. The output is in the format 'aa:bb:cc:dd:ee:ff'.

%p

Inserts the IP address of the LANCOM device into the ARF context of the respective client.

If your device is active in different IP networks, this variable enables you to specify the IP address used by the device in same the network as the client.

%r

Inserts the client's IP address.

9.7 User-dependent HTML output on the voucher

As of LCOS 8.84, you can add conditional HTML-code to the voucher page, which is only printed for specific users or administrators. You use this by entering the tag `<pbcond>` and the identifier `USER NAME`. `USER` is a prefix that **must** be placed before a space character and then the user name (`NAME`). For example, to generate HTML output specifically for the user 'root' when printing the voucher page, you use the following syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

When used in large-scale Public Spot scenarios with central administration—e.g. with a WLAN controller—this dependency can also be used to identify the site: To do this, you create a specific Public Spot admin account on each of the relevant access points and specify the conditional voucher text for the different administrators.

9.8 Show/hide the LANCOM logo and header image in the voucher

By default, a voucher issued by the device contains the 'Hotspot' header image and the logo "Powered by LANCOM". You can disable these graphics directly in the device with the option **Print header and company emblem**. There is no need to use a customized voucher template to remove these graphics. Using this option outputs a voucher containing neutral text only.

To decide whether the device shows a header image and logo when you create a voucher, go to the dialog **Public Spot > Wizard** and adjust the setting **Print header and company emblem**.

9.8.1 Additions to the Setup menu

Print logo and header image

In the default settings, the device outputs a voucher with the header image "Hotspot" and the logo "Powered by LANCOM". You have the option of disabling these graphics directly on the device without having to upload a customized version of the voucher template without the graphics. If you disable the graphics, a text-only voucher is issued.

SNMP ID:

2.24.35

Telnet path:

Setup > Public-Spot-Module

Possible values:

No

Yes

Default:

Yes

9.9 Additional languages for the authentication pages

With LCOS 8.84, the Public Spot module authentication pages now support the languages French, Spanish, Italian and Dutch (i.e. all pre-installed default pages except for the voucher page). This allows you to offer Public Spot access to a broader range of international users. The language displayed is determined by the settings in the Web browser used to access the Public Spot.



Multilingual support refers exclusively to the LCOS internal default pages. You can implement multilingual customized template pages with an external server.

9.10 Special template pages for Smart Ticket

The Public Spot module up until LCOS version 8.82 used a central login page to for all authentication modes. As of LCOS 8.84, you can optionally equip the device with separate template pages for the Smart Ticket function (for self-sufficient user registration via e-mail/SMS). Two pages have to be configured for registration via e-mail/SMS: **Registration(...)** and **Login(...)**.

- On the registration page, users enter their personal data (e-mail address or mobile phone number) to register for the Public Spot and to request its login data.
- On the login page, users then enter their credentials in order to authenticate at the Public Spot.

The following table provides an overview of the related dependencies that you need to create your own page templates:

Table 5: Overview of dependencies of the SmartTicket login pages

Authentication mode	Page designation	Local URL on your device	Page template identifiers
Login data will be sent by e-mail	Prelogin (e-mail)...	file://pbspot_template_reg_email	<regemailform>
	Authentication (e-mail)...	file://pbspot_template_login_email	<loginemailform>
Login data will be sent by SMS (text message)	Prelogin (e-mail to SMS)...	file://pbspot_template_reg_sms	<regsmsform>
	Login (e-mail to SMS)...	file://pbspot_template_login_sms	<loginsmsform>

9.10.1 Login pages depending on the login mode

The following table provides an overview of which login page is displayed by the device in the various authentication modes. If a login mode has no customized page template, the Public Spot module takes the default LCOS page:

Table 6: Overview of login pages of each authentication mode

Authentication mode	Page designation
No authentication required	–
No credentials required (login after agreement)	Welcome...
Authenticate with name and password	Login...
Authenticate with name, password and MAC address	Login...
Login data will be sent by e-mail	<ul style="list-style-type: none"> ■ Prelogin (e-mail)... ■ Authentication (e-mail)...
Login data will be sent by SMS (text message)	<ul style="list-style-type: none"> ■ Prelogin (e-mail to SMS)... ■ Login (e-mail to SMS)...

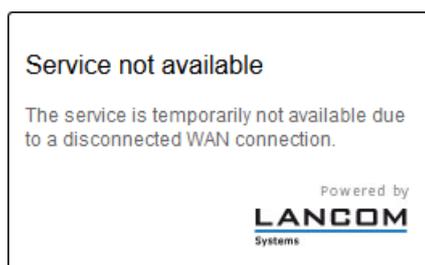
9.11 Error page in case of WAN connection failure

In addition to the general login error pages, you can also inform non-authenticated Public Spot users of a WAN connection error. Potential users are informed about the lack of network availability beforehand. This **Error** page is displayed whenever the Public Spot module registers a WAN link failure.

In order for the error page to be displayed properly, a corresponding remote site **must** be named, the connection to which is monitored by the Public Spot module. Make an appropriate entry in the dialog **Public Spot > Server Remote site**. The **Select** button allows you to assign an existing entry to the input field, or to create a new remote site.

! If no remote site is named for monitoring, the Public Spot module disables the display of the connection error page. If the WAN connection fails, unauthenticated will not see an error page and their browsers will timeout instead.

On your custom error page, use the identifier `LOGINERRORMSG` to insert the error message issued by LCOS in case of a WAN link failure. In the event of a WAN link failure, the following error message is displayed:



Users who are already authenticated will see an appropriate error message from their browser.

9.11.1 Additions to the Setup menu

WAN connection

The Public Spot module monitors the connection status of the remote station named here. If the WAN connection should fail, a corresponding message appears on the error page shown to unauthenticated users. This gives potential users information about the lack of network availability in advance.

If no remote station is named, the Public Spot module will not output connection errors on the error page. In case of a failure of the WAN connection, unauthenticated users will instead experience a connection timeout by their browser.

Already authenticated users, however, always receive an error message from their browser, irrespective of the error page.

SNMP ID:

2.24.34

Telnet path:**Setup > Public-Spot-Module****Possible values:**

Valid name of a remote station, max. 16 characters

Default:

9.12 Template caching

When configuring user-defined template pages on devices with sufficient memory (e.g., Public Spot gateways), you have the option to cache templates on the device. Caching improves the performance of the Public Spot module, particularly in large-scale scenarios where the device internally caches templates and the HTML pages that were generated from them.

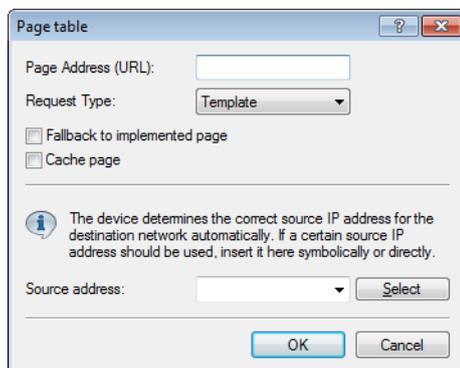
Caching is possible for:

- Templates stored in the local file system
- Templates stored on external HTTP(S) servers with static URLs

Templates on external servers that are referenced with template variables are not cached on the system.

Enable template caching

In LANconfig under **Public Spot > Server > Page table > <Name of the page template>**, caching for a page template is enabled by setting **Cache page**.



The corresponding parameter can be found under **Public Spot Module > Page table > Template cache**.

Delete template cache

The device automatically deletes or updates the templates stored in the cache once you load a new template file in the file system of your device (for local storage) or when the cache period for an HTTP(S) template runs out (for storage on an external server). The device evaluates the `Cache control` header of an HTTP(S) template in order to determine the maximum cache period.

! If no `Cache control` header is set, the website is not cached and is immediately discarded. When setting up an individual template, ensure that you combine any `META` tag with a reasonable cache period (in seconds),

for example, `<meta http-equiv="cache-control" content="max-age=60">`. The duration of the cache period depends on the scenario; there are no specific recommendations.

However, you do have the option of manually deleting the template cache with an action. In the status menu under **Public Spot** you can do this by starting the action **Flush template cache**.

9.12.1 Additions to the Status menu

Flush template cache

This action is for the manual deletion of the template cache.

The device automatically deletes and/or updates the templates stored in the cache once a new template file is uploaded to the file system of your device (local storage) or upon expiry of the cache time for an HTTP(S) template (storage on an external server). For this purpose, the device evaluates the `Cache-Control` header of an HTTP(S) template to discover the maximum cache time.

SNMP ID:

1.44.9

Telnet path:

Setup > Public-Spot

9.12.2 Additions to the Setup menu

Template cache

Using this parameter, you enable caching of Public Spot templates.

When configuring user-defined template pages on devices with sufficient memory (e.g., Public Spot gateways), you have the option to cache templates on the device. Caching improves the performance of the Public Spot module, particularly in large-scale scenarios where the device internally caches templates and the HTML pages that were generated from them.

Caching is possible for:

- Templates stored in the local file system
- Templates stored on external HTTP(S) servers with static URLs

Templates on external servers that are referenced with template variables are not cached on the system.

SNMP ID:

2.24.8.6

Telnet path:

Setup > Public-Spot-Module > Page-Table

Possible values:

No

Yes

Default:

No

9.13 Quick link to the session information window

As of LCOS 8.84, users who are logged-in to the Public Spot can enter the short URL `http://logout` into the address bar to access the session information window and to logout of the Public Spot. Users who closed the browser window, either accidentally or on purpose, can quickly restore the page using this short URL.

9.13.1 Additions to the Setup menu

Print logout link

This parameter determines whether a voucher printout shows the URL for logging out from the Public Spot.



In order for the correct URL to appear on the voucher, the parameter **Device host name** (SNMP ID 2.24.22) must contain the value `logout`.

SNMP ID:

2.24.37

Telnet path:

Setup > Public-Spot-Module

Possible values:

No

Yes

Default:

Yes

10 RADIUS

10.1 Targeted (de-)activation of RADIUS user accounts

As of LCOS 8.84, have the option to enable or disable individual RADIUS user accounts. In LANconfig, this is done under **RADIUS Server > General > User database** using the **Entry active** option. This makes it possible, for example, to disable individual accounts temporarily without deleting the entire account.

10.1.1 Additions to the Setup menu

Active

Using this parameter, you specifically enable or disable individual RADIUS user accounts. This makes it possible, for example, to disable individual accounts temporarily without deleting the entire account.

SNMP ID:

2.25.10.7.20

Telnet path:

Setup > RADIUS > Server > Users

Possible values:

No

Yes

Default:

Yes

10.2 Login to the LCOS administration interface via RADIUS

As of LCOS version 8.84, logging in to the administration interface can now be controlled via RADIUS as well as TACACS+.

10.2.1 Login to the LCOS administration interface via RADIUS

Currently there are three ways to login to the LANCOM administration interface:

- **internal:** The LANCOM handles the user management itself by means of user login name, password, and the assignment of access and function rights.
- **TACACS+:** User management is handled by a TACACS+ server in the network.
- **RADIUS:** User management is handled by a RADIUS server in the network.

The user can login with RADIUS over the following connections:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

 A RADIUS authentication over SNMP is currently not supported.

 A RADIUS authentication via LL2M (LANCOM Layer 2 Management protocol) is not supported as LL2M requires plain-text access to the password stored in the LANCOM.

The RADIUS server handles user management with regard to authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin accounts in large network installations with multiple routers.

Authentication via a RADIUS server is conducted as follows:

1. On login, the LANCOM sends the user credentials to the RADIUS server in the network. The necessary server data are in stored in the LANCOM.
2. The server checks the credentials for their validity.
3. If the credentials are invalid, it sends the LANCOM a corresponding message and the LANCOM aborts the login process with an error message.
4. If the credentials are valid, the server informs the LANCOM that the user has permission of access, and also sends information on the access rights and function rights, so that the user has access only to the corresponding functions and directories.
5. If the user's sessions are budgeted by the RADIUS server (accounting section), the LANCOM stores the session data such as start, end, user name, authentication mode and, if available, the port used.

10.2.2 Additions to the Setup menu

Authentication

This menu item is eliminated with the introduction of authentication via RADIUS.

The authentication method is now selected under **Setup > Config > Authentication** (see [Authentication](#)).

Authentication

Various options are available to log on to the LANCOM's administration interface:

- **Internal:** The LANCOM manages the users internally in the table **Setup > Config > Admins**.

- **Radius:** A RADIUS server handles user management.
- **Tacacs+:** A TACACS+ server handles user management.

! The data relating to the RADIUS server is managed under **Setup > Config > RADIUS > Server**. The data relating to the TACACS+ server is managed under **Setup > Tacacs+ > Server**.

! Since the RADIUS protocol does not allow for password changes, users who have logged in via RADIUS cannot change their password in the LANCOM.

SNMP ID:

2.11.80

Telnet path:

Setup > Config

Possible values:

Internal

Radius

TACACS+

Default:

Internal

Radius

If the user login to the LANCOM administration interface is to be authenticated by RADIUS server, you specify the necessary server data and the additional administrative data here.

SNMP ID:

2.11.81

Telnet path:

Setup > Config

Server

This table contains the settings for the RADIUS server.

SNMP ID:

2.11.81.1

Telnet path:

Setup > Config > Radius

Name

Enter a name for the RADIUS server here.

SNMP ID:

2.11.81.1.1

Telnet path:

Setup > Config > Radius > Server

Possible values:

Max. 16 characters

Default:

Blank

Server

Enter the IPv4 address of the RADIUS server here.

SNMP ID:

2.11.81.1.2

Telnet path:

Setup > Config > Radius > Server

Possible values:

Max. 64 characters

Default:

Blank

Port

Enter the port used by the RADIUS server to communicate with the LANCOM.

SNMP ID:

2.11.81.1.3

Telnet path:

Setup > Config > Radius > Server

Possible values:

Max. 5 characters

Default:

1812

Protocol

Enter the protocol used by the RADIUS server to communicate with the LANCOM.

SNMP ID:

2.11.81.1.4

Telnet path:

Setup > Config > Radius > Server

Possible values:

RADIUS

RADSEC

Default:

RADIUS

Loopback address

This is where you can configure an optional sender address to be used by the LANCOM instead of the one that would normally be automatically selected for this target address.

SNMP ID:

2.11.81.1.5

Telnet path:

Setup > Config > Radius > Server

Possible values:

Name of the IP networks whose addresses are to be used by the LANCOM.

"INT" for the address of the first intranet.

"DMZ" for the address of the first DMZ.



If the list of IP networks or loopback addresses contains an entry named 'DMZ', then the LANCOM uses the associated IP address.

LB0 to LBF for one of the 16 loopback addresses

Any valid IP address

Default:

Blank

Secret

Enter the password for accessing the RADIUS server here, and repeat the entry in the second input field.

SNMP ID:

2.11.81.1.6

Telnet path:

Setup > Config > Radius > Server

Possible values:

Max. 64 characters

Default:

Blank

Backup

Enter the name of the alternate RADIUS server to which the LANCOM forwards its requests if the first RADIUS server is unavailable.



The backup server requires an additional entry in the Server table.

SNMP ID:

2.11.81.1.7

Telnet path:**Setup > Config > Radius > Server****Possible values:**

Max. 16 characters

Default:

Blank

Category

Set the category for the RADIUS server.

You can select neither, one or both categories.

SNMP ID:

2.11.81.1.8

Telnet path:**Setup > Config > Radius > Server****Possible values:**

Authentication

Accounting

Default:

Authentication

Access rights transfer

The authorization of the user is stored in the RADIUS server. When a request arrives, the RADIUS server sends the access- and function rights to the LANCOM along with the login data, which then logs in the user with the appropriate privileges.

Access rights are usually defined in the RADIUS management privilege level (attribute 136), and the LANCOM simply maps this value to its internal access rights (option: "Mapped"). The attribute can have the following values, which are then mapped by the LANCOM:

- 1: User, read-only
- 3: User, write-only
- 5: Admin, read only, no trace rights
- 7: Admin, read and write, no trace rights
- 9: Admin, read-only
- 11: Admin, read and write
- 15: Supervisor
- The LANCOM maps any other values to "no access".

However, some RADIUS servers may also need to assign function rights, they may use attribute 136 differently, or they may use different, vendor-specific attributes for the authorization. In this case, you must select the vendor-specific attributes. These attributes are defined as follows, based on the LANCOM vendor ID '2356':

- Access rights ID: 11
- Function rights ID: 12

The transferred access-right values are identical to the above. If the RADIUS server also has to transfer function rights, you achieve this as follows:

1. Open the console for the LANCOM.
2. Change to the directory **Setup > Config > Admins**.
3. The command `set?` shows you the current mapping of the function rights to the corresponding hexadecimal code (e.g. `Device-Search (0x80)`).
4. To combine function rights, you add their hex values together.
5. Convert the hexadecimal value to a decimal number.
6. By using this decimal value in the function rights ID, you can transfer the corresponding rights.

SNMP ID:

2.11.81.2

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

Vendor-specific

Mapped

Default:

Vendor-specific

Accounting

Here, you specify whether the LANCOM should record the user's session. In this case, session data is saved including the start, end, username, authentication mode and, if available, the port used.

SNMP ID:

2.11.81.3

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

No

Yes

Default:

No

10.2.3 Enhancements to LANconfig

Login to the LCOS administration interface via RADIUS

Currently, users can login to the administration interface of the device by using RADIUS, TACACS+, or the internal user management of the device.

With RADIUS, this is possible over the following connections:

- Telnet
- SSH
- WEBconfig

- TFTP
- Outband

! A RADIUS authentication over SNMP is currently not supported.

! A RADIUS authentication via LL2M (LANCOM Layer 2 Management protocol) is not supported as LL2M requires plain-text access to the password stored in the LANCOM.

The RADIUS server handles user management with regard to authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin accounts in large network installations with multiple routers.

Authentication via a RADIUS server is conducted as follows:

1. On login, the LANCOM sends the user credentials to the RADIUS server in the network. The necessary server data are in stored in the LANCOM.
2. The server checks the credentials for their validity.
3. If the credentials are invalid, it sends the LANCOM a corresponding message and the LANCOM aborts the login process with an error message.
4. If the credentials are valid, the server informs the LANCOM that the user has permission of access, and also sends information on the access rights and function rights, so that the user has access only to the corresponding functions and directories.
5. If the user's sessions are budgeted by the RADIUS server (accounting section), the LANCOM stores the session data such as start, end, user name, authentication mode and, if available, the port used.

In the LANconfig, you can set the authentication method under **Management > Authentication**.

The screenshot shows two configuration sections. The first section, 'Device Login Authentication', has a dropdown menu for 'Authentication via:' set to 'Internal administrator table'. The second section, 'RADIUS authentication', has a dropdown menu for 'Access rights via:' set to 'Provider specific attribute', a dropdown for 'Accounting:' set to 'No', and a 'RADIUS server...' button.

In the section **Device login authentication**, you choose the method for users to authenticate when accessing the LANCOM administration interface:

- Internal administrator table: The LANCOM handles the user management itself by means of user login name, password, and the assignment of access and function rights.
- RADIUS: User management is handled by a RADIUS server in the network.
- TACACS+: User management is handled by a TACACS+ server in the network.

In the **RADIUS authentication** section, you enter the necessary RADIUS server data and additional administrative data.

Access rights via

The authorization of the user is stored in the RADIUS server. When a request arrives, the RADIUS server sends the access- and function rights to the LANCOM along with the login data, which then logs in the user with the appropriate privileges.

Access and function rights are usually defined in the RADIUS management privilege level (attribute 136), and the LANCOM simply maps these values to its internal access and function rights. However, some RADIUS

servers use this attribute differently, or they may use different, vendor-specific attributes for the authorization. In this situation, the LANCOM is also able to evaluate provider-specific authorizations. Possible values are:

- Provider-specific attribute: The LANCOM processes the provider-specific attribute (default).
- Management privilege level attribute: The LANCOM processes the RADIUS server's management privilege level attribute.

Accounting

Here, you specify whether the LANCOM should record the user's session. Possible values are:

- No: The LANCOM does not record any session data (default).
- Yes: The LANCOM records the session data (start, end, user name, authentication mode, port).

RADIUS server

This table is used to define the RADIUS server settings.

- **Profile name:** Enter a name for the RADIUS server here.
- **Backup profile:** Enter the name of the alternate RADIUS server to which the LANCOM forwards its requests if the first RADIUS server is unavailable.



The backup server requires an additional entry in the Server table.

- **Server address:** Enter the IPv4 address of the RADIUS server here.
- **Port:** Enter the port used by the RADIUS server to communicate with the LANCOM (default: 1812).
- **Shared secret:** Enter the password for accessing the RADIUS server here, and repeat the entry in the second input field.
- **Source address:** This is where you can configure an optional sender address to be used by the LANCOM instead of the one that would normally be automatically selected for this target address.
- **Protocol:** Enter the protocol used by the RADIUS server to communicate with the LANCOM. Possible values are:
 - RADIUS (default)
 - RADSEC
- **Category:** Set the category for the RADIUS server. Possible values are:
 - Deactivated
 - Authentication (default)
 - Accounting
 - Authentication & accounting

10.3 Separate RADIUS accounting server for each SSID

As of LCOS 8.84 you can assign a separate RADIUS accounting server to each logical WLAN interface.

10.3.1 Additions to the Setup menu

Servers

This table provides the option to configure alternative RADIUS accounting servers for logical WLAN interfaces. This means that you can use special accounting servers for selected WLAN interfaces instead of the globally configured server.

SNMP ID:

2.12.45.17

Telnet path:

Setup > WLAN > RADIUS-Accounting

Name

Name of the RADIUS server performing the accounting for WLAN clients. The name entered here is used to reference that server from other tables.

SNMP ID:

2.12.45.17.1

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

String, max. 16 characters from

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

Default:

Server address

IP address of the RADIUS server used to perform the accounting for WLAN clients.



The general values for retry and timeout must also be configured in the RADIUS section.

SNMP ID:

2.12.45.17.2

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

Valid IPv4 address

Default:

0.0.0.0

Port

Port for communication with the RADIUS server during accounting

SNMP ID:

2.12.45.17.3

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

0 to 65535

Default:

0

Key

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that in the accounting server.

SNMP ID:

2.12.45.17.4

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

Any valid shared secret, max. 64 characters

Default:**Loopback addr.**

You have the option to enter a different address here (name or IP) to which the RADIUS accounting server sends its reply message.

By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

SNMP ID:

2.12.45.17.5

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

- Name of the IP network (ARF network), whose address should be used.
- INT for the address of the first Intranet
- DMZ for the address of the first DMZ



If an interface with the name "DMZ" already exists, the device will select that address instead.

- LB0...LB15 for one of the 16 loopback addresses or its name
- Any IPv4 address



If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

Default:**Protocol**

Using this item you specify the protocol that the accounting server uses.

SNMP ID:

2.12.45.17.6

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

RADIUS

RADSEC

Default:

RADIUS

Backup

Enter the name of the RADIUS backup server used for the accounting of WLAN clients if the actual accounting server is not available. This allows you to configure a backup chaining of multiple backup servers.

SNMP ID:

2.12.45.17.7

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

Name from **Setup > WLAN > RADIUS-Accounting > Servers**, max. 16 characters

Default:**Accounting server**

An alternate RADIUS accounting server for this logical WLAN interface. If you leave this field blank, the device uses the globally configured accounting server (if RADIUS accounting is enabled on the interface).

SNMP ID:

2.23.20.1.22

Telnet path:

Telnet path: Setup > Interfaces > WLAN > Network

Possible values:

Name from **Setup > WLAN > RADIUS-Accounting > Servers**, max. 16 characters

Default:

11 Sending and receiving SMS text messages

If your device has a 3G/4G WWAN module, is capable of sending and receiving text messages via the Short Message Service (SMS).

In this case the SMS function is mainly used as a messaging and function-enhancing interface for the internal LCOS modules, but also for external instances such as routers, management solutions, accounting systems, and so on. You as a user also have the option to send SMS text messages using the corresponding *function in LANmonitor* or the `smssend` command at the command prompt. LANmonitor also provides you with convenient functions for *managing* sent and received messages.

 The sending and receiving of SMS text messages must also be included in the SIM card's contract.

11.1 Receiving SMS text messages

Your device uses the ETSI standard TS 127.005 to receive and request these SMS text messages, to store them and, if required, to log the receipt of an SMS to the SYSLOG. The entry in the SYSLOG counts as a "notice" to inform you about any important messages, such as a notification from an external instance, for example. An instance might be the accounting system of your provider:

If you connect to the Internet via a 3G/4G WWAN module and the contract with your Internet provider includes a volume limit, then depending on the contract your provider will throttle or stop data transfer once this volume limit has been reached. In countries with the appropriate legislation, this also applies when a charging limit for data roaming has been reached. Before the data transfer is throttled or stopped, many providers send an SMS text message informing the customer that the volume limit has been reached. With the corresponding notification settings in the SYSLOG and/or via e-mail, the device can immediately inform you about the reception of the SMS, so that you can respond promptly.

11.2 Basic configuration of the SMS module

The following steps show you the basic configuration of the SMS module in a 3G/4G WWAN-enabled device.

1. Start LANconfig and open the configuration dialog for the device.
2. Navigate to the menu item **Log & trace > SMS messages**.



SMS messages

The device is capable of sending and receiving SMS messages.

 For utilization, the used SIM card must support SMS transmission and reception.

Inbox size: messages

Deletion of sent messages:

Outbox size: messages

Mail forward address:

Syslog messaging:

3. Under **Inbox size** you set the maximum number of text messages stored in the device inbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value 0 disables the limit, i.e. an unlimited number of messages will be stored.

4. The item **Deletion of sent messages** decides how the device handles sent text messages.
 - **Immediately**: Sent messages are not saved.
 - **Never**: Sent messages are saved permanently.
5. Under **Outbox size** you set the maximum number of text messages stored in the device outbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value 0 disables the limit, i.e. an unlimited number of messages will be stored.
6. Under **Syslog messaging** you specify if and how the arrival of text messages is logged to the SYSLOG.
 - **No**: Incoming text messages are not logged to SYSLOG.
 - **Only sender/no content**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number.
 - **Full**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number and the message in full.
7. Optional: Under **Mail forwarding address** you specify the e-mail address to which the device is to forward the incoming SMS text messages.

! E-mail routing will only work if a valid SMTP account is configured in the device.

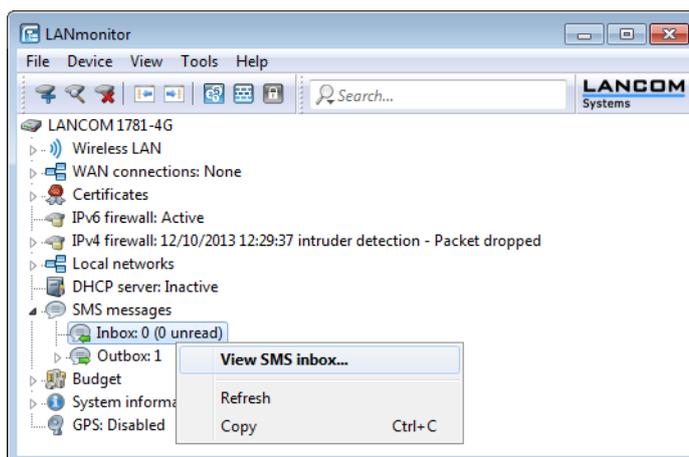
8. Now write the configuration back to the device.

That's it! This concludes the basic configuration of the SMS module.

11.3 Managing SMS text messages with LANmonitor

The following section explains shows how you can use LANmonitor to read and delete text messages sent or received by a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages > Inbox** or **Outbox**. If there are already text messages on the device, LANmonitor displays the last five received messages under **Inbox** and the last five sent messages under **Outbox**.
2. Open the context menu on the entry and choose **Show SMS inbox** or **Show SMS outbox**.



LANmonitor then displays a window listing all of the sent and received text messages and their status. In the **Inbox** you have the option to delete single or multiple selected messages, or to mark them as read/unread; the Status shows whether they have been read or not (**New** or **Read**). In the **Outbox**, the messages can only be deleted; the Status shows their send status (**Sent** or **Unsent**).

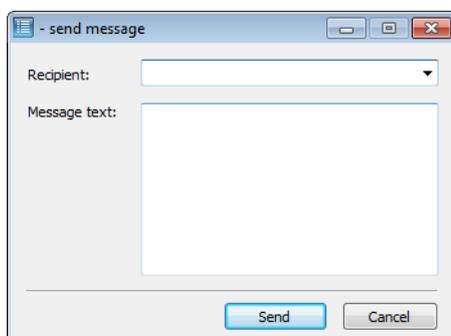
You can manage these messages by using the context menu. To delete all messages in the inbox or outbox, go to the menu bar under **Messages** and select the appropriate action.

 You can easily toggle between the inbox and outbox by selecting **View** from the menu bar and selecting the desired option.

11.4 Sending SMS text messages with LANmonitor

The following section explains how you can use LANmonitor to send SMS text messages via a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages**.
2. Open the context menu on the entry and select **Send message**.
3. In the Editor window that opens, enter the phone number of the recipient and the message content to be sent. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section [Character set for sending SMS](#) on page 144.



4. Click **Send** to send the message via the internal SMS module.

11.5 URL placeholder for sending SMS text messages

You have the option of addressing the SMS module as an interface by means of a URL. By integrating predefined placeholders (parameters) into the URL, you can use the device to send SMS text messages by means of an HTTP(S) call. This makes LANCOM cellular routers ideal for use as an SMS gateway.

 SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

You use your access credentials to authenticate at the device; just how these are integrated into the URL is determined by your browser's requirements. The typical notation is `Username:Password@Host`.

 Depending on the use case (for example, SMS gateway), we recommended that you create an administrator without access rights (**None**) and with just one function right, **Send SMS**.

 Not all Web browsers support the transmission of credentials via the URL. This includes current versions of the Microsoft Internet Explorer, among others. In this case you should use another browser to send SMS via the URL.

The URL call uses the syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&...&oldauth
```

11 Sending and receiving SMS text messages

The parameter `oldauth` is **vital**, otherwise none of the available browsers will send the access credentials to the device. In addition, the following placeholders are defined:

DestinationAddress

Phone number to which the device should send the SMS. The same conventions apply as for normal telephone calls. Specify the parameters as follows:

```
&DestinationAddress=01511234567  
&DestinationAddress=00491511234567
```

Content

Content of the text message. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section [Character set for sending SMS](#) on page 144.

Spaces and other special characters to be included into an SMS must be sent to the device in the URL-encoded form. For example, spaces are encoded with `%20` and full stops with `%2E`. Specify the parameters as follows:

```
&Content=This%20is%20a%20message%2E
```

Learn more about this topic on the Internet under the keyword "URL encoding" and also at www.w3schools.com.



Some browsers perform the URL encoding automatically. Despite this, we recommend that you encode the content yourself to ensure that all of the characters are converted correctly.

11.6 Character set for sending SMS

An SMS can contain a maximum of 160 characters (each of 7 bits = 1,120 bits). These are made up of the GSM basic character set (total of 128 characters) as well as selected characters from the extended GSM character set. Although the extended character set allows the use of some additional characters, these take up twice the space and correspondingly reduce the maximum number of characters that the SMS can contain. Characters not implemented in the SMS module are ignored by the device.

The following characters are defined in the **GSM basic character set**:

@	Δ	SP	0	i	P	ı	p
£	_	!	1	A	Q	a	q
\$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	α	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(8	H	X	h	x
Ç	Θ)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü

The following characters are implemented from the **extended GSM character set**:

{|}[]~^\\€

11.7 Additions to the Status menu

11.7.1 SMS

This menu contains the status values for the SMS module that handles the sending and receiving of text messages (SMS).

SNMP ID:

1.83

Telnet path:

Status

Inbox

This table caches all text messages (SMS) received by the device.

SNMP ID:

1.83.1

Telnet path:

Status > SMS

Idx

This status shows the index entry of the text message.

MsgRef

This status value groups multiple parts of a message into a single multi-part message.

PartNo

This status value indicates the order of multi-part messages.

Sender

This status value shows the number of the phone that sent the message to the device.

Status

This status value indicates the read status for the message, i.e. if a message was already read by an administrator or not.

Possible values:

- new
- read

Time stamp

This status value shows the time when the text message was received.

Contents

This status value displays the contents of the received message.

Outbox

This table stores all text messages (SMS) sent by the device.

SNMP ID:

1.83.2

Telnet path:

Status > SMS

Idx

This status shows the index entry of the text message.

MsgRef

This status value groups multiple parts of a message into a single multi-part message.

PartNo

This status value indicates the order of multi-part messages.

Destination

This status value shows the phone number that sent the device sent the message to.

Status

This status value displays the transmission status of the text message.

Possible values:

- **Unsent:** The message was not yet passed to the radio module.
- **Sent:** The message was passed to the service center for delivery to the recipient.

Time stamp

This status value shows the time when the text message was send.

Contents

This status value displays the contents of the sent message.

Inbox messages

This status value indicates the total number of messages that are in the Inbox.

SNMP ID:

1.83.3

Telnet path:

Status > SMS

Unread messages

This status value indicates the total number of unread messages in the inbox.

SNMP ID:

1.83.4

Telnet path:

Status > SMS

Outbox messages

This status value indicates the total number of messages in the outbox.

SNMP ID:

1.83.5

Telnet path:

Status > SMS

SMSC address

This status value displays the phone number of the service center as stored on the USIM card of the device. In this case, the service center is a unit in the network of your service provider, which forwards the messages between the network and the device, and which caches them if necessary. The device uses this number unless there is a different number under [SNMP-ID 2.83.1](#).

SNMP ID:

1.83.6

Telnet path:

Status > SMS

Clear inbox

This action clears the table [1.83.1](#).

SNMP ID:

1.83.7

Telnet path:**Status > SMS****Possible parameters:**

No parameters available

Clear outboxThis action clears the table [1.83.2](#).**SNMP ID:**

1.83.8

Telnet path:**Status > SMS****Possible parameters:**

No parameters available

Mark read inboxWith this action you can mark all of the messages stored in the table [1.83.1](#) as read.**SNMP ID:**

1.83.9

Telnet path:**Status > SMS****Possible parameters:**

No parameters available

11.8 Additions to the Setup menu

11.8.1 SMS

This menu contains the settings for the SMS module that handles the sending and receiving of text messages (SMS).

SNMP ID:

2.83

Telnet path:**Setup****SMSC address**

This parameter allows you to configure an alternative number for the "short message service center" (SMSC).

By default, the device uses the phone number stored in the USIM card, which you can view by calling the status value **SMSC number** (*SNMP ID 1.83.5*). The SMS messages can be sent to a specific SMSC if you specify a different phone number.

SNMP ID:

2.83.1

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

Valid SMSC phone number, max. 31 characters

Default:**Inbox size**

This parameter lets you set the maximum number of text messages stored in the device inbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry.

SNMP ID:

2.83.2

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

0 to 999999

Special values:

0: This value disables the limit, i.e. an unlimited number of messages will be stored.

Default:

100

Outbox size

This parameter lets you set the maximum number of text messages stored in the device outbox. If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry.

SNMP ID:

2.83.3

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

0 to 999999

Special values:

0: This value disables the limit, i.e. an unlimited number of messages will be stored.

Default:

100

Outbox preservation

This parameter defines what the device does with sent text messages.

SNMP ID:

2.83.4

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

- **None:** Sent messages are not saved.
- **All:** Sent messages are saved permanently.

Default:

All

Mail-Forward-Addr.

This parameter sets an optional e-mail address, to which the device will forward any incoming text messages.



E-mail routing will only work if a valid SMTP account is configured in the device.

SNMP ID:

2.83.5

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

Any valid e-mail address, max. 31 characters

Default:**Syslog**

This parameter specifies if and how the arrival of text messages is logged to the SYSLOG.

SNMP ID:

2.83.8

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

- **No:** Incoming text messages are not logged to SYSLOG.
- **SenderOnly:** The arrival of a text message is recorded to the SYSLOG together with the sender's phone number.
- **Full:** The arrival of a text message is recorded to the SYSLOG together with the sender's phone number and the message in full.

Default:

No

11.9 Enhancements to command-line commands

11.9.1 SMS send command

As of LCOS 8.84, you can manually send SMS text messages with the command-line entry `smssend`, assuming that your device has a 3G/4G WWAN module.

Table 7: Overview of all commands available at the command line

Command	Description
<code>smssend [-s <SMSC-Number>] (-d <Destination>) (-t <Text>)</code>	<p>Available only on devices with 3G/4G WWAN module: Sends a text message to the destination number entered.</p> <ul style="list-style-type: none"> ■ <code>-s <SMSC-Number></code>: Alternative SMSC phone number (optional). If you omit this part of the command, the device uses the phone number stored on the USIM card or that configured under SNMP ID 2.83. ■ <code>-d <Destination></code>: Destination phone number ■ <code>-t <Text></code>: Contents of the message with ≤ 160 characters. For an overview of available characters, see the section Character set for sending SMS on page 144. Special characters must be in UTF8 encoded form.

Legend

- Characters and brackets:
 - Objects, in this case dynamic or situation-dependent, are in angle brackets.
 - Round brackets group command components, for a better overview.
 - Vertical lines (pipes) separate alternative inputs.
 - Square brackets describe optional switches.

It follows that all command components that are not in square brackets are necessary information.