connecting your business



# Addendum LCOS 9.20 RC2



## Contents

1 Addendum to LCOS version 9.20	7
2 Overview of new features of the LCOS version 9.20	8
3 Configuration	11
3.1 Preventing password form fields in the browser from storing passwords	11
3.1.1 Preventing password form fields in the browser from storing passwords	11
3.1.2 Additions to the Setup menu	11
3.2 DHCP rollout agent	12
3.2.1 Receiving LSR information via DHCP server (zero-touch rollout)	12
3.2.2 Additions to the Setup menu	17
3.3 Support of ChaCha20/Poly1305 for SSH access	23
3.3.1 Additions to the Setup menu	23
3.4 Enforcing password complexity for device passwords	24
3.4.1 Additions to the Setup menu	25
3.5 LBS server 1.1: Making elements in the LBS measurements fields selectable	25
3.5.1 Making elements in the LBS measurements fields selectable in WEBconfig	26
3.5.2 Additions to the Setup menu	26
3.6 Preventing the storage of passwords in WEBconfig	30
3.6.1 Additions to the Setup menu	
3.7 LANconfig: Icon for *.LCS files in Windows Explorer	31
4 Diagnosis	32
4.1 Specifying the SYSLOG server address as an IPv6 address or DNS name	
4.2 IPv6 support for LCOScap	32
5 Routing and WAN connections	33
5.1 Border Gateway Protocol version 4 (BGPv4)	33
5.1.1 Border Gateway Protocol version 4 (BGPv4)	
5.1.2 Best-path selection algorithm	
5.1.3 Tutorial: Setting up BGPv4 under LANconfig	
5.1.4 Tutorial: Setting preferences for prefixes	
5.1.5 Tutorial: Setting the Community attribute	61
5.1.6 Tutorial: Filtering received prefixes	63
5.1.7 Additions to the Setup menu	65
5.1.8 Additions to the Status menu	125
5.2 Route monitor	133
5.2.1 Route monitor	133
5.2.2 Additions to the Setup menu	134
5.2.3 Additions to the Status menu	138
5.3 DiffServ field enabled by default	141
-	1/1
5.3.1 Additions to the Setup menu	

	5.4.1 Bandwidth measurements with iPerf	142
	5.4.2 Setting up iPerf with LANconfig	143
	5.4.3 Temporary iPerf server and client	144
	5.4.4 Analyzing iPerf results with LANmonitor	144
	5.4.5 iPerf commands on the command line	145
	5.4.6 Additions to the Setup menu	146
	5.4.7 Additions to the Status menu	150
5.5	5 SLA monitor	163
	5.5.1 SLA monitoring	163
	5.5.2 Configuring SLA monitoring with LANconfig	163
	5.5.3 Displaying the SLA monitoring results in LANmonitor	165
	5.5.4 Additions to the Status menu	166
	5.5.5 Additions to the Setup menu	171
5.6	5 Additional DSL-modem status values	179
	5.6.1 Read out DSL modem status values with LANmonitor	179
	5.6.2 Additions to the Status menu	
5.7	Displaying the mobile/cellular standards	
	5.7.1 Additions to the Setup menu	
	5.7.2 Additions to the Status menu	
6 IPv6		184
6.1	IPv6 support for (S)NTP client and server	
	6.1.1 Configuring the time server under LANconfig	
	6.1.2 Additions to the Setup menu	
7 VPN		
7.1	IKEv2 support	
	7.1.1 Functions of the VPN module	
	7.1.2 IKEv2	
	7.1.3 Configuring IKEv2 with LANconfig	
	7.1.4 Tutorial: Setting up IKEv2 under LANconfig	
	7.1.5 Additions to the Setup menu	
7.2	PIKEv2 fragmentation support	
	7.2.1 IKEv2 fragmentation	
	7.2.2 Additions to the Setup menu	
7.3	RADIUS support for IKEv2	
	7.3.1 RADIUS support for IKEv2	
	7.3.2 Additions to the Setup menu	
	7.3.3 Additions to the Status menu	
7.4	IKEv2 routing support	
	7.4.1 IPv4 routing	
	7.4.2 IPv6 routing	
	7.4.3 Additions to the Setup menu	
7.5	5 "Match Remote Identity" for IKEv2	
	7.5.1 Identity list	
	7.5.2 Identities	

## Addendum

	7.5.3 Additions to the Setup menu	
	7.6 Redirect mechanism for IKEv2	271
	7.6.1 Additions to the Setup menu	271
	7.7 VPN via IPv6 connections with IKEv1	271
	7.7.1 Additions to the Setup menu	271
	7.8 VPN network rules for IPv4 and IPv6	271
	7.8.1 Additions to the Setup menu	271
8 1	Virtual LANs (VLAN)	277
	8.1 VLAN-tagging mode "ingress mixed" removed	
	8.1.1 The port table	
9	WLAN	279
	9.1 Adaptive RF Optimization	279
	9.1.1 Setting up Adaptive RF Optimization with LANconfig	
	9.1.2 Additions to the Setup menu	
	9.2 Managed RF Optimization	
	9.2.1 Managed RF Optimization	
	9.3 Airtime Fairness	
	9.3.1 Setting up Airtime Fairness with LANconfig	
	9.3.2 Additions to the Setup menu	
	9.3.3 Additions to the Status menu	
	9.4 Encrypted OKC via IAPP	
	9.4.1 Encrypted OKC via IAPP	
	9.4.2 Additions to the Setup menu	
	9.5 Fast roaming	
	9.5.1 Fast roaming with IAPP	
	9.5.2 Additions to the Setup menu	
	9.6 Wireless Intrusion Detection System (WIDS)	
	9.6.1 Configuring WIDS on the AP with LANconfig	
	9.6.2 Configuring WIDS profiles on the WLC with LANconfig	
	9.6.3 Additions to the Setup menu	
	9.6.4 Additions to the Status menu	
	9.7 Status counters for failed WPA-PSK/IEEE 802.1X login attempts	
	9.7.1 Status counters for WPA-PSK login attempts	
	9.7.2 Status counters for IEEE 802.1X login attempts	
	9.7.3 Additions to the Status menu	
	9.8 Adaptive transmission power	
	9.8.1 Adaptive transmission power	
	9.8.2 Additions to the Setup menu	
	9.9 Improved start-up conditions for WLAN RADIUS accounting	
	9.9.1 Additions to the Setup menu	
	9.10 Selecting a RADIUS server profile for 802.1X authentication	
	9.10.1 Additions to the Setup menu	
	9.11 Configurable data rates per WLAN module	
	9.11.1 Configurable data rates per WLAN module	

9.11.2 Additions to the Setup menu	347
9.12 Maximum length of the AP device name in the WLC config increased to 64 characters	376
9.12.1 Additions to the Setup menu	376
9.13 LANconfig: Modified WLAN encryption dialog	376
10 WLAN management	
10.1 WIDS integration in WLCs	
10.1.1 Managing the Wireless Intrusion Detection System with WLC profiles	377
10.1.2 Additions to the Setup menu	380
10.1.3 Additions to the Status menu	396
10.2 Automatically switch off IAPP if a CAPWAP tunnel exists	398
10.3 Multiple configurable AutoWDS profiles	398
10.3.1 Additions to the Setup menu	398
11 Public Spot	401
11.1 Shorter units for absolute expiry	401
11.2 Circuit ID as a Public Spot URL-redirect variable	401
11.3 Creating Public Spot users on a remote Public Spot gateway	402
11.3.1 Creating Public Spot users on a remote Public Spot gateway	402
11.3.2 Additions to the Setup menu	402
11.4 PMS template: Accept GTC	403
11.5 Hiding fields in the setup wizard "Manage Public Spot Account"	403
11.5.1 Hiding fields in WEBconfig	404
11.6 Redirect for HTTPS connections switchable	411
11.6.1 Redirect for HTTPS connections	411
11.6.2 Additions to the Setup menu	412
11.7 Printout of bandwidth profile on the voucher	413
11.8 Template preview	413
11.8.1 Template preview in WEBconfig	414
11.9 Logging DNS requests and responses to external SYSLOG servers	414
11.9.1 Logging DNS requests and responses to external SYSLOG servers	415
11.9.2 Additions to the Setup menu	415
11.10 Protection against brute force attacks	
11.10.1 Protection against brute force attacks	
11.10.2 Additions to the Setup menu	
12 LANCOM Location Based Services (LBS)	423
12.1 Dynamic and persistent tracking lists for WLAN clients	423
12.1.1 Using the LBS tracking lists of Public Spot users	
12.1.2 Additions to the Setup menu	425
13 Voice over IP – VoIP	427
13.1 Signaling parallel calls in the ISDN	427
13.1.1 Signaling parallel calls in the ISDN	427
13.1.2 Additions to the Setup menu	427
13.2 VoSIP support in the Voice Call Manager	428
13.2.1 Additions to the Setup menu	429

## Addendum

Contents

13.3 SIP over TCP in the Voice Call Manager	430
13.4 DTMF signaling on All-IP connections	432
13.4.1 Additions to the Setup menu	434
13.5 Configurable RTP port range in the Voice Call Manager	436
13.5.1 Additions to the Setup menu	436
13.6 Allow SIP messages only from registrar	438
13.6.1 Additions to the Setup menu	438
14 RADIUS	440
14.1 User-definable attributes in the RADIUS client	
14.2 Automatic clean-up of access information on the RADIUS server	
14.2.1 Additions to the Setup menu	441
14.3 Vendor-specific RADIUS attribute "LCS-Routing-Tag"	
15 Other services	443
15.1 DHCP snooping: New variable for LAN MAC address	
15.2 DHCP lease time per network	
15.2.1 Additions to the Setup menu	
15.3 DHCP lease RADIUS accounting	445
15.3.1 DHCP lease RADIUS accounting	445
15.3.2 Additions to the Setup menu	447
15.4 SNMPv3 support	454
15.4.1 Simple Network Management Protocol (SNMP)	454
15.4.2 Configuring SNMP read-only access	462
15.4.3 Additions to the Setup menu	463
15.5 Logging DNS queries with SYSLOG	482
15.5.1 Logging DNS queries with SYSLOG	482
15.5.2 Additions to the Setup menu	484

## 1 Addendum to LCOS version 9.20

This document describes the changes and enhancements in LCOS version 9.20 since the previous version.

## 2 Overview of new features of the LCOS version 9.20

A variety of new features have been implemented in LCOS version 9.20.

Table 1: New features of the LCOS version 9.20

Voice over Secure IP (VoSIP) – encrypted IP telephony		
	A genuine plus for secure telephony! The LANCOM All-IP option comes with the Voice Call Manager, which features a session border controller functionality and now supports Voice over Secure IP (VoSIP). Encrypted signaling and voice data (SIPS/SRTP) provides secure telephony on IP-based exchange lines.	
SNMPv3		
	LANCOM customers now benefit from improved security in network monitoring thanks to SNMPv3 (Simple Network Management Protocol version 3). This protocol combines user-friendly device monitoring with strong security thanks to its encrypted data communications. And since it is enabled automatically, there is no need for you to make any configuration changes.	
Maximum WLAN	l quality	
	Noticeable improvements in the performance, reliability, and range of LANCOM access points, WLAN routers, and WLAN controllers: As of LCOS9.20, all WLAN devices support the highlight features Airtime Fairness, Adaptive RF Optimization, the Wireless Intrusion Detection System, and many others. What's more, substantial quality improvements give LANCOM users and administrators the best-ever WLAN experience!	
IKEv2		
	IKEv2 facilitates a fast and secure establishment of VPN tunnels. For the first time, encrypted VPN networking is now possible between IPv6-based sites, including those using mixed operation with IPv4.	
IKEv1 with IPv6	support	
	As well as supporting IKEv2, LCOS 9.20 also supports IKEv1 for negotiating VPN connections between IPv6 networks.	
BGP		
	Efficient VPN-based site connectivity thanks to dynamic routing in medium to large-scale networks. BGP (Border Gateway Protocol) ensures that all networked routers communicate effectively by sharing the best paths from their routing tables.	

## 2 Overview of new features of the LCOS version 9.20

#### Advanced telephony features

The Voice Call Manager (VCM) included with the LANCOM All-IP Option supports many additional features such as simultaneous call signaling across multiple internal ISDN buses, integrated DTMF conversion for reliable transmission of dial tones on All-IP lines, as well as the support of SIP packets over TCP connections.

#### Logging of DNS queries

Client-side DNS queries are optionally sent to an external SYSLOG server for logging and analysis.

#### Performance measurement with iPerf

iPerf, a tool integrated into LCOS, allows you to precisely measure the maximum and momentary TCP and UDP throughputs between two devices on the network. The bandwidth losses derived from this can be used to identify and correct bottlenecks on the network.

#### Higher complexity for device passwords

Improved security with a new password policy requiring at least eight characters consisting of letters, digits and special characters.

#### Adaptive RF Optimization

#### Dynamic selection of the best WLAN channel

Improved WLAN throughput due to dynamic selection of the best WLAN channel by the access point in case of interference.

#### **Airtime Fairness**

#### Improved exploitation of WLAN bandwidth

By fairly sharing the WLAN transmission time between all of the active clients, the available bandwidth is used to maximum effect and WLAN performance is improved.

#### Wireless IDS

Detection of attacks or unusual behavior of clients in the WLAN infrastructure by permanently monitoring the radio field. If attack-like events occur with a certain frequency within a set period of time, alerts are sent via e-mail, SYSLOG message, SNMP, or LANmonitor.

#### Adaptive transmission power

Ideal for professional backup scenarios in WLAN environments: If an access point fails, the transmission power of the remaining access points is increased automatically, so that full WLAN coverage is assured at all times.

#### Configurable data rates for each SSID

Communication data rates between the access point and WLAN clients can now be tightly controlled for a genuine gain in flexibility. For instance, data rates made unusable by environmental conditions can be excluded from use.

#### Flexible access models for Public Spot accounts

As of LCOS 9.20, the bandwidth that was booked for the Public Spot can be displayed on vouchers. Also the validity period (time of expiry) of vouchers can be set with shorter time units (days, hours, minutes), which is ideal for scenarios with higher customer frequencies and shorter linger times.

#### **Controller-less WLAN management**

The LANCOM Management Cloud and the LANCOM Large Scale Rollout & Management (LSR) facilitate the automatic commissioning and configuration assignment (zero-touch deployment) and also LANCOM access point management.

## 3.1 Preventing password form fields in the browser from storing passwords

As of LCOS version 9.20, it is possible to suppress the storage of passwords by your web browser for the WEBconfig login form.

## 3.1.1 Preventing password form fields in the browser from storing passwords

Input dialogs on web pages allow web browsers to store any passwords that are entered. This makes things easier for a user accessing the page again in future. This web browser feature is a vulnerability that malicious software can exploit to read out the confidential form data.

To force the manual input of login passwords each time a page is accessed, open WEBconfig and navigate to **Setup** > **HTTP** > **Disable-Password-Autocompletion** and prevent the storage of passwords with the setting "Yes".

## 3.1.2 Additions to the Setup menu

#### **Disable-Password-Autocompletion**

This switch controls whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

#### SNMP ID:

2.21.22

#### Telnet path:

Setup > HTTP

#### Possible values:

#### No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

#### Yes

The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

#### Default:

No

## 3.2 DHCP rollout agent

As of LCOS version 9.20, a device in an unconfigured state requests the vendor-specific DHCP option 43 from the DHCP server. The DHCP server can then send the device further information about how to contact the LSR or other roll-out server.

The following LANCOM devices support this feature: L-3xx, L-4xx, L-13xx, L-151 LN-830, L-822, 178x-series OAPs, IAPs, WLCs, 7100(+), 9100(+), 831A, 1631E, E-series.

## 3.2.1 Receiving LSR information via DHCP server (zero-touch rollout)

An unconfigured LANCOM device boots with an activated DHCP client and uses this to retrieve an IP address, netmask, DNS address, and gateway address from the network's DHCP server.

By means of the vendor-specific DHCP option 43, a suitably configured DHCP server sends information about how to reach an LSR (Large Scale Rollout) server, among other things. The rollout agent of the LANCOM device processes this information, contacts the LSR server and, according to the rollout strategy, it retrieves its configuration or updates its firmware.

This function simplifies the rollout process as the devices no longer have to be preconfigured.

The LSR server connects via HTTP, HTTPS or TFTP, in which case an SSL certificate needs to be stored on the LANCOM device to secure the connection.

It is also possible to configure (also partially) a rollout agent in advance. For example, the rollout server URL sent from the DHCP server can be adopted, although a project number in the device must be configured in advance.

## Configuring the zero-touch rollout

#### Initial situation

In the case of a rollout to a number of branch sites, the large number of devices means that pre-configuring the LANCOM devices is not a viable option. Instead they should be commissioned after they have retrieved a configuration from a central LSR server, in a similar manner to the "zero-touch management" with a WLC.

### Prerequisites

In order for the "zero-touch rollout" by means of the rollout agent in the device to work properly, a number of prerequisites need to be met first:

- A central rollout server must be available and the zero-touch devices must be able to contact it via HTTP/HTTPS.
- DHCP must be active in the network at the branch. That is,
  - a DHCP server is available on the branch network, or
  - a DHCP relay server on the branch network exchanges the DHCP data packets between the devices on the branch network and a DHCP server at the main office.
- The DHCP server has to be able to deliver the DHCP option 43.
- () The DHCP server transmits sensitive data such as the rollout password unsecured as a DHCP message. So take care to transport the data only over appropriately secured connections.

#### Process

The rollout of the configuration proceeds as follows:

**1.** The unconfigured device is connected to the branch network.

- 2. The device retrieves connection data (such as IP address, gateway, netmask, DNS address, and DHCP option 43) from the DHCP server.
- The device uses the DHCP option 43 to decode various pieces of information including the URL of the rollout server and uses this to configure the rollout agent on the device.
- 4. The rollout agent then contacts the rollout server and performs the rollout in two steps:
  - Firmware-Update
  - Configuration update

The rollout agent contacts the rollout server at the configured firmware server URL and retrieves a firmware file in the .upx format, which it is then uses to update the device.

After the firmware update, the device restarts and contacts the rollout server again. The rollout agent checks whether the firmware provided by the rollout server is already installed. This test succeeds if the latest firmware was received by the device in the first step. The rollout agent continues with the configuration update and it downloads script files. It contacts the rollout server at the configured config-server URL and retrieves a script in the .lcs format, which it is then uploaded to the device.

#### **DHCP option 43**

DHCP option 43 is vendor-specific, i.e. each vendor is free to decide how to structure this option and what information is coded into it. The option can contain several sub-types, which are used for the detailed structuring of the data.

The following sub-types are specified for the device rollout agent:

#### Sub-type 1: Config-Server-URL

Server addresses are entered in the following available formats:

- HTTP, HTTPS, TFTP
- IP address, FQDN

Examples:

- https://rollout:443/
- tftp://10.1.1.1
- http://10.1.1.2/test

It is also possible to specify LCOS variables

The rollout agent expects that the rollout server available at this address will respond to its request by sending a configuration script with the extension .lcs.

If the rollout server is an LSR, the address requires the prefix lsr:, e.g.

lsr:https://rollout:443/. The rollout agent then assembles the correct LSR-rollout URL from the sub-type 5 and the following. Accordingly, the sub-types 5 and up are only of importance when using this prefix.

If the rollout server is not an LSR, then specifying the URLs for the config-server and firmware server have to be done by hand with the use of variables.

#### Sub-type 2: Firmware-Server-URL

As with sub-type 1, the rollout agent expects the rollout server at this address to respond by sending a firmware file with the extension .upx.

#### Sub-type 3: HTTP-Username

Contains the user name for HTTP authentication in the URL (in the form http://username:password@server)

#### Sub-type 4: HTTP-Password

Contains the password for HTTP authentication in the URL (in the form http://username:password@server)

#### Sub-type 5: LSR project number

Contains the project number for the rollout project stored in the rollout server.

#### Sub-type 6: Additional URL parameters for LSR keyword

The rollout agent appends this content to the constructed LSR URL (e.g. ?approval=yes).

#### Sub-type 7: Reboot-Time

Specifies the wait time in minutes before the device restarts after the update by the rollout server.

#### Sub-type 8: Request-Interval

Specifies the interval in minutes in which the rollout agent sends its requests to the rollout server.

#### Sub-type 9: TAN

This entry contains the rollout TAN.

#### Sub-type 10: Device number

Contains the device number of the device being updated.

#### Sub-type 11: Request-Delay

Contains the time in minutes that the rollout agent waits between request 1 and request 2.

#### Sub-type 12: Request-Random

This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time. The following entries are allowed:

### 0

Requests take place after set time delays.

#### 1

With this entry, you specify that the request for a rollout takes place after a random delay.

#### Sub-type 13: Omit-Certificate-Check

This value determines whether the rollout agent skips the verification of rollout-server certificate.

**(i)** 

If this subtype is missing or its content is empty, the rollout agent assumes the value is "0" and carries out a check of the server certificate.

Please note that the configuration received from the rollout server needs to switch off the rollout agent on completion (**Operating: no**), otherwise the device will reboot after the specified reboot time.

#### Variables

URLs can contain any of the variables that are available at the LCOS console. These variables can be output by the console by using the command printerv.

The variables are specified in the URL with a leading "\$" character (e.g. \$\_\_\_SERIALNO).

#### **Generating DHCP option 43**

The DHCP option 43 is generated on the basis of RFC 2132, section 8.4.

The following configuration section can be used to generate the option 43 with the use of an ISC DHCPd DHCP server:

Within the general configuration

```
option space Rollout;
option Rollout.config-server code 1 = text;
option Rollout.firmware-server code 2 = text;
option Rollout.HTTP-Username code 3 = text;
option Rollout.HTTP-Password code 4 = text;
option Rollout.Projectnumber code 5 = text;
option Rollout.AdditionalParams code 6 = text;
option Rollout.RebootTime code 7 = text;
option Rollout.RequestInterval code 8 = text;
option Rollout.Tan code 9 = text;
option Rollout.Devicenumber code 10 = text;
option Rollout.RequestDelay code 11 = text;
option Rollout.RequestRandom code 12 = text;
option Rollout.OmitCertCheck code 13 = text;
```

Within the subnet-specific configuration

```
vendor-option-space Rollout;
option Rollout.config-server "LSR:https://10.200.50.1:443";
option Rollout.firmware-server "LSR:https:// 10.200.50.1:443";
option Rollout.HTTP-Username "RolloutUser";
option Rollout.HTTP-Password "Secret";
option Rollout.Projectnumber "1";
option Rollout.RebootTime "300";
option Rollout.RequestDelay "20";
option Rollout.RequestRandom "0";
option Rollout.OmitCertCheck "2";
```

Other DHCP servers (such as the Microsoft DHCP server) do not permit the definition of option 43 in the configuration. In this case, the byte sequence that the server is to deliver as option 43 needs to be prefabricated and inserted into the configuration.

To avoid having to generate this byte sequence manually, the Python script linked in the following can be used to do this: *wiki.snom.com/Category:HowTo:Option\_43*.

## **Configuration with LANconfig**

The rollout agent is configured in LANconfig under Management > Rollout Agent.

Rollout agent			
Operating mode:	DHCP-controlled •		
If you select the operating mode "DHCP-controlled", the rollout agent sends attributes to the rollout server that were transmitted to the device by the DHCPv4 server in the DHCP option 43. Select the operating mode "Active" to send the here configured attributes to the rollout server.			
Rollout server (Configuration):		]	
Rollout server (Firmware):		]	
HTTP Username:		]	
HTTP Password:		Show	
	Generate password 🛛 🔻		
Project number:		]	
Additional parameter:		]	
TAN:		Show	
	Generate password 🛛 🔻		
Device number:		]	
Reboot time:	0	minutes	
Request interval:	0	minutes	
Request delay:	0	minutes	
Randomly spread request dela	ays		

### **Operating mode**

 $(\mathbf{\hat{n}})$ 

If you select the operating mode "DHCP-controlled", the rollout agent sends the rollout server the attributes that the device received from the DHCP server by means of the vendor-specific DHCP option 43. In the "Active" setting, the device transfers the attributes configured in this dialog (for example, if no DHCP is available on the network). Setting the mode to "Off" disables the rollout agent.

The "DHCP-controlled" operating mode does not overwrite manually configured attributes. This makes it possible to perform a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

#### **Rollout server (configuration)**

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.

(i) An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

#### **Rollout server (firmware)**

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

#### **HTTP username**

Set the user name used by the rollout agent to log on to the rollout server.

#### **HTTP** password

Set the user password used by the rollout agent to log on to the rollout server.

#### Project number

This entry specifies the rollout project number for the rollout agent.

#### Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

#### TAN

Use this entry to specify the rollout TAN.

#### **Device number**

Contains the device number of the device that is running the rollout agent.

#### **Reboot time**

Here you set the time after which the device reboots after a rollout.

#### **Request interval**

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.



If the value is "0", the renewed attempt starts in 1 minute.

#### **Request delay**

This entry contains the delay time in seconds for a rollout request.

#### Randomly spread request delays

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

## 3.2.2 Additions to the Setup menu

#### **Rollout** agent

This menu allows you to configure the settings for the rollout agent.

#### SNMP ID:

2.11.92

Telnet path: Setup > Config

#### Operating

This entry determines how the rollout agent operates.

#### SNMP ID:

2.11.92.1

#### Telnet path:

Setup > Config > Rollout-Agent

### Possible values:

#### No

The rollout agent is disabled.

#### Yes

The rollout agent is enabled and transmits the rollout data that is configured in the device to the rollout server.

#### **DHCP** initiated

The rollout agent is enabled. It processes the information received from the DHCP server in the DHCP option 43.



The "DHCP-initiated" operating mode does not overwrite manually configured attributes. This makes it possible to perform a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

### Default:

DHCP initiated

#### **Configuration server**

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.

An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

#### SNMP ID:

2.11.92.2

#### **Telnet path:**

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

#### Firmware server

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.



An entry can take the following forms:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

#### SNMP ID:

2.11.92.3

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

#### User name

Set the user name used by the rollout agent to log on to the rollout server.

#### SNMP ID:

2.11.92.4

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

### Default:

empty

#### Password

Set the user password used by the rollout agent to log on to the rollout server.

#### SNMP ID:

2.11.92.5

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

#### Addendum

3 Configuration

#### **Project number**

This entry specifies the rollout project number for the rollout agent.

#### SNMP ID:

2.11.92.6

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

### Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

#### SNMP ID:

2.11.92.7

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

### **Reboot time**

Here you set the time after which the device reboots after a rollout.

## SNMP ID:

2.11.92.8

#### **Telnet path:**

Setup > Config > Rollout-Agent

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

0

#### **Request-Interval**

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.

#### SNMP ID:

2.11.92.9

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

0

#### Special values:

0

The next attempt starts in 1 minute.

## TAN

Use this entry to specify the rollout TAN.

#### SNMP ID:

2.11.92.10

#### Telnet path:

Setup > Config > Rollout-Agent

#### **Possible values:**

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

#### Default:

empty

### **Device number**

Contains the device number of the device that is running the rollout agent.

#### SNMP ID:

2.11.92.11

#### **Telnet path:**

Setup > Config > Rollout-Agent

### Possible values:

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

#### Default:

empty

#### **Request delay**

This entry contains the delay time in seconds for a rollout request.

#### SNMP ID:

2.11.92.12

## Telnet path:

Setup > Config > Rollout-Agent

### Possible values:

Max. 10 characters from [0-9]

### Default:

0

### **Request time random**

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

#### SNMP ID:

2.11.92.13

#### Telnet path:

Setup > Config > Rollout-Agent

Possible values:

No Yes

#### Default:

No

### **Omit certificate check**

Specifies whether a server certificate verification is carried out on HTTPS connections.

#### SNMP ID:

2.11.92.14

## Telnet path: Setup > Config > Rollout-Agent Possible values: No A certificate check is carried out. Yes No certificate check is carried out. Default:

No

## 3.3 Support of ChaCha20/Poly1305 for SSH access

As of version 9.20, LCOS additionally supports the following cipher algorithms for access via SSH:

- chacha20-poly1305
- aes128-gcm
- aes256-gcm

## 3.3.1 Additions to the Setup menu

## **Cipher-Algorithms**

The cipher algorithms are used for encrypting and decrypting data. Select one or more of the available algorithms.

### SNMP ID:

2.11.28.1

#### Telnet path:

Setup > Config > SSH

#### Possible values:

3des-cbc 3des-ctr arcfour arcfour128 arcfour256 blowfish-cbc blowfish-ctr aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr chacha20-poly1305 aes128-gcm aes256-gcm

#### Default:

3des-cbc 3des-ctr arcfour arcfour128 arcfour256 blowfish-cbc blowfish-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes192-ctr aes256-ctr

## 3.4 Enforcing password complexity for device passwords

As of LCOS version 9.20, you have the option to enforce a predefined password policy for setting device passwords.

Device configuration		
Administrator name (optional):	root	
Main device password:		Show
	Generate password	
You also can set up further dev	ice administrators:	
	Further administrators	
SNMP read only community	'public' disabled	
SNMP read only community:		

The switch **Enforce device password policy** determines the following policies for the main device password and the administrator passwords:

- The length of the password is at least 8 characters.
- The password contains at least 3 of the 4 character classes, i.e. lowercase letters, uppercase letters, numbers, and special characters.

Please note that this feature has no effect on existing passwords. Only when passwords are changed are they checked for their policy compliance.

## 3.4.1 Additions to the Setup menu

## **Enforce-Password-Rules**

This entry gives you the option to disable or enable the enforcing of password rules.

#### SNMP ID:

2.11.93

#### Telnet path:

Setup > Config

#### **Possible values:**

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

#### Default:

Yes

## 3.5 LBS server 1.1: Making elements in the LBS measurements fields selectable

As of LCOS version 9.20, you have the option in WEBconfig to select the elements of the LBS measurement fields that are to be transmitted.

Until now, APs and WLCs sent all of the available data for all of the management frames, which resulted in an increased overhead.

## 3.5.1 Making elements in the LBS measurements fields selectable in WEBconfig

Enable or disable the individual elements of the LANCOM Location Based Services measurement fields in the LCOS menu tree under **Setup** > **LBS** > **Measurements-Fields**.



The elements clientid, deviceid and timestamp are compulsory and are not available for selection.

#### **BSSID-Transmit**

Determines whether the device transmits the BSSID, which was sent by the WLAN client in its management frames, to the LBS server.

#### **Frequency-Transmit**

Determines whether the frequency used by the device is transmitted to the LBS server.

#### Noise-Transmit

Determines whether the device transmits the noise level to the LBS server.

#### Interface-Identifier-Transmit

Determines whether the device sends the name of the interface used to the LBS server.

#### Sequence-Number-Transmit

Determines whether the sequence number is transmitted.

#### Signal-Level-Transmit

Determines whether the signal strength observed for the WLAN client is transmitted to the LBS server.

#### SSID-Transmit

Determines whether the device transmits the SSID, that was sent by the WLAN client in its management frames, is sent to the LBS server.

#### WLAN-Frame-Type-Transmit

Determines whether the device transmits the WLAN-Frame-Type to the LBS server.



On a WLC, the LBS measurements fields are located in the LCOS menu tree under **Setup** > **WLAN-Management** > **AP-Configuration** > **LBS** > **General**.

## 3.5.2 Additions to the Setup menu

#### **Measurements-Fields**

This menu contains the settings for the LBS measurement fields.

#### SNMP ID:

2.100.16

### Telnet path:

Setup > LBS

#### Sequence-Number-Transmit

This entry determines whether the sequence number is transmitted.

#### SNMP ID:

2.100.16.1

#### Telnet path:

Setup > LBS > Measurements-Fields

### Possible values:

Yes No

#### Default:

Yes

#### SSID-Transmit

Determines whether the device transmits the SSID, which was sent by the WLAN client in its management frames, to the LBS server.

#### SNMP ID:

2.100.16.2

#### Telnet path:

Setup > LBS > Measurements-Fields

#### **Possible values:**

Yes No

Default:

Yes

#### Addendum

3 Configuration

#### Interface-Identifier-Transmit

This entry specifies whether the device sends the name of the interface used to the LBS server.

#### SNMP ID:

2.100.16.3

#### Telnet path:

Setup > LBS > Measurements-Fields

#### **Possible values:**

Yes No

#### Default:

Yes

#### **BSSID-Transmit**

Determines whether the device transmits the BSSID, which was sent by the WLAN client in its management frames, to the LBS server.

#### SNMP ID:

2.100.16.4

### Telnet path:

Setup > LBS > Measurements-Fields

### Possible values:

Yes No

#### Default:

Yes

### Signal-Level-Transmit

Determines whether the signal strength observed for the WLAN client is transmitted to the LBS server.

### SNMP ID:

2.100.16.5

### Telnet path:

Setup > LBS > Measurements-Fields

**Possible values:** 

Yes No

#### Default:

Yes

## **Frequency-Transmit**

This entry determines whether the frequency used by the device is transmitted to the LBS server.

#### SNMP ID:

2.100.16.6

#### Telnet path:

Setup > LBS > Measurements-Fields

#### **Possible values:**

Yes No

#### Default:

Yes

#### Noise-Transmit

Determines whether the device transmits the noise level to the LBS server.

#### SNMP ID:

2.100.16.7

#### Telnet path:

Setup > LBS > Measurements-Fields

#### **Possible values:**

Yes No

#### Default:

Yes

#### Addendum

3 Configuration

#### WLAN-Frame-Type-Transmit

Determines whether the device transmits the WLAN-Frame-Type to the LBS server.

#### SNMP ID:

2.100.16.8

#### Telnet path:

Setup > LBS > Measurements-Fields

**Possible values:** 

Yes No

Default:

Yes

## 3.6 Preventing the storage of passwords in WEBconfig

As of LCOS version 9.20, you have the option to deactivate the auto-completion of password fields.

## 3.6.1 Additions to the Setup menu

## **Disable-Password-Autocompletion**

This switch controls whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

#### SNMP ID:

2.21.22

Telnet path:

Setup > HTTP

#### **Possible values:**

#### No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

#### Yes

The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

#### Default:

No

## 3.7 LANconfig: Icon for \*.LCS files in Windows Explorer

As of LCOS version 9.20, the Windows Explorer displays \*.LCS files with a dedicated icon. The context menu or a double-click on the file opens the LANconfig "What's this" direct help.

The following functions are available from the Windows Explorer context menu:

😋 🔍 🗢 🚺 🕨 Computer	▶ Lokaler Datenträger (C:) ▶ Temp ▶ Conf	fig 🔹 🍫 Config durchsuchen 👂
Organisieren 👻 🛐 Öffr	nen 🔻 Drucken Neuer Ordner	≡ - □ 0
숨 Favoriten	Name	Änderungsdatum Typ Größe
💻 Desktop 🚺 Downloads 🖭 Zule <del>tzt</del> besucht	<b>75</b> V9.20 D2016-02-23 T1624 Öffnen Direkthilfe	23.02.2016 16:24 LANconfig Konfig 68 KB
詞 Bibliotheken 📄 Bilder 📔 Dokumente	Drucken Setup-Assistent Senden an	•
🎝 Musik 📑 Videos	Ausschneiden Kopieren	
19 Computer 실실 Lokaler Datenträger 장 DVD-Laufwerk (D:) V	Verknuprung erstellen Löschen Umbenennen	
🗣 Netzwerk	Eigenschaften	

#### Open

This menu item opens the configuration in LANconfig.

(i) This item only appears for configuration files with the extension .lcf.

#### What's this

This menu item opens a help text which gives users information about dealing with this file.

#### Print

This menu item enables you to print the file.

#### Setup Wizard

This menu item starts the LANconfig Setup Wizard.

(i) This item only appears for configuration files with the extension .lcf.

## 4 Diagnosis

## 4.1 Specifying the SYSLOG server address as an IPv6 address or DNS name

As of LCOS version 9.20, the addresses of a SYSLOG server can be entered in the form of an IPv6 address or a DNS name.

SYSLOG servers - Edit Entry	/	? 💌
Server address:	127.0.0.1	
Source address (opt.):	INTRANET -	Select
Source		
✓ System	🔲 Login	
Connections	Accounting	
Administration	Router	
Priority		
📝 Alert	V Error	
📝 Warning	👽 Information	
V Debug		
	ОК	Cancel

#### Server address

Used to set the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a host name.

## 4.2 IPv6 support for LCOScap

As of LCOS version 9.20, LCOScap also supports IPv6 connections.

The LCOScap client is able to connect to the device via IPv4 or IPv6.

## **5** Routing and WAN connections

## 5.1 Border Gateway Protocol version 4 (BGPv4)

From LCOS version 9.20, it is possible to operate the Border Gateway Protocol version 4.

## 5.1.1 Border Gateway Protocol version 4 (BGPv4)

The network of a network provider is also referred to as an "autonomous system" (AS). The Border Gateway Protocol version 4 (BGPv4) is used to exchange routing information between autonomous systems (eBGP: external BGP) and to re-distribute this information to the routers of your own AS (iBGP: internal BGP).

## **Configuring BGPv4 with LANconfig**

In order to configure BGPv4 with LANconfig, navigate to the **Routing protocols** > **BGP** menu.

Border Gateway Protokoll (BGP) activated			
BGP-Instance			
In dieser Tabelle können Parameter der BGP-Instanz wie AS-Nummer oder Router-ID konfiguriert werden.			
BGP-Instance			
Neighbors			
Definieren Sie hier die Parameter der BGP-Nachbarn.			
Neighbors Neighbor profiles			
Network			
Definieren Sie hier die Präfixe bzw. Netzwerke, die über BGP propagiert werden sollen.			
IPv4 network IPv6 networks			
Addressfamily			
Definieren Sie hier die Parameter der Adressfamilien.			
IPv4 Addressfamily IPv6 Addressfamily			
BGP Policy			
Here you can define policies which are applied per neighbor to incoming or outgoing attributes of prefixes.			
BGP Policy			

#### **Enabling BGP**

To activate the BGP function, set a check mark for Border Gateway Protocol (BGP) active.

#### **BGP** instance

LCOS associates the BGP configuration of the BGP router with what is known as a **BGP instance**. This BGP instance contains the AS number and the router ID, among other things.

() Currently LCOS supports only one BGP instance at a time.

#### 5 Routing and WAN connections

#### Neighbors

The term Neighbors refers to the BGP gateways of other autonomous systems. These autonomous systems do not have to be immediate neighbors, although they must be known to at least one neighboring BGP gateway.

Neighbor profiles offer a convenient way to configure the BGP neighbors.

#### Networks

The BGP router propagates its managed networks to the BGP neighbors.

#### Address families

The BGP router organizes the BGP neighbors into address families as a convenient way to manage the communications with these neighbors.

#### **BGP** policy

Filter policies allow the BGP router to decide how to handle the inbound and outbound BGP messages.

#### **BGP** instance

You configure the BGP instance of the device under BGP instance.

BGP Instance - DEFAULT		? 💌
V Active		
Name:	DEFAULT	
AS Number:	0	
Router ID:	0.0.0.0	
Port:	179	
Send Syslog notifications:	No	
Check first AS:	Yes 🔹	
AS path limit:	0	
Route reflector:	On 🔻	
Cluster ID:	0.0.0.0	
Comment:	Default Instance	
	ОК	Cancel

#### Operating

Activates or deactivates this BGP instance



This setting only takes effect if BGP is activated on the device.

#### Name

Contains the name of the BGP instance.

(i)

Since the device only supports one BGP instance at a time, this table contains one entry only, "DEFAULT".

#### AS number

The AS number assigned to this BGP instance.



It is only possible to connect to a BGP router that does not support 32-bit AS numbers if you enter a 16-bit AS number here (less than 65536).

#### **Router ID**

The router ID (IPv4 address) of this particular BGP instance.

The router ID must be unique among the neighbors of a BGP router.



When using IPv6 connections, you enter a fictional IPv4 address or any IPv4 address for the router here.

#### Port

Contains the port used by the BGP instance to listen to inbound connections from neighbors.

#### Send SYSLOG message

The device is able to store events, such as disconnects of neighbors associated with this BGP instance, to the SYSLOG. Use this option to enable or disable this feature.

#### **Check-First-AS**

Checks whether the first AS number in the AS path of received Update messages corresponds to the AS number of the neighbor. If this is not the case, this route is discarded.



This check must be disabled if the router is connected with a BGP route server which, although it distributes routes, is not itself in the routing path and/or inserts its own AS into the AS path.

#### AS-Path-Limit

Maximum number of permitted AS numbers in the AS path of received Update messages. If the limit is exceeded, the device discards the route. An AS-Path-Limit provides protection against messages from incorrectly configured routers that advertise AS paths that are too long.

#### **Route-Reflector**

This specifies whether the router assumes the function of a route reflector.

When operating iBGP, all of the BGP routers usually need to be fully meshed, i.e. each BGP router must have established a BGP connection to every other BGP router. A route reflector negates this requirement and enables iBGP routers to form, for example, a star-shaped topology. A route reflector forwards the iBGP routes to all of the route-reflector clients.

A route reflector is able to serve route-reflector clients as well as normal BGP clients. In both cases no special configuration of the client is necessary.

#### **Cluster-ID**

Cluster-ID of the router in case it is configured as a route reflector. This is entered as an IPv4 address.

#### Comment

Comment about this BGP instance.

Addendum

5 Routing and WAN connections

#### Neighbors

#### **BGP** neighbors

You configure the BGP neighbors of the device under Neighbors.

Neighbors - New Entry		? 🔀
📝 Entry active		
Name:		
IP address:		
Port:	179	
Source address (opt.):	•	Select
Routing tag:	0	
Remote AS:	0	
Password:		Show
	Generate password 🖛	
Connection mode:	Active •	
Connection delay:	120	seconds
Route reflector client:	No 🔻	
Neighbor profile:	DEFAULT -	Select
Inbound policy:	•	Select
Outbound policy:	-	Select
Comment:		
	ОК	Cancel

#### **Entry active**

Activates or deactivates the entry for this BGP neighbor.

It is not possible to connect to disabled BGP neighbors.

The activation of the BGP neighbor triggers the establishment of a BGP connection, if applicable.

(i)

#### Name

Contains the name of the BGP neighbor.

#### **IP** address

Specifies this BGP neighbor's IP address (IPv4 or IPv6) as used by the device to establish a BGP connection in the "active" or "delayed" connection mode.

Alternatively, you have the option to configure an entire IPv4 subnet, e.g. 192.168.1.0/24. In this case, the router accepts BGP connections from other routers on the subnet 192.168.1.0 with a subnet mask of 255.255.255.0. For this it is necessary to define the connection mode as "Passive".

IPv6 subnets are not supported.

This entry must match the IP address (e.g. physical interface address, loopback address) reported by this neighbor in an incoming connection.

#### Port

Shows the port on which the BGP neighbor expects inbound BGP messages and, correspondingly, the port used by the device for outbound connections of the connection type "active" or "delayed".



G

The device accepts incoming connections from any source port used by the sender.
#### Source address (optional)

Contains the sender address (IPv4 or IPv6) that the device communicated to the BGP neighbor when connecting.

**(i)** 

Entry is optional and is only relevant for the connection modes "active" and "delayed".

# **Routing tag**

Contains the routing tag. The device denies the connection if the routing tag does not match with the incoming connection.

# Remote AS

Contains the AS number of the BGP neighbor.

If the AS number of the BGP neighbor is identical to the AS number of the device's own BGP instance, then this neighbor is an iBGP peer (internal BGP) in its own AS.

### Password

The device and the BGP neighbor authenticate themselves by exchanging this password in the form of an MD5 signature in the TCP packets.



Authentication is not used if no password is set.

#### **Connection mode**

Sets the mode in which the connection is established from the device to this BGP neighbor. The following modes are available:

- Active: In this mode the device attempts to connect to the BGP neighbor as soon as, among other things, one of the following conditions is met:
  - □ The BGP neighbor is configured completely.
  - □ Using WEBconfig or via the console, you execute the action Manual start.
  - You start the device.
  - □ The BGP instance is enabled under **Routing protocols** > **BGP** > **BGP instance**.
  - You enable this BGP neighbor under Entry active.
- Passive: In this mode the device does not actively connect to the BGP neighbor; instead, it waits for a connection request from the BGP neighbor.
- Delayed: In this mode the device waits for a timeout before it tries to connect to the BGP neighbor. The conditions for establishing a connection are the same as for the "Active" mode.

#### **Connection delay**

Specifies the wait time in seconds before the device in the "Delayed" connection mode establishes a connection to this BGP neighbor.

#### **Route reflector client**

Specifies whether this neighbor is treated as a route-reflector client, in which case the device reflects iBGP routes to it.

This switch is valid only if

- The device has been configured as a route reflector in the BGP instance, i.e. it is a route reflector itself, and
- The remote AS number matches its own AS number (iBGP).

#### **Neighbor profile**

Contains the name of the BGP neighbor profile from Routing protocols > BGP > Neighbor profiles.



If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

# Inbound policy

Specifies the policy used by the device to filter the inbound connections from this BGP neighbor.

The policy is configured under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.

If you leave this field empty, the device filters the inbound connections according to the default policy under Routing protocols > BGP > BGP policy > Standard.

# **Outbound policy**

Specifies the policy used by the device to filter the outbound connections from this BGP neighbor.

The policy is configured under **Routing protocols** > **BGP** > **BGP policy** > **Filters**.



If you leave this field empty, the device filters the inbound connections according to the default policy under **Routing protocols** > **BGP** > **BGP policy** > **Standard**.

# Comment

Contains a comment about this BGP neighbor.

# **BGP** neighbor profiles

You configure the profiles of the BGP neighbors of the device under BGP instance.

Neighbor profiles - New	/ Entry	8 23
Name:		
Route update delay:	30	seconds
Send TTL:	1	
Recv TTL:	0	
Keepalive:	30	seconds
Holdtime:	90	seconds
Filter Private AS:	No	-
AS override:	No	<b>~</b>
Comment:		
		DK Cancel

# Name

(î)

Contains the name of the profile.

This name is used in the following tables, among other things:

- Neighbor profile under Routing protocols > BGP > Neighbors
- Neighbor profile under Routing protocols > BGP > IPv4 address family
- Neighbor profile under Setup > Routing protocols > BGP > IPv6 address family

# Route update delay

This is the minimum delay in seconds between BGP advertisements sent by the device to neighbors using this profile.

#### Send TTL

Specifies the TTL (time to live) that the device adds to TCP packets sent to the BGP neighbors that use this profile.

For directly connected neighbors, this value is set to "1". For eBGP environments, you can increase this value by 1 per hop.

For iBGP sessions, the device ignores this value and defaults to the maximum TTL value.

This value must be "0" if **Recv TTL** is set to a value other than "0". The device automatically uses the value "1" if both **Send TTL** and **Recv TTL** are set to "0".

# Recv TTL

Specifies the minimum TTL (time to live) required of inbound TCP packets from BGP neighbors that use this profile. Inbound TCP packets must have a TTL greater than or equal to this value in order to be accepted.

The device ignores this value in iBGP sessions.

f this value is not equal to "0", the device sets the internal value for **Send TTL** to "255".

This

This value must be "0" if **Send TTL** is set to a value other than "0".

#### Keepalive

Specifies the time in seconds for the keepalive timer. After this time has elapsed, the device sends a keepalive message to the neighbors using this profile in order to keep the BGP connection intact.

The device must send at least three keepalive messages per unit of holdtime. For this reason the value should be max. one third of the holdtime. If the value is set higher than this or equal to "0", the LCOS automatically sets an internal value that is one-third of the holdtime.

#### Holdtime

Specifies the time in seconds for which the device considers a BGP connection without traffic to still be valid.

The device negotiates this value with the BGP neighbors during connection establishment. The lower of the two values is considered to be valid.

If negotiation results in a value of "0", the device considers the connection to be valid until it receives a connection error or the connection breaks. No keepalive messages are sent to the BGP neighbors during this period, even if the keepalive timer is set with a value.

In accordance with the RFC, the values "1" and "2" are not permitted.

#### Filter private AS

Controls the removal/replacement of private AS entries (64512 - 65535, 420000000 - 4294967294) from the AS\_PATH list of outbound Network Layer Reachability Information (NLRI) messages of BGP neighbors that use this profile.

**(î**)

This option has no function for iBGP connections.

### AS override

Enables or disables the overriding of AS numbers in the AS\_PATH outbound Network Layer Reachability Information (NLRI).

With this option enabled, the device replaces all of the AS numbers of the BGP neighbors with its own AS number.

# Comment

Comment on this entry.

#### IPv4 networks

Use this table to configure the IPv4 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Routing protocols** > **BGP** > **IPv4 address** family.



The minimum specification for a valid new entry is one IP address.

IPv4 network - New Entry		? 💌
IP address:	0.0.0.0	
Netmask:	0.0.0.0	
Routing tag:	0	
Туре:	Static 👻	
Comment:		
	ОК	Cancel

#### **IP** address

Contains the IPv4 address or the prefix of the network.

# Netmask

Includes the IPv4 netmask of the network.

The route is the default route for this address family if this entry contains the default setting 0.0.0.0.

### **Routing tag**

(i)

Contains the routing tag for this network.

The table under **Routing protocols** > **BGP** > **IPv4 address family** uses this entry to filter the communication with BGP neighbors.

#### Туре

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

- In the "Static" setting the network is always selected for advertisement.
- In the "Dynamic" setting, the network is only selected for advertisement if it appears in the active routing table.

#### Comment

Comment on this entry.

#### IPv6 networks

Use this table to configure the IPv6 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Routing protocols** > **BGP** > **IPv6 address** family.



The minimum specification for a valid new entry is one **Prefix**.

IPv6 networks - New Er	ntry	? 💌
Prefix:	::	
Prefix length:	0	
Routing tag:	0	
Туре:	Static	•
Comment:		
	OK	Cancel

#### Prefix

Contains the prefix (IPv6 address portion) of the network.

# **Prefix length**

Contains the prefix length of the IPv6 network.

(f) The route is the default route for this address family if this entry contains the default setting 0.

#### **Routing tag**

Contains the routing tag for this network.

The table under **Routing protocols** > **BGP** > **IPv6 address family** uses this entry to filter the communication with BGP neighbors.

### Туре

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

- In the "Static" setting the network is always selected for advertisement.
- In the "Dynamic" setting, the network is only selected for advertisement if it appears in the active routing table.

### Comment

Comment on this entry.

## **IPv4 address family**

Use this table to configure the settings for the IPv4 parameters that apply to all of the devices of a BGP neighbor profile.

IPv4 address family - New	Entry	? <b>×</b>
Entry active		
Neighbor profile:	•	Select
Routing tag:	0	
Weight:	0	
Locale preference:	100	
Prefix limit:	0	
Communities:	Standard and Extended	•
🔲 Use own IP address as r	next hop	
Route redistribute		
C Static	Connected	
Comment:		
	ОК	Cancel

# **Entry active**

Enables or disables the distribution of IPv4 NLRI of this address family to the BGP neighbors that use this neighbor profile.

# **Neighbor profile**

Contains the name of the corresponding neighbor profile as saved under **Routing protocols** > **BGP** > **Neighbor profiles**.

# **Routing tag**

Specifies that the device only re-distributes routes if they use the routing tag as configured in the routing table. The routes received from the neighbors for this routing tag are stored by the device in the routing table.

#### Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.



"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

#### Local preference

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

()

"Local preference" is a BGP standard attribute (LOCAL\_PREF) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

#### **Prefix limit**

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

# Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options "Standard" and "Extended" are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

#### Use own IP address as next hop

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

Possible values:

# Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

#### No

Leaves the IP address of the next hop in the NLRI unchanged.

#### Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

#### **Route redistribute**

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

- Static: The device distributes static routes from the routing table to the BGP neighbors.
- Connected: The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

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

# Comment

Comment on this entry.

#### IPv6 address family

Use this table to configure the settings for the IPv6 parameters that apply to all of the devices of a BGP neighbor profile.

IPv6 Addressfamily - New	Entry	? 💌
Entry active		
Neighbor profile:	-	Select
Routing tag:	0	
Weight:	0	
Locale preference:	100	
Prefix limit:	0	
Communities:	Standard and Extended	•
📄 Eigene IP-Adresse als n	ächsten Hop setzen	
Route redistribute		
C Static	Connected	
Comment:		
	ОК	Cancel

#### **Entry active**

Enables or disables the distribution of IPv6 NLRI of this address family to the BGP neighbors that use this neighbor profile.

#### Neighbor profile

Contains the name of the corresponding neighbor profile as saved under **Routing protocols** > **BGP** > **Neighbor profiles**.

# **Routing tag**

Specifies that the device only re-distributes routes if they use the routing tag as configured in the routing table. The routes received from the neighbors for this routing tag are stored by the device in the routing table.

#### Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

**(i)** 

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

### Local preference

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Local preference" is a BGP standard attribute (LOCAL\_PREF) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

#### Prefix limit

(î)

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

#### Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options "Standard" and "Extended" are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.



This option is of no relevance for communications with iBGP neighbors.

#### Use own IP address as next hop

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

Possible values:

#### Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

#### No

Leaves the IP address of the next hop in the NLRI unchanged.

#### Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

## **Route redistribute**

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

- Static: The device distributes static routes from the routing table to the BGP neighbors.
- Connected: The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

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

#### Comment

Comment on this entry.

# **BGP** policy

Use this section to configure the filter settings for outbound and inbound NLRIs.

BGP Policy	? 🔀
Standard:	Permit
In this table you can define Filters	filters which can be applied per neighbor.
In this table you can define	match lists for filters.
Matches	
In this table you can define AS-Path Prefix	match lists of prefixes or attributes.
In this table you can define Actions	actions which are applied for matches.
In this table you define ove attributes.	rrides which can be applied to prefix
AS-Path Basic	Communities
	OK Cancel

# Default

The device applies this default policy for a BGP neighbor if it is unclear whether it should accept its prefix or not. The cause for this may be:

- There is no policy configured for this BGP neighbor.
- The specified filter does not exist.
- None of the filters under **Filters** match.

### Filters

Here you specify the filters, which should be available for each neighbor.

#### Matches

Specify the match lists for the filters here.

<sup>(</sup>i

# Prefix and attribute lists

Here you specify the lists of prefixes and attributes for the device to recognize as a match.

# Actions

Here you specify the actions that are executed by the device in case of a match.

# Overrides

Here you specify the overrides used by the device to modify prefix attributes.

#### Filters

This table contains filters that an NLRI to or from a BGP neighbor must pass through if the neighbor is configured with a corresponding policy.

Filters - New Entry	? 💌
Name:	
Priority:	0
Addressfamily:	IPv4 + IPv6 ▼
Policy:	Deny 🔻
Match:	Select
Action:	✓ Select
Comment:	
	OK Cancel

#### Name

Contains the name of this entry.

For multiple filter entries with the same name, the device processes the filters according to the configured priority, until a filter matches the NLRI. The device then stops the filter pass.

# Priority

Sets the priority of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value. A higher value means a higher priority.

### Address families

Specifies the address family for which this filter applies.



If no option is selected, the entry is disabled.

# Policy

Specifies whether the device should further process the filtered NLRI in the case that the filter is valid for the NLRI.

- Deny: No further processing.
- Permit: The device processes the NLRI further.

#### Matches

Specifies the name of an entry from the table **Matches**.

The device applies this filter if the NLRI matches the criteria.

() If this field indicates an invalid name, the device denies the NLRI and performs no further filters in the current filter chain.

#### Action

Specifies which of the actions from the Actions table is applied by the device to the NLRI.

If this field is empty or refers to an invalid name, the device performs no action.

### Comment

**(i)** 

Comment on this entry.

# Matches

This table combines lists of prefixes and attributes in order to compare multiple list entries for matches with the NLRI.

Matches - New Entry		? <mark>×</mark>
Name:	[	
Prefix:		✓ Select
AS-Path:		Select
Communities:		Select
Comment:		
	OK	Cancel

#### Name

Contains the name of this entry.

# Prefix

Contains the corresponding item in the list under Prefix.

# **AS-Path**

Contains the corresponding item in the list under AS path in the section "Prefix and attribute lists".

# Communities

Contains the corresponding item in the list under **Communities** in the section "Prefix and attribute lists".

#### Comment

Comment on this entry.

#### AS Path (attribute list)

This table contains AS-path lists in order to identify NLRIs by their AS\_PATH attributes.

AS-Path - New Entry		? 🗙
Name:		
AS-Path-Regex:		
Regex match:	Full	•
Comment		
	OK	Cancel

#### Name

Contains the name of this entry.

# **AS Path Regex**

Contains a regular expression that checks the AS\_PATH of the NLRI. Examples:

- .\*\_100: filters all NLRIs originating from "AS100".
- .\*\_(100|200): filters all NLRIs originating from "AS100" or "AS200".
- 100\_(.\*\_)?(500|400)\_.\*: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which were also previously routed via networks with the AS numbers "AS500" or "AS400" (or both).
- 100\_(500|400|123)\_.\*: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand directly from BGP neighbors with the AS numbers "AS500", "AS400" or "AS123".
- 100\_(100\_)\*(300\_)\*300: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand from the BGP neighbor with the AS number "AS300". This expression also allows for AS prepend paths.
- 100\_ 200: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which originated from the network with the AS number "AS200". The route taken by the NLRIs from "AS200" to "AS100" is unimportant.

### **Regex-Match**

Determines how closely the regular expression under **AS-Path-Regex** needs to match the **AS\_PATH** attribute of the NLRI in order for the list entry to apply.

- Full: The regular expression fully describes the AS\_PATH attribute of the NLRI.
- Partial: The regular expression only describes parts of the AS\_PATH attribute.

#### Comment

Comment on this entry.

# **Communities (attribute list)**

This table contains community lists in order to identify NLRIs by their community attributes.

Communities - New	Entry		? <mark>- x -</mark>
Name:	I		]
Communities:			
Comment:			
		UK	Lancel

#### Name

Contains the name of this entry.

#### Communities

Contains communities that the community attribute of the NLRI must match with.

```
Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>:<Value2>, <AS-number3>:<Value3>).
```

#### Comment

Comment on this entry.

#### Prefix (attribute list)

This table contains prefix lists that are used to identify NLRIs based on their network (prefix) and netmask (prefix length). An entry can contain several prefixes.

Prefix - New Entry			? 💌
Name:	I		
IP address:			
Prefix length:	0		
Min. Prefix-Length:	0		
Max. Prefix-Length:	0		
Comment:			
		ОК	Cancel

#### Name

Contains the name of this entry.

### **IP** address

Contains the IPv4 or IPv6 address of the network.

# **Prefix length**

Contains the netmask or prefix length of the network.

This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address.

The prefix length of the NLRI must exactly match this value unless "Min. prefix length" and "Max. prefix length" are set to values not equal to zero.

If the value is "0", the network of the NLRI matches when it comes from same IP address family as that specified under "IP address".

# Min. prefix length

Specifies the minimum prefix length value that the network of the NLRI needs in order to match.

## Max. prefix length

Specifies the maximum prefix length value that the network of the NLRI needs in order to match.

# Comment

Comment on this entry.

# Action

This table combines override lists in order to perform multiple modifications of an NLRI by means of a single action.

Actions - New Entry	? 🗙
Name:	
Basic:	✓ Select
AS-Path:	✓ Select
Communities:	▼ Select
Comment:	
	OK Cancel

#### Name

Contains the name of this entry.

# Basic

Contains the name of an override of basic entries in the NLRI.

This entry refers to the entries in the override table under Basic.

#### AS-Path

Contains the name of an override of AS\_PATH attributes in the NLRI.

This entry refers to the entries in the override table under AS Path.

# Communities

Contains the name of an override of Community entries in the NLRI.

This entry refers to the entries in the override table under Communities.

#### Comment

Comment on this entry.

### AS Path (override list)

This table contains overrides that manipulate the AS\_PATH attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

- 1. "Filter private AS"
- 2. "Replace"
- 3. Together "Prepend count" and "Prepend"

AS-Path - New Entry		? <mark>×</mark>
Name:	I	]
Filter Private-AS:	No	•
Replace:		]
Prepend:		
Prepend count:	0	
Comment:		
		Cancel
	UK	Cancer

#### Name

Contains the name of this entry.

# Filter private AS

If configured, this entry causes the device to modify the specification of the private AS numbers in the AS\_PATH attribute of an NLRI in accordance with this setting.

- No: The device retains the existing private AS numbers of the NLRI.
- Remove: The device removes all private AS numbers.
- Replace: The device replaces the existing private AS numbers with the AS number of the current BGP instance.

#### Replace

If configured, this entry causes the device to change the AS\_PATH attribute of the NLRI to the value specified here.

#### Prepend

If configured, this entry causes the device to prepend the AS\_PATH attribute of the NLRI with the value entered here as often as is specified under "Prepend count". Special values:

- self: The device prepends the AS\_PATH attribute of the NLRI with its own AS number.
- last: The device prepends the AS\_PATH attribute of the NLRI with the most recently used AS number.

#### **Prepend count**

Determines how often the device prepends the AS\_PATH attribute of the NLRI with an AS number.

#### Comment

Comment on this entry.

# **Communities (override list)**

This table contains overrides that manipulate the Communities attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

- 1. "Clear"
- 2. "Add"
- 3. "Remove"

Communities - New Entry	/	? 🗙
Name:	[	
Clear:	No 🔻	
Add:		
Remove:		
Comment:		
	ОК	Cancel

#### Name

Contains the name of this entry.

#### Clear

Determines whether the device deletes unknown communities from the NLRI.

(f) Known communities remain in place even if this option to set to "Yes".

Known communities are:

- no-peer
- no-export
- no-advertise
- no-export-subconfed



# Add

Specifies which communities the device adds to an NLRI.

```
Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>: <Value2>, <AS-number3>: <Value3>).
```

#### Remove

Specifies which communities the device removes from an NLRI.

```
Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>: <Value2>, <AS-number3>: <Value3>).
```

(i) Known communities are not removed from NLRI. Known communities are:

- no-peer
- no-export
- no-advertise
- no-export-subconfed

The following input formats are available for communities:

Input format	Community
1:2	Standard community
1.2.3.4:1	IPv4-specific extended community
roc:1.2.3.4:1	IPv4-specific route origin extended community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4-specific route target extended community
ext2:1:2	Two-byte AS extended community
ext4:1:2	Four-byte AS extended community
roc:1:2	Two-byte AS route origin extended community (Site-of-Origin (SoO))
rtc:1:2	Two-byte AS route origin extended community
roc:ext4:1:2	Four-byte AS route origin extended community (Site-of-Origin (SoO))

#### Comment

Comment on this entry.

# **Basic (override list)**

This table contains overrides that manipulate the basic attributes of NLRIs.

If an action applies a row of this table, all of the manipulations that this row implements are processed.

The specification of basic attributes is optional. If you want the action to change just one basic attribute, enter the desired value at the appropriate place and leave the remaining attributes in their default setting.

Basic - New Entry			8 X
Name:			
Set weight:	0		
Set local pref.	0		
Remove MED:	No		•
Set MED:	0		
Set nexthop:			
Set link-local-nexthop:			
Comment:			
		ОК	Cancel

### Name

 $(\mathbf{i})$ 

Contains the name of this entry.

## Set weight

The device modifies the weighting of an NLRI to the value specified here.

# Local preference

The device modifies the local preference value of an NLRI to the value specified here.

#### Remove MED

If set to "Yes", the device deletes the multi-exit discriminator (MED) of an NLRI before it processes the setting under "Set MED".

### Set MED

The device modifies the multi-exit discriminator (MED) of an NLRI to the value specified here. If the NLRI contains no MED, the device creates this attribute.

# Set nexthop

The device modifies the next-hop IP of an NLRI to the value specified here. Possible values are an IPv4 address or a global IPv6 address.

### Set link-local-nexthop

The device modifies the IPv6 link-local-nexthop of an NLRI to the value specified here. This only effects IPv6 prefixes.

# Comment

Comment on this entry.

# 5.1.2 Best-path selection algorithm

The following algorithm is applied for the selection of the best path:

- 1. The next hop in the BGP update message is available.
- 2. The device's own AS is not in the AS-Path.
- 3. The next hop is not the device's own address.
- 4. Highest weight
- 5. Highest local preference
- 6. Shortest AS\_PATH (AS\_SET counts as length 1)

- 7. Lowest origin (IGP < EGP < Incomplete)
- 8. Lowest MED

This applies only if the compared routes are from the same neighbor AS.

- **9.** eBGP is preferred before iBGP.
- 10. Lowest router ID
- **11.** Neighbor with lowest IP address
- 12. Neighbor with lowest RTG tag
- 13. The oldest path is preferred over a newly learned path.

# Influencing the routing algorithm with attributes

You have the option to influence the selection of the best path to a destination by means of the following attributes:

# Weight

Weight is a proprietary attribute, which is not propagated to neighbors by means of BGP update messages. "Weight" is valid on the local router only. You can set the attribute locally either by means of the address family or with filter policies.

# Local preference

Local preference is a BGP standard attribute (LOCAL\_PREF) and is propagated to neighbors via iBGP. All paths have a local preference of 100 by default. This attribute can be used to favor certain prefixes. The attribute can be set by address family or by filter policies.

# AS\_PATH

The AS-Path contains details of the path taken by a route. Filter policies can be used to manipulate the AS path, for example by prepending the device's own AS number multiple times. This makes the AS path appear longer to a neighbor.

# Origin

Origin is a default BGP attribute, which is propagated to all neighbors. This attribute indicates where a route originated. This could be an Interior Gateway Protocol (IGP), the Exterior Gateway Protocol (EGP, RFC 904), or "Incomplete". Here, "Incomplete" indicates a redistribution by a different routing protocol. The **origin** attribute is set automatically by the router. The origin of a route is set to IGP if it was added to BGP by means of an entry in the IPv4/IPv6 network table. The origin for a route is set to "Incomplete" if it was configured for re-distribution in the address families.

# MED

MED (MULTI\_EXIT\_DISC) is an optional BGP attribute used to distinguish between multiple inputs or outputs to the same neighbor AS. The attribute can be set by filter policies.

# **Router ID**

The router ID, also known as the BGP identifier, is the unique identifier of a router. It consists of the IPv4 address of the router. You can manually configure the router ID under **BGP instance** > **Router ID**.

# 5.1.3 Tutorial: Setting up BGPv4 under LANconfig

Two LANCOM routers are inter-connected over a WAN link and they are to be configured to use BGP to propagate certain IPv4 networks. The routers are a LANCOM 1781AW at the main office and a LANCOM 1781VA-4G at the branch office.

 $(\mathbf{\hat{n}})$ 

We assume that a WAN connection exists between the two devices.

 Enabling BGP: Open the menu item Routing protocols > BGP in the configuration of both routers and activate the Border Gateway Protocol (BGP) active check box. This enables BGP on that specific device. In the next steps you configure each BGP instance, the associated neighbors, and the networks that are to be propagated.

✓ Border Gateway Protokoll (BGP) activated
BGP-Instance
In dieser Tabelle können Parameter der BGP-Instanz wie AS-Nummer oder Router-ID konfiguriert werden.
BGP-Instance
Definieren Sie hier die Parameter der BGP-Nachbarn.
Neighbors Neighbor profiles
Network
Definieren Sie hier die Präfixe bzw. Netzwerke, die über BGP propagiert werden sollen.
IPv6 network IPv6 networks
Addressfamily
Definieren Sie hier die Parameter der Adressfamilien.
IPv4 Addressfamily IPv6 Addressfamily
BGP Policy
Here you can define policies which are applied per neighbor to incoming or outgoing attributes of prefixes.
BGP Policy

2. Configuring individual BGP instances: To configure the BGP instance of each router, click the BGP instance button.

Border Gateway Protokoll (BGP) activated	
BUP-Instance In dieser Tabelle können Parameter der BGP-In konfiguriert werden. BGP-Instance	istanz wie AS-Nummer oder Router-ID
Neighbors	
Definieren Sie hier die Parameter der BGP-Nac	hbarn.
Neighbors	Neighbor profiles
Network	
Definieren Sie hier die Präfixe bzw. Netzwerke,	die über BGP propagiert werden sollen.
IPv4 network	IPv6 networks
Addressfamily	
Definieren Sie hier die Parameter der Adressfan	ilien.
IPv4 Addressfamily	IPv6 Addressfamily
BGP Policy	
Here you can define policies which are applied of prefixes.	per neighbor to incoming or outgoing attributes
BGP Policy	

**3.** Use the configuration window to specify the general information about the BGP instance for each router. The screenshots below show the configurations for both devices for direct comparison side by side.

BGP-Instance - DEFAULT		? <b>- X-</b>	BGP-Instance - DEFAULT		? <b>×</b>
📝 Active			V Active		
Name:	DEFAULT		Name:	DEFAULT	
AS-Number:	65.000		AS-Number:	65.001	
Router-ID:	192.168.1.1		Router-ID:	192.168.2.1	
Port:	179		Port:	179	
Send Syslog notifications:	Yes 🔹		Send Syslog notifications:	Yes 🔻	
Comment:	Default Instance		Comment:	Default Instance	
	ОК	Cancel		ОК	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

Parameter	Description		
Checkbox <b>Active</b>	Enable the BGP instance of the router. This is necessary to enable communication between the two routers.		
AS number	The AS number ( <b>A</b> utonomous <b>S</b> ystem number) collects routers into the same administration unit. Entering different numbers here specifies the eBGP peers. Identical numbers indicate peers that share the same AS (iBGP).		
	() Learn which entries are valid by visiting http://www.iana.org/assignments/as-numbers/as-numbers.xhtml.		
Router ID	Specify an IP address for the router. Enter 0.0.0.0 if you want the IP address to be set automatically. The router ID must be unique among the neighbors of a BGP router.		
	① Different entries are required here.		
Port	Configure the TCP-IP port that the router uses for inbound BGP connections. The default value is 179.		
Send Syslog notifications	Specify whether the device is to generate SYSLOG messages. Use WEBconfig to view these.		
Comment	Enter a comment to make it easier to understand the configuration later.		

4. Configuring the BGP neighbors: Once the configuration of the BGP instance is complete, the next step is to define the associated neighbors for exchanging information about the propagated networks. Click on the Neighbors button.

Border Gateway Protokoll (BGP) activated	
BuP-Instance	
In dieser Tabelle können Parameter der BGP-Inst konfiguriert werden.	tanz wie AS-Nummer oder Router-ID
BGP-Instance	
Neighbors	
Definieren Sie hier die Parameter der BGP-Nacht	parn.
Neighbors	Neighbor profiles
Network	
Definieren Sie hier die Präfixe bzw. Netzwerke, d	ie über BGP propagiert werden sollen.
IPv4 network	IPv6 networks
Addressfamily	
Definieren Sie hier die Parameter der Adressfamili	ien.
IPv4 Addressfamily	IPv6 Addressfamily
BGP Policy	
Here you can define policies which are applied p of prefixes.	er neighbor to incoming or outgoing attributes
BGP Policy	

- 5. Click on the Add button to configure a new BGP neighbor. Use the configuration window to specify the information about the BGP neighbors for each router.
  - ① The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

Neighbors - New Entry		? <b>×</b>	Neighbors - Edit Entry		? 💌
🔽 Entry active			🔽 Entry active		
Name:	1781VA-4G	]	Name:	1781AW	
IP address:	1.1.1.2		IP address:	1.1.1.1	
Port:	179		Port:	179	
Source address (opt.):	•	Select	Source address (opt.):	•	Select
Routing tag:	0		Routing tag:	0	
Remote-AS:	65.001		Remote-AS:	65.000	
Password:	•	Show	Password:	•	🔲 Show
	Generate password	]		Generate password 🖛	
Connection mode:	Active -	]	Connection mode:	Active •	]
Connection delay:	120	seconds	Connection delay:	120	seconds
Neighbor profile:	DEFAULT -	Select	Neighbor profile:	DEFAULT -	Select
Inbound-Policy:	-	Select	Inbound-Policy:	-	Select
Outbound-Policy:	•	Select	Outbound-Policy:	-	Select
Comment:		]	Comment:		
	OK	Cancel		OK	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

#### Parameter Description

Entry active Activate the entry for the corresponding neighbor.

Parameter	Description
Name	Set the name for the neighbor. This example uses an abbreviated version of the device name for easy identification in the configuration.
IP address	Enter the IP address where the neighbor is to be reached. In this example, the WAN address of 1781AW is 1.1.1.1 and that of 1781VA-4G is 1.1.1.2.
Remote AS	Enter the AS numbers of the corresponding neighbors as specified in <b>step 2</b> .
Password	Enter a password, which is used to obscure communications between the two BGP neighbors by means of an MD5 hash. The password must be identical at both ends.

6. Configuring the IPv4 networks to be propagated: Configure the networks that are to be propagated by the individual BGP instances. Click on the IPv4 networks button.

📝 Border Gateway Protokoll (BGP) activated

BGP-Instance
In dieser Tabelle können Parameter der BGP-Instanz wie AS-Nummer oder Router-ID konfiguriert werden.
BGP-Instance
Neighbors
Definieren Sie hier die Parameter der BGP-Nachbarn.
Neighbors Neighbor profiles
Network
Definieren Sie hier die Präfixe bzw. Netzwerke, die über BGP propagiert werden sollen.
IPv4 network IPv6 networks
Addressfamily
Definieren Sie hier die Parameter der Adressfamilien.
IPv4 Addressfamily IPv6 Addressfamily
BGP Policy
Here you can define policies which are applied per neighbor to incoming or outgoing attributes of prefixes.
BGP Policy

7. Click the Add button to define a new IPv4 network, which is to be propagated.

() The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

IPv4 network - New Entry		? <b>×</b>	IPv4 network - New Entry		? <b>X</b>
IP address:	172.16.200.0		IP address:	172.17.100.0	
Netmask:	255.255.255.0		Netmask:	255.255.255.0	
Routing tag:	0		Routing tag:	0	
Туре:	Static 💌		Туре:	Static 💌	
Comment:			Comment:		
	ОК	Cancel		ОК	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

# Parameter Description

IP address The IPv4 address range of the network to be propagated.

Parameter	Description
Netmask	The netmask corresponding to the defined network.
Туре	The type of propagation to be used. This example is static for ease of configuration.

- 8. Write the respective configurations back to the two devices.
- 9. The BGP connection is easily checked via the command line. The command show bgp-neighbors displays all active neighbors and their status.

# 5.1.4 Tutorial: Setting preferences for prefixes

"Preference" is an optional BGP attribute used to set preferred paths to certain prefixes. The device prefers a path with a higher preference over a path with a lower preference.

Within an AS, the iBGP neighbors exchange the BGP attribute LOCAL\_PREFERENCE. The eBGP neighbors in neighboring ASs do not transmit this attribute.

There are two ways to configure preferences:

- By address family
- By policy

This example explains how to configure the prioritization of the prefix from a BGP neighbor with the preference "200" over the prefix from another BGP neighbor with the preference "100".

- The default setting for preferences is "100". In this case all you have to do is configure the neighbor that requires preferential treatment with the preference "200".
- Navigate to Routing protocols > BGP > BGP policy > Basic and add a new entry to the manipulation of basic attributes of the NLRI (in this case the basic attribute LOCAL\_PREFERENCE).

Basic - New Entry		? 💌
Name:	LOCAL_PREF	
Set Weight:	0	
Locale preference:	200	
Remove MED:	No 🔻	
Set MED:	0	
Set Nexthop:		
Comment:		
	OK	Cancel

Give the entry a descriptive name.

Under Set local preference enter the value "200" for the new local preference.

2. Under Routing protocols > BGP > Actions add a new action.

Actions - New Entry		? 🗙
Name:	Action_1	]
Basic:	LOCAL_PREF -	Select
AS Path:	-	Select
Communities:	-	Select
Comment:		
	ОК	Cancel

Give the action a descriptive name.

Under **Basic** you select the basic entry you created previously.

3. Add a new filter under Routing protocols > BGP > BGP policy > Filters.

Filters - New Entry		? 🗙
Name:	Filter_1	
Priority:	0	
Address family:	IPv4	•
Policy:	Permit	•
Match:		Select
Action:	Action_1	✓ Select
Comment:		
	ОК	Cancel

Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting "Permit" in the field **Policy** you specify that the device should modify the outbound NLRI. Under **Action** you select the action you created previously.

4. Under Routing protocols > BGP > Neighbors you add a new entry for a BGP neighbor.

Neighbors - New Entry		? <b>-</b> ×
👿 Entry active		
Name:	Headquarter	]
IP address:	192.168.1.177	]
Port:	179	]
Source address (opt.):	•	Select
Routing tag:	0	]
Remote AS:	200	]
Password:		Show
	Generate password 🖛	]
Connection mode:	Active -	]
Connection delay:	120	seconds
Route reflector client:	No 🕶	]
Neighbor profile:	DEFAULT -	Select
Inbound policy:	Filter_1 👻	Select
Outbound policy:	-	Select
Comment:		]
	OK	Cancel

Give the neighbor a descriptive name and configure its IP address along with the number of the remote AS where it is located.

If you have not created a dedicated neighbor profile for this BGP neighbor, use the "Default" profile.

Under Inbound policy you select the filter you created previously.

**5.** To check the configuration, open a terminal connection to the device.

The command show bgp-policy Filter\_1 displays the current setting for the policy "Filter\_1".

```
> show bgp-policy Filter_1
Traverse chain "Filter_1"
Inspect filter of priority 0
Match IPv4 routes
Execute action "Action_1"
No AS-path override configured
Apply basic override "LOCAL_PREF"
Set local preference to 200
No community override configured
Permit route
>
```

-

The command show bgp-v4-adj-rib-in displays the routing information base (RIB).

# 5.1.5 Tutorial: Setting the Community attribute

"Community" is an optional BGP attribute that can be used to identify prefixes and collect them into logical groups. Inbound and outbound policies can be applied to these groups. It is possible to specify multiple communities for a single prefix.

In addition to the well-known communities NO-ADVERTISE or NO-EXPORT, the meaning of a community can be freely defined by the provider. So for example, the provider of AS "64500" specifies that customer routes with the community "64500:200" are to be treated with preference "200", and routes with the community "64500:90" are to be treated with preference with the preference "90".

The following example shows how the community "64500:200" is added to all outbound routes.

1. Add a new community under Routing protocols > BGP > BGP policy > Communities (overrides).

Communities - New Entry	/	? 🗙
Name:	Community_set	
Clear:	No 👻	
Add:	64500:200	
Remove:		
Comment:		
	ОК	Cancel

Give the community a descriptive name.

Under **Add** enter the value "64500:200" for the community attribute. This value adds the device to the community attribute of the outbound NLRI.

2. Under Routing protocols > BGP > Actions add a new action.

Actions - New Entry		? 🗙
Name:	Action_2	]
Basic:		Select
AS Path:	-	Select
Communities:	Community_set 🗸	Select
Comment:		
	OK	Cancel

Give the action a descriptive name.

Under **Communities** you select the community you created previously.

3. Add a new filter under Routing protocols > BGP > BGP policy > Filters.

Filters - New Entry	? 🗙
Name:	Filter_2
Priority:	0
Address family:	IPv4 💌
Policy:	Permit 👻
Match:	Select
Action:	Action_2   Select
Comment:	
	OK Cancel

Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting "Permit" in the field **Policy** you specify that the device should modify the outbound NLRI. Under **Action** you select the action you created previously.

4. Under Routing protocols > BGP > Neighbors you add a new entry for a BGP neighbor.

		-
Name:	Central	
IP address:	192.168.1.177	
Port:	179	]
Source address (opt.):	-	Select
Routing tag:	0	
Remote AS:	200	]
Password:		📄 Show
	Generate password 🔻	]
Connection mode:	Active -	
Connection delay:	120	seconds
Route reflector client:	No	
Neighbor profile:	DEFAULT -	Select
Inbound policy:	-	Select
Outbound policy:	Filter_2 🗸	Select
Comment:		

Give the neighbor a descriptive name and configure its IP address along with the number of the remote AS where it is located.

If you have not created a dedicated neighbor profile for this BGP neighbor, use the "Default" profile.

Under **Outbound policy** you select the filter you created previously.

**5.** To check the configuration, open a terminal connection to the device.

The command show bgp-policy Filter\_2 displays the current setting for the policy "Filter\_2".

```
> show bgp-policy Filter_2
Traverse chain "Filter_2"
Inspect filter of priority 0
Match IPv4 routes
Execute action "Action_2"
No AS-path override configured
No basic override configured
Apply community override "Community_set"
Add community 64500:200
Permit route
> _
```

# 5.1.6 Tutorial: Filtering received prefixes

This example explains the configuration steps required to filter out the following inbound prefixes from a BGP neighbor:

- All prefixes in the range "192.168.0.0/16"
- The individual prefix "172.16.200.0/24"

1. Create two new entries for the prefixes to be filtered under **Routing protocols** > **BGP** > **BGP policy** > **Prefix**.

Prefix - Edit Entry		-?	🖂 🛛 Prefix - Edit Er	ntry		? 🗙
Name:	Forbidden1		Name:		Forbidden1	]
IP address:	192.168.0.0		IP address:		172.16.200.0	
Prefix length:	16		Prefix length:		24	]
Min. Prefix Length:	0		Min. Prefix Le	ngth:	0	
Max. Prefix Length:	32		Max. Prefix Le	ength:	0	
Comment:			Comment:			]
	OK	Cancel			OK	Cancel
Prefix					-?	
Name IP address	Prefix length Mi	n. Prefix Length	Max. Prefix Length	Comment	ОК	
Forbidden1 172.16.200 Forbidden1 192.168.0.0	.0 24 0 ) 16 0		0 32		Cano	el

Give each entry a descriptive name.

₽ QuickFinder

(i) Add an entry for each prefix to be filtered, but give each entry the same name.

Add...

Edit...

For each entry specify the IP address and the prefix length.

2. Specify a match for the previously created prefix entries under **Routing protocols** > **BGP** > **BGP policy** > **Matches**.

Copy...

Remove

Matches - New Entry		? 💌
Name:	Matchlist	]
Prefix:	Forbidden1 -	Select
AS Path:		Select
Communities:		Select
Comment:		]
	OK	Cancel

Give the entry a descriptive name.

Under **Prefix** you select the name of the prefix you added previously.

3. Add a new filter under Routing protocols > BGP > BGP policy > Filters.

Filters - New Entry		? 🗙
Name:	Filter_3	
Priority:	0	]
Address family:	IPv4	•
Policy:	Deny	•
Match:	Matchlist	Select
Action:	-	Select
Comment:		
	OK	Cancel

Give the filter a descriptive name.

Under **Address family** you select the protocol used for connections to the BGP neighbors. With the setting "Deny" in the field **Policy** you instruct the device to filter out the inbound prefixes. Under **Match** you select the match you created previously.

4. To check the configuration, open a terminal connection to the device.

The command show bgp-policy Filter\_3 displays the current setting for the policy "Filter\_3".

```
> show bgp-policy Filter_3
Traverse chain "Filter 3"
   Inspect filter of priority 0
     Match IPv4 routes
     Assess match "Matchlist"
        Evaluate prefix list "Prohibited1"
           Analyze prefix 172.16.200.0
              Match IPv4 routes
              Match route's 24 MSB
              Match route prefix length in [24, 24]
            Analyze prefix 172.168.0.0
              Match IPv4 routes
              Match route's 16 MSB
              Match route prefix length in [16, 32]
        No AS-path list configured
        No community list configured
      Deny route
```

# 5.1.7 Additions to the Setup menu

# **Routing protocols**

In this directory, you configure the routing protocols and the route monitor.

#### SNMP ID:

2.93

Telnet path:

Setup

# BGP

This directory is used to configure the device for the Border Gateway Protocol version 4 (BGPv4).

#### SNMP ID:

2.93.1

### Telnet path:

Setup > Routing-protocols

# **BGP** instance

This table is used to configure the BGP instances.

**(i)** 

Since the device only supports one BGP instance at a time, this table contains just one entry.

SNMP ID:

2.93.1.1

Telnet path:

Setup > Routing-Protocols > BGP

# Name

Contains the name of the BGP instance.



The factory settings already include the entry "DEFAULT".

# SNMP ID:

2.93.1.1.1

Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

# Operating

Activates or deactivates this BGP instance



This setting only takes effect if BGP is activated on the device.

# SNMP ID:

2.93.1.1.2

# Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

# **Possible values:**

Yes

The BGP instance is enabled.

# No

The BGP instance is disabled.

#### Default:

No

# **AS number**

The AS number assigned to this BGP instance.

It is only possible to connect to a BGP router that does not support 32-bit AS numbers if you enter a 16-bit AS number here (less than 65536).

# SNMP ID:

2.93.1.1.3

# Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

0

# **Router ID**

The router ID (IPv4 address) of this particular BGP instance.

#### SNMP ID:

2.93.1.1.4

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

#### **Possible values:**

Max. 15 characters from [0-9].

# Default:

0.0.0.0

# Syslog

The device is able to store events, such as disconnects of neighbors associated with this BGP instance, to the SYSLOG. Use this option to enable or disable this feature.

# SNMP ID:

2.93.1.1.5

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

Addendum

5 Routing and WAN connections

#### **Possible values:**

Yes

Logging to SYSLOG is enabled.

No

Logging to SYSLOG is disabled.

# Default:

No

# Port

Here you specify the port used by the BGP instance to listen to incoming connections from neighbors.

# SNMP ID:

2.93.1.1.6

# Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

# Possible values:

Max. 5 characters from [0-9]

# Default:

179

# Comment

Comment about this BGP instance.

# SNMP ID:

2.93.1.1.7

# Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

# **Possible values:**

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

# Default:

Default instance

# **Check-First-AS**

Checks whether the first AS number in the AS path of received Update messages corresponds to the AS number of the neighbor. If this is not the case, this route is discarded.

(1) This check must be disabled if the router is connected with a BGP route server which, although it distributes routes, is not itself in the routing path and/or inserts its own AS into the AS path.

### SNMP ID:

2.93.1.1.8

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

**Possible values:** 

Yes No

#### Default:

Yes

# **AS-Path-Limit**

Maximum number of permitted AS numbers in the AS path of received Update messages. If the limit is exceeded, the device discards the route. An AS-Path-Limit provides protection against messages from incorrectly configured routers that advertise AS paths that are too long.

# SNMP ID:

2.93.1.1.9

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

#### **Possible values:**

Max. 5 characters from [0-9]

#### Default:

0

# Cluster-ID

Cluster-ID of the router in case it is configured as a route reflector. This is entered as an IPv4 address.

### SNMP ID:

2.93.1.1.10

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

### **Possible values:**

Max. 15 characters from [0-9]

# Default:

0.0.0.0

# **Route-Reflector**

This specifies whether the router assumes the function of a route reflector.

When operating iBGP, all of the BGP routers usually need to be fully meshed, i.e. each BGP router must have established a BGP connection to every other BGP router. A route reflector negates this requirement and enables iBGP routers to form, for example, a star-shaped topology. A route reflector forwards the iBGP routes to all of the route-reflector clients.

A route reflector is able to serve route-reflector clients as well as normal BGP clients. In both cases no special configuration of the client is necessary.

# SNMP ID:

2.93.1.1.11

#### Telnet path:

Setup > Routing-Protocols > BGP > BGP-Instance

Possible values:

Yes No

# Default:

No

# **TX-Loop-Detection**

When activated, loop detection influences the behavior of the BGP instance as follows:

- 1. The BGP instance does not propagate any routes to neighbors, whose AS numbers are in the AS path of the route.
- 2. The BGP instance sends local routes to iBGP neighbors only if the neighbor is a route-reflector client and the local BGP instance is a route reflector.
- 3. The BGP instance does not distribute a route to neighbors who have already learned it.

These measures reduce the unnecessary sending of messages that a neighbor might reject due to its own loop detection.

In certain VPN/ARF scenarios, the TX-loop detection must be disabled.

# SNMP ID:

2.93.1.1.12

Telnet path:

```
Setup > Routing-Protocols > BGP > BGP-Instance
```

**Possible values:** 

Yes No

#### Default:

Yes

# Neighbors

This table is used to configure the BGP neighbors.

A new entry can be created here simply by specifying an **IP address**, although BGP instances will ignore this entry unless the following conditions are met:

- The entry is enabled by setting **Operating** to "Yes".
- The Instance name corresponds to the BGP instance name configured under Setup > Routing-Protocols > BGP > BGP-Instance.
- The Neighbor profile corresponds to a profile entered under Setup > Routing-Protocols > BGP > Neighbor-Profiles.

The table is empty by default.

# SNMP ID:

2.93.1.2

**Telnet path:** 

Setup > Routing-Protocols > BGP

# **IP** address

Specifies this BGP neighbor's IP address (IPv4 or IPv6) as used by the device to establish a BGP connection in the "active" or "delayed" connection mode.



This entry must match the IP address (e.g. physical interface address, loopback address) reported by this neighbor in an incoming connection.

# SNMP ID:

2.93.1.2.1

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### **Possible values:**

```
Max. 56 characters from [A-F][a-f][0-9].:-%
```

#### Default:

empty

# Port

Shows the port on which the BGP neighbor expects inbound BGP messages and, correspondingly, the port used by the device for outbound connections of the connection type "active" or "delayed".

The device accepts incoming connections from any source port that is used by the sender.

# SNMP ID:

2.93.1.2.2

# Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### **Possible values:**

Max. 5 characters from [0-9]

#### Default:

179

# Loopback address

Contains the sender address (IPv4 or IPv6) that the device uses when connecting to the BGP neighbor. The field allows you to enter loopback addresses as configured under **Setup** > **TCP-IP** > **Loopback-List** and **Setup** > **IPv6** > **Network** > **Loopback**.



Entry is optional and is only relevant for the connection modes "active" and "delayed".

# SNMP ID:

2.93.1.2.3

#### **Telnet path:**

Setup > Routing-Protocols > BGP > Neighbors

#### **Possible values:**

```
Max. 56 characters from [A-Z][0-9]@{|}~! $%&'()+-,/:;<=>?[\]^_.
```

#### Default:

empty

# Special values:

empty

When setting the sender address for the TCP connection, the device attempts to find a suitable loopback address from the same subnet as the IP address of the BGP neighbor.
# **Rtg-Tag**

Contains the routing tag. The device denies the connection if the routing tag does not match with the incoming connection.

#### SNMP ID:

2.93.1.2.4

# Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

## **Possible values:**

Max. 5 characters from [0-9] 0...65536

# Default:

0

# **Remote AS**

Contains the AS number of the BGP neighbor.



If the AS number of the BGP neighbor is identical to the AS number of the device's own BGP instance, then this neighbor is an iBGP peer (internal BGP) within the AS.

# SNMP ID:

2.93.1.2.5

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

0

## Name

Contains the name of the BGP neighbor.

(i) Use this name as an argument when executing the following actions:

- Manual start under Setup > Routing-Protocols > BGP
- Manual stop under Setup > Routing-Protocols > BGP
- Active start under Setup > Routing-Protocols > BGP

SNMP ID:

2.93.1.2.6

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

# Possible values:

Max. 16 characters from [A-Z][a-z][0-9]-\_

# Default:

empty

# Operating

Activates or deactivates this BGP neighbor.

(i) The activation of the BGP neighbor triggers the establishment of a BGP connection, if applicable.



Outbound and inbound connections are not possible with a disabled BGP neighbor.

## SNMP ID:

2.93.1.2.7

# Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

#### **Possible values:**

#### Yes

The BGP neighbor is enabled. It is possible to establish a BGP connection with it.

# No

The BGP neighbor is disabled. It is not possible to establish a BGP connection (transmit or receive) with it.

# Default:

Yes

# Password

The device and the BGP neighbor authenticate themselves by exchanging this password in the form of an MD5 signature in the TCP packets.



Authentication is not used if no password is set.

# SNMP ID:

2.93.1.2.8

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### **Possible values:**

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

Default:

empty

# **Neighbor profile**

Contains the name of the BGP neighbor profile from **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

**()** 

If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

### SNMP ID:

2.93.1.2.9

# Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

# Possible values:

Max. 16 characters from [A-Z][a-z][0-9]-\_

# Default:

DEFAULT

# **Connection mode**

Sets the mode in which the connection is established from the device to this BGP neighbor.

(i) All three modes accept connections initiated by the neighbor.

#### **SNMP ID:**

2.93.1.2.10

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

# Possible values:

### Operating

In this mode the device attempts to connect to the BGP neighbor as soon as, among other things, one of the following conditions is met:

- The BGP neighbor is completely configured.
- You execute the action Manual start.

- You start the device.
- The BGP instance is enabled under Setup > Routing-Protocols > BGP > BGP-Instance > Operating.
- You enable this BGP neighbor under **Operating**.

#### Passive

In this mode the device does not actively connect to the BGP neighbor; instead, it waits for a connection request from the BGP neighbor.

### Delayed

In this mode the device waits for a timeout before it tries to connect to the BGP neighbor. The conditions for establishing a connection are the same as for the "Active" mode.

### Default:

Operating

# **Connection delay**

Specifies the wait time in seconds before the device in the "delayed" connection mode establishes a connection to this BGP neighbor.

### SNMP ID:

2.93.1.2.11

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### Possible values:

Max. 5 characters from [0-9]

#### Default:

120

# Special values:

0

Corresponds to the "active" connection mode, i.e. connection establishment is immediate.

### Instance name

Specifies the name of the associated BGP instance under **Setup** > **Routing-Protocols** > **BGP** > **BGP-Instance**.

() If an entry is missing or incorrect, the BGP neighbor configuration is considered to be incomplete, and it is not possible to connect to it.

### SNMP ID:

2.93.1.2.12

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-

### Default:

DEFAULT

# Inbound policy

Specifies the policy used by the device to filter the incoming prefixes from this BGP neighbor.

The policy is configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters**.



If you leave this field empty, the device filters the incoming prefixes according to the default policy under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Default**.

## SNMP ID:

2.93.1.2.13

## Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

# Possible values:

Max. 16 characters from [A-Z][a-z][0-9]-\_

# Default:

empty

### Outbound policy

Specifies the policy used by the device to filter the outbound prefixes to this BGP neighbor.

The policy is configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Filters**.

If you leave this field empty, the device filters the outbound prefixes according to the default policy under Setup > Routing-Protocols > BGP > Policy > Default.

## SNMP ID:

2.93.1.2.14

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

### **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

### Default:

empty

## Comment

Contains a comment about this BGP neighbor.

#### SNMP ID:

2.93.1.2.15

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

## **Possible values:**

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

### Default:

empty

# **Route-Reflector-Client**

Specifies whether this neighbor is treated as a route-reflector client, in which case the device reflects iBGP routes back to it.

(i) This switch is valid only if

- The device has been configured as a route reflector in the in the BGP instance, i.e. is a route reflector itself, or
- The remote AS number matches its own AS number (iBGP).

### SNMP ID:

2.93.1.2.16

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbors

**Possible values:** 

Yes No

# Default:

No

# **Neighbor profiles**

This table is used to configure the BGP neighbor profiles.

Neighbor profiles are used to specify a general configuration, which can be assigned to different BGP neighbors.

A default entry already exists under the name "DEFAULT" and containing the comment "Default Entry".

#### SNMP ID:

2.93.1.3

Telnet path:

Setup > Routing-Protocols > BGP

# Name

Contains the name of the profile.

This name is used in the following tables, among other things:

- Neighbor profile under Setup > Routing-Protocols > BGP > Neighbors
- Neighbor profile under Setup > Routing-Protocols > BGP > Address-Family > IPv4
- Neighbor profile under Setup > Routing-Protocols > BGP > Address-Family > IPv6

### SNMP ID:

2.93.1.3.1

## Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

## **Possible values:**

```
Max. 16 characters from [A-Z][a-z][0-9]-_
```

# Default:

empty

# Route update delay

This is the minimum delay in seconds between BGP advertisements sent by the device to neighbors using this profile.

# SNMP ID:

2.93.1.3.2

### **Telnet path:**

Setup > Routing-Protocols > BGP > Neighbor-Profiles

#### **Possible values:**

Max. 5 characters from [0-9]

# Default:

30

# Send-TTL

Specifies the TTL (time to live) that the device sets for TCP packets sent to the BGP neighbors that use this profile.

For directly connected neighbors, this value is set to "1". For eBGP environments, you can increase this value by 1 per hop.

For iBGP sessions, the device ignores this value and defaults to the maximum TTL value.

This value must be "0" if Recv-TTL is set to a value other than "0". The device automatically uses the value "1" if both Send-TTL and Recv-TTL are set to "0".

# SNMP ID:

2.93.1.3.3

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

### **Possible values:**

Max. 3 characters from [0-9]

## Default:

1

# **Recv-TTL**

Specifies the minimum TTL (time to live) required of inbound TCP packets from BGP neighbors that use this profile. Inbound TCP packets must have a TTL greater than or equal to this value in order to be accepted.



#### SNMP ID:

2.93.1.3.4

# Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

## Possible values:

Max. 3 characters from [0-9]

# Default:

1

# Special values:

0

Disables TTL checks of inbound TCP packets.

# Keepalive

Specifies the time in seconds for the keepalive timer. After this time has elapsed, the device sends a keepalive message to the neighbors using this profile in order to keep the BGP connection intact.

The device should send at least three keepalive messages per unit of holdtime. For this reason the value should be max. one third of the holdtime. If the value is set higher than this or equal to "0", the LCOS automatically sets an internal value that is one-third of the holdtime.

## SNMP ID:

2.93.1.3.5

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

#### **Possible values:**

Max. 5 characters from [0-9]

### Default:

30

0 ... 65536

# Holdtime

Specifies the time in seconds for which the device considers a BGP connection without traffic to still be valid.

The device negotiates this value with the BGP neighbors during connection establishment. The lower of the two values is considered to be valid.

If negotiation results in a value of "0", the device considers the connection to be valid until it receives a connection error or the connection breaks. No keepalive messages are sent to the BGP neighbors during this period, even if the keepalive timer is set with a value.

 $( \mathbf{I} )$ 

In accordance with the RFC, the values "1" and "2" are not permitted.

# SNMP ID:

2.93.1.3.6

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

#### **Possible values:**

Max. 5 characters from [0-9]

#### Default:

90

# **Special values:**

0

The device considers the connection to be valid until an error notification is received or the connection breaks. The transmission of keepalive messages is deactivated even if the keepalive timer is set with a value.

# Filter private AS

Controls the removal/replacement of private AS entries (64512 - 65535, 420000000 - 4294967294) from the AS\_PATH list of outbound prefixes of BGP neighbors that use this profile.



This option has no function for iBGP connections.

#### SNMP ID:

2.93.1.3.7

#### Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

### Possible values:

Replace

Replaces all private AS numbers in the AS\_PATH with the AS number of the device.

Remove

Removes all private AS numbers from the AS\_PATH.

## No

Leaves all of the private AS numbers in the AS\_PATH.

## Default:

No

# AS override

Enables or disables the overriding of AS numbers in the AS\_PATH outbound prefixes.

With this option enabled, the device replaces all of the AS numbers of the BGP neighbors with its own AS number.

### SNMP ID:

2.93.1.3.8

## Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

### **Possible values:**

Yes

Replaces all AS numbers of BGP neighbors in the AS\_PATH with its own AS number.

No

Leaves all AS numbers of BGP neighbors in the AS\_PATH.

### Default:

No

# Comment

Comment on this entry.

#### SNMP ID:

2.93.1.3.10

### Telnet path:

Setup > Routing-Protocols > BGP > Neighbor-Profiles

# **Possible values:**

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

#### Default:

empty

### **Address family**

Use this directory to configure the settings of the IPv4 and IPv6 parameters that apply to all of the devices of a BGP neighbor profile.

### SNMP ID:

2.93.1.4

#### Telnet path:

Setup > Routing-Protocols > BGP

## IPv4

Use this table to configure the IPv4 settings that apply to all of the devices of a BGP neighbor profile. By default, an "activated" entry named "DEFAULT" is already provided.

#### SNMP ID:

2.93.1.4.1

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily

# **Neighbor profile**

Contains the name of the corresponding neighbor profile as saved under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

#### SNMP ID:

2.93.1.4.1.1

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

### **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

### Default:

empty

# **Rtg-Tag**

This determines that the device only advertises the IPv4 routes set under **Setup** > **Routing-Protocols** > **BGP** > **Networks** > **IPv4** to the BGP neighbors if their routing tag matches the one configured here.

## SNMP ID:

2.93.1.4.1.2

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

#### **Possible values:**

Max. 5 characters from [0-9]

#### Default:

empty

# Operating

Enables or disables the distribution of IPv4 NLRI of this address family to the BGP neighbors that use this neighbor profile.

# SNMP ID:

2.93.1.4.1.3

#### Telnet path:

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

# **Possible values:**

# Yes

This entry is enabled. The device sends IPv4 routes to the BGP neighbors.

#### No

This entry is disabled. The device does not send IPv4 routes to the BGP neighbors, but depending on the setting it may send IPv6 routes.

### Default:

No

# Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options "Standard" and "Extended" are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

(f) This option is of no relevance for communications with iBGP neighbors.

#### SNMP ID:

2.93.1.4.1.4

#### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

# **Possible values:**

# Default

When activated, the device permits the standard community attributes in the NLRI in accordance with *RFC 1997*.

#### Advanced

When activated, the device permits the extended community attributes in the NLRI in accordance with *RFC 4360*.

#### Default:

Default

Advanced

# Nexthop-Self

Enables or disables the replacement in the NLRI of the next hop attribute by the device's own IP address.

#### SNMP ID:

2.93.1.4.1.5

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

## **Possible values:**

Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

#### No

Leaves the IP address of the next hop in the NLRI unchanged.

# Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

# Default:

No

# Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.



"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

# SNMP ID:

2.93.1.4.1.6

## Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

## **Possible values:**

```
Max. 5 characters from [0-9]
0...65535
```

## Default:

0

# Local-Pref

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Local preference" is a BGP standard attribute (LOCAL\_PREF) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

#### SNMP ID:

 $(\mathbf{i})$ 

2.93.1.4.1.7

### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

#### **Possible values:**

Max. 5 characters from [0-9] 0... 99999

#### Default:

100

# **Prefix limit**

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

### SNMP ID:

2.93.1.4.1.8

#### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

0

# **Special values:**

0

The prefix limit is disabled.

# **Route redistribute**

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



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

#### SNMP ID:

2.93.1.4.1.9

### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

# Possible values:

Static

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

### Connected

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

### Comment

Comment on this entry.

#### SNMP ID:

2.93.1.4.1.10

## Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

# **Possible values:**

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

# IPv6

Use this table to configure the IPv6 settings that apply to all of the devices of a BGP neighbor profile. By default, one "deactivated" entry named "DEFAULT" is already provided.

#### SNMP ID:

2.93.1.4.2

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily

# **Neighbor profile**

Contains the name of the corresponding neighbor profile as saved under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

### SNMP ID:

2.93.1.4.2.1

#### Telnet path:

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

# **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

## Default:

empty

# **Rtg-Tag**

This determines that the device only advertises the IPv6 routes set under **Setup** > **Routing-Protocols** > **BGP** > **Networks** > **IPv6** to the BGP neighbors if their routing tag matches the one configured here.

#### SNMP ID:

2.93.1.4.2.2

#### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

# Possible values:

Max. 5 characters from [0-9]

## Default:

empty

# Operating

Enables or disables the distribution of NLRI of this address family to the BGP neighbors that use this neighbor profile.

### SNMP ID:

2.93.1.4.2.3

### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

### **Possible values:**

# Yes

This entry is enabled. The device sends IPv6 routes to the BGP neighbors.

#### No

This entry is disabled. The device does not send IPv6 routes to the BGP neighbors, but depending on the setting it may send IPv4 routes.

### Default:

No

# Communities

Controls which community attributes are sent in the NLRI of this address family to eBGP neighbors that use the referenced neighbor profile.

If the options "Standard" and "Extended" are both disabled, the device transmits no community attributes in the NLRI to the eBGP neighbors.

This option is of no relevance for communications with iBGP neighbors.

# SNMP ID:

2.93.1.4.2.4

## Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

# Possible values:

### Default

When activated, the device permits the standard community attributes in the NLRI in accordance with *RFC 1997*.

### Advanced

When activated, the device permits the extended community attributes in the NLRI in accordance with *RFC 4360*.

#### Default:

Default

Advanced

# Nexthop-Self

Enables or disables the replacement in the NLRI of the next-hop attribute by the device's own IP address.

## SNMP ID:

2.93.1.4.2.5

### Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

#### **Possible values:**

### Yes

In the NLRI, the IP address of the next hop is replaced with the device's own IP address.

### No

Leaves the IP address of the next hop in the NLRI unchanged.

### Always

Always exchanges the IP address of the next hop in the NLRI with its own IP address, even if the device is configured as a route reflector.

Default:

No

# Weight

Specifies the default weight for the NLRI.

This information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.

"Weight" is a proprietary attribute that the device does not propagate to other eBGP neighbors in BGP update messages. This attribute is valid on the local router only.

## SNMP ID:

2.93.1.4.2.6

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

#### Possible values:

Max. 5 characters from [0-9] 0... 65535

# Default:

0

# Local-Pref

Similar to the **Weight** attribute, this information influences the preference of identical prefix advertisements that the device receives from different BGP neighbors. The prefix with the higher weight is given preference.



"Local preference" is a BGP standard attribute (LOCAL\_PREF) that the device propagates to neighbors via iBGP. All paths have a "local preference" of 100 by default.

#### SNMP ID:

2.93.1.4.2.7

## Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

# Possible values:

Max. 5 characters from [0-9] 0... 99999

#### Default:

100

# **Prefix limit**

Determines the number of prefixes accepted for each BGP neighbor of the specified neighbor profile.

The device rejects all prefixes received beyond this limit.

## SNMP ID:

2.93.1.4.2.8

# Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

### **Possible values:**

Max. 10 characters from [0-9]

# Default:

0

### **Special values:**

0

The prefix limit is disabled.

# **Route redistribute**

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



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

## SNMP ID:

2.93.1.4.2.9

## Telnet path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv6

### **Possible values:**

## Static

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

## Connected

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

# Comment

Comment on this entry.

## SNMP ID:

2.93.1.4.2.10

#### Telnet path:

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

### **Possible values:**

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

### Policy

Use this directory to configure the filter settings for outbound and inbound NLRIs.

#### SNMP ID:

2.93.1.5

### Telnet path:

Setup > Routing-Protocols > BGP

# Default

The device applies this default policy for a BGP neighbor if it is unclear whether it should accept its prefix or not. The cause for this may be:

- There is no policy configured for this BGP neighbor.
- The specified filter does not exist.
- None of the filters specified under Setup > Routing-Protocols > BGP > Policy > Filters applies.

#### SNMP ID:

2.93.1.5.1

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy

# **Possible values:**

### Permit

The device accepts the prefix from the BGP neighbor.

#### Deny

The device rejects the prefix from the BGP neighbor.

# **Overrides**

This directory contains the list of possible manipulations to NLRIs. The actions in the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions** apply the overrides configured here.

### SNMP ID:

2.93.1.5.2

# Telnet path:

Setup > Routing-Protocols > BGP > Policy

# Basic

This table contains overrides that manipulate the basic attributes of NLRIs.

If an action applies a row of this table, all of the manipulations that this row implements are processed.

The specification of basic attributes is optional. If you want the action to change just one basic attribute, enter the desired value at the appropriate place and leave the remaining attributes in their default setting.

## SNMP ID:

```
2.93.1.5.2.1
```

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides

# Name

Contains the name of this modification.

This entry is referenced by the actions configured under **Setup** > **Routing**-**Protocols** > **BGP** > **Policy** > **Actions**.

#### **SNMP ID:**

2.93.1.5.2.1.1

#### Telnet path:

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

## **Possible values:**

Max. 16 characters from [A-z][a-z][0-9]-\_

### Default:

empty

# Set-Weight

If configured, this entry causes the device to modify the weighting of an NLRI to the value specified here.

#### SNMP ID:

2.93.1.5.2.1.2

# Telnet path:

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

### Possible values:

Max. 5 characters from [0-9]

# Default:

0

# Special values:

0

The device retains the original value of the NLRI.

# Set-Local-Pref.

If configured, this entry causes the device to modify the local preference value of an NLRI to the value specified here.

### SNMP ID:

2.93.1.5.2.1.3

## Telnet path:

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

# **Possible values:**

Max. 10 characters from [0-9]

## Default:

0

## Special values:

0

The device retains the original value of the NLRI.

# **Remove-MED**

If configured, the device deletes the multi-exit discriminator (MED) of an NLRI before it processes the setting under **Set-MED**.

#### SNMP ID:

2.93.1.5.2.1.4

# Telnet path:

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

### **Possible values:**

No

The MED remains in the NLRI.

#### Yes

The device deletes the MED of the NLRI.

### Default:

No

# Set-MED

If configured, this entry causes the device to modify the multi-exit discriminator (MED) of an NLRI to the value specified here. If the NLRI contains no MED, the device creates this attribute.

#### SNMP ID:

2.93.1.5.2.1.5

# Telnet path:

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

### **Possible values:**

Max. 10 characters from [0-9]

# Default:

0

## Special values:

0

The device retains the original value of the NLRI.

# Set-Nexthop

If configured, this entry causes the device to modify the next-hop IP address of an NLRI to the value specified here.

## SNMP ID:

2.93.1.5.2.1.6

# Telnet path:

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

# **Possible values:**

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

### Default:

empty

# **Special values:**

empty

The device retains the original value of the NLRI.

# self

The device replaced the next-hop IP address with its own IP address.

## Comment

Comment on this entry.

#### SNMP ID:

2.93.1.5.2.1.7

### Telnet path:

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

## **Possible values:**

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

### Default:

empty

# Set-Link-Local-Nexthop

If configured, this entry causes the device to modify the next-hop link-local IPv6 address of an NLRI to the value specified here. This only effects IPv6 prefixes.

### SNMP ID:

2.93.1.5.2.1.8

# Telnet path:

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

# **Possible values:**

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

## Default:

empty

# AS-Path

This table contains overrides that manipulate the AS\_PATH attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

- 1. Filter private
- 2. Replace
- 3. Together Prepend count and Prepend

# SNMP ID:

2.93.1.5.2.2

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides

# Name

Contains the name of this modification.

This entry is referenced by the actions configured under Setup > Routing-Protocols > BGP > Policy > Actions.

### SNMP ID:

2.93.1.5.2.2.1

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

## Possible values:

Max. 16 characters from [A-z][a-z][0-9]-\_

### Default:

empty

# Filter private AS

If configured, this entry causes the device to modify the specification of the private AS numbers in the AS\_PATH attribute of an NLRI in accordance with this setting.

### SNMP ID:

2.93.1.5.2.2.2

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

## Possible values:

# Replace

The device replaces the existing private AS numbers with the AS number of the current BGP instance.

# Remove The device removes all private AS numbers.

No

The device retains the existing private AS numbers of the NLRI.

### Default:

No

# Replace

If configured, this entry causes the device to change the AS\_PATH attribute of the NLRI to the value specified here.

#### SNMP ID:

2.93.1.5.2.2.3

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

#### **Possible values:**

Max. 62 characters from [0-1],

# Default:

empty

## **Special values:**

empty

The device retains the original value of the NLRI.

# Prepend

If configured, this entry causes the device to prepend the AS\_PATH attribute of the NLRI with the value entered here as often as is specified under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path** > **Prepend-Count**.

### SNMP ID:

2.93.1.5.2.2.4

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

### **Possible values:**

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

### Default:

empty

### Special values:

empty

The device retains the original value of the NLRI.

#### self

The device prepends the AS\_PATH attribute of the NLRI with its own AS number.

#### last

The device prepends the AS\_PATH attribute of the NLRI with the most recently used AS number.

# **Prepend count**

Determines how often the device prepends the AS\_PATH attribute of the NLRI with an AS number.

#### SNMP ID:

2.93.1.5.2.2.5

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

#### Addendum

5 Routing and WAN connections

### **Possible values:**

Max. 2 characters from [0-9]

# Default:

0

# Special values:

0

The device retains the original value of the NLRI even if an entry is configured under Prepend.

# Comment

Comment on this entry.

#### SNMP ID:

2.93.1.5.2.2.6

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > AS-Path

# **Possible values:**

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

### Default:

empty

# Communities

This table contains overrides that manipulate the Communities attributes of NLRI.

If an action applies a row of this table, all of the manipulations that this row implements are processed in the following sequence:

- 1. Delete
- 2. Add
- 3. Remove

### SNMP ID:

2.93.1.5.2.3

Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides

# Name

Contains the name of this modification.

This entry is referenced by the actions configured under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions**.

#### SNMP ID:

2.93.1.5.2.3.1

# Telnet path:

```
Setup > Routing-Protocols > BGP > Policy > Overrides > Communities
```

# **Possible values:**

Max. 16 characters from [A-z][a-z][0-9]-

## Default:

empty

# Clear

Determines whether the device deletes unknown communities from the NLRI.

(i) Known communities remain in place even if this option to set to "Yes".

Known communities are:

```
no-peer
```

```
no-export
```

- no-advertise
- no-export-subconfed

(i) For more information, please see *RFC 1997* and *RFC 3765*.

### SNMP ID:

2.93.1.5.2.3.2

## Telnet path:

### Setup > Routing-Protocols > BGP > Policy > Overrides > Communities

#### **Possible values:**

# Yes

The device deletes unknown communities from the NLRI.

## No

The device does not change the communities of an NLRI.

# Default:

No

# Add alarm

Specifies which communities the device adds to an NLRI.

```
Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>: <Value2>, <AS-number3>: <Value3>).
```

#### SNMP ID:

2.93.1.5.2.3.3

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Overrides > Communities

### **Possible values:**

```
Max. 62 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

# Default:

empty

# Remove

Specifies which communities the device removes from an NLRI.

Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>: <Value2>, <AS-number3>: <Value3>).

(i) Known communities are not removed from NLRI. Known communities are:

- no-peer
- no-export
- no-advertise
- no-export-subconfed

The following input formats are available for communities:

Input format	Community
1:2	Standard community
1.2.3.4:1	IPv4-specific extended community
roc:1.2.3.4:1	IPv4-specific route origin extended community (Site-of-Origin (SoO))
rtc:1.2.3.4:1	IPv4-specific route target extended community
ext2:1:2	Two-byte AS extended community
ext4:1:2	Four-byte AS extended community
roc:1:2	Two-byte AS route origin extended community (Site-of-Origin (SoO))
rtc:1:2	Two-byte AS route origin extended community
roc:ext4:1:2	Four-byte AS route origin extended community (Site-of-Origin (SoO))

### SNMP ID:

2.93.1.5.2.3.4

#### **Telnet path:**

Setup > Routing-Protocols > BGP > Policy > Overrides > Communities

### **Possible values:**

```
Max. 62 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

## Default:

empty

# Comment

Comment on this entry.

### SNMP ID:

2.93.1.5.2.3.5

## Telnet path:

### Setup > Routing-Protocols > BGP > Policy > Overrides > Communities

### **Possible values:**

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

# Default:

empty

# Actions

This table lists actions that carry out modifications to NLRIs.

The modifications carried out by each action are specified in the directory **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides**.

#### SNMP ID:

2.93.1.5.3

# Telnet path:

Setup > Routing-Protocols > BGP > Policy

# Name

Contains the name of this action.

This entry is referenced by the actions entered under Setup > Routing-Protocols > BGP > Policy > Filters.

## SNMP ID:

2.93.1.5.3.1

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Actions

### **Possible values:**

```
Max. 16 characters from [A-z][a-z][0-9]-_
```

# Default:

empty

# Basic

Contains the name of an override of basic entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**.

#### SNMP ID:

2.93.1.5.3.2

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Actions

# Possible values:

Max. 16 characters from [A-z][a-z][0-9]-

### Default:

empty

# **AS-Path**

Contains the name of an override of AS\_PATH entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **AS-Path**.

#### SNMP ID:

2.93.1.5.3.3

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Actions

# **Possible values:**

Max. 16 characters from [A-z][a-z][0-9]-

# Default:

empty

# Community

Contains the name of an override of Community entries in the NLRI.

This entry refers to the entries in the table under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Communities**.

#### SNMP ID:

2.93.1.5.3.4

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Actions

# **Possible values:**

Max. 16 characters from [A-z][a-z][0-9]-

### Default:

empty

# Comment

Comment on this entry.

### SNMP ID:

2.93.1.5.3.5

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Actions

## Possible values:

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

### Default:

empty

# Lists

This directory contains definitions used by BGP filters to identify NLRIs and execute the corresponding actions.

# SNMP ID:

2.93.1.5.4

# Telnet path:

Setup > Routing-Protocols > BGP > Policy

# Prefix

This table contains prefix lists that are used to identify NLRIs based on their network (prefix) and netmask (prefix length). An entry can contain several prefixes.

#### SNMP ID:

2.93.1.5.4.1

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists

# Name

Contains the name of this prefix list.

### SNMP ID:

2.93.1.5.4.1.1

# Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

### **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

### Default:

empty

# **IP** address

Contains the IPv4 or IPv6 address of the network.

### SNMP ID:

2.93.1.5.4.1.2

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

# **Possible values:**

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

# Default:

empty

# **Prefix-Length**

Contains the netmask or prefix length of the network.

This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address.

The prefix length of the NLRI must exactly match this value unless **Length-min** and **Length-max** are set to values not equal to zero.

#### SNMP ID:

2.93.1.5.4.1.3

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

# **Possible values:**

Max. 3 characters from [0-9]

# Default:

0

## **Special values:**

0

The network of the NLRI matches if it comes from same IP address family as that specified under IP address.

# Length-Min

Specifies the minimum prefix length value that the network of the NLRI needs in order to match.

## SNMP ID:

2.93.1.5.4.1.4

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

# Possible values:

Max. 3 characters from [0-9]

### Default:

0

# Length-Max

Specifies the maximum prefix length value that the network of the NLRI needs in order to match.

(i) If this entry is less than the value for **Prefix-Min**, the value "0" applies.

### SNMP ID:

2.93.1.5.4.1.5

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

### **Possible values:**

Max. 3 characters from [0-9]

### Default:

0

Addendum

5 Routing and WAN connections

## Special values:

0

No maximum prefix length.

# Comment

Comment on this entry.

## SNMP ID:

2.93.1.5.4.1.6

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Prefix

## **Possible values:**

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

# Default:

empty

# **AS-Path**

This table contains AS-path lists in order to identify NLRIs by their AS\_PATH attributes.

# SNMP ID:

2.93.1.5.4.2

### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists

# Name

Contains the name of this AS-path list.

# SNMP ID:

2.93.1.5.4.2.1

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > AS-Path

## **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

# Default:

empty
## **AS Path Regex**

Contains a regular expression that checks the AS\_PATH of the NLRI. Examples:

- .\*\_100: filters all NLRIs originating from "AS100".
- .\*\_(100|200): filters all NLRIs originating from "AS100" or "AS200".
- 100\_(.\*\_)?(500|400)\_.\*: filters all NLRIs from the BGP neighbor with the AS number "AS100", which were also previously routed via networks with the AS numbers "AS500" or "AS400" (or both).
- 100\_(500|400|123)\_.\*: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand directly from BGP neighbors with the AS numbers "AS500", "AS400" or "AS123".
- 100\_(100\_)\*(300\_)\*300: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which received this number beforehand from the BGP neighbor with the AS number "AS300". The expression also allows for AS prepend paths.
- 100\_ 200: filters all NLRIs from the BGP neighbor with the AS number "AS100" and which originated from the network with the AS number "AS200". The route taken by the NLRIs from "AS200" to "AS100" is unimportant.

Expressions must be constructed in PERL syntax.

## SNMP ID:

2.93.1.5.4.2.2

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > AS-Path

#### **Possible values:**

Max. 62 characters from [0-9]\$()\*+-.?[\]^\_{|}

#### Default:

empty

#### **Special values:**

empty

This list entry applies to all AS\_PATH attributes of the NLRI.

## **Regex-Match**

Determines how closely the regular expression under **AS-Path-Regex** needs to match the **AS\_PATH** attribute of the NLRI in order for the list entry to apply.

## SNMP ID:

2.93.1.5.4.2.3

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > AS-Path

#### **Possible values:**

Full

The regular expression fully describes the AS\_PATH attribute of the NLRI.

## Partial

The regular expression only describes parts of the AS\_PATH attribute.

#### Default:

Full

# Comment

Comment on this entry.

## SNMP ID:

2.93.1.5.4.2.4

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > AS-Path

## Possible values:

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

## Default:

empty

# Communities

This table contains community lists in order to identify NLRIs by their community attributes.

## SNMP ID:

2.93.1.5.4.3

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists

## Name

Contains the name of this community list.

## SNMP ID:

2.93.1.5.4.3.1

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Communities

#### **Possible values:**

```
Max. 16 characters from [A-Z][a-z][0-9]-_
```

Default:

empty

## Communities

Contains communities that the community attribute of the NLRI must match with.

Communities are specified by means of a comma-separated list (<AS-number1>: <Value1>, <AS-number2>: <Value2>, <AS-number3>: <Value3>).

## SNMP ID:

2.93.1.5.4.3.2

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Communities

#### **Possible values:**

```
Max. 62 characters from [A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`
```

## Default:

empty

# Comment

Comment on this entry.

#### SNMP ID:

2.93.1.5.4.3.3

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Lists > Communities

## Possible values:

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

## Default:

empty

## Matches

This table combines list entries from the directory **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** to find matches between multiple list entries and NLRI.

#### SNMP ID:

2.93.1.5.5

## Telnet path:

Setup > Routing-Protocols > BGP > Policy

## Name

Contains the name of this entry.

## SNMP ID:

2.93.1.5.5.1

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Matches

#### **Possible values:**

Max. 16 characters from [A-Z][a-z][0-9]-\_

## Default:

empty

## Prefix

Contains the corresponding entry from a prefix list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Prefixes**.

## SNMP ID:

2.93.1.5.5.2

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Matches

## Possible values:

Max. 16 characters from [A-Z][a-z][0-9]-\_

## Default:

empty

## **Special values:**

empty

Handles the NLRI as if there were a match with the prefix list.

# **AS-Path**

Contains the corresponding entry from an AS-path list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **AS-Paths**.

#### SNMP ID:

2.93.1.5.5.3

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Matches

## **Possible values:**

Max. 80 characters from  $[A-Z][a-z][0-9]-_$ ,

## Default:

empty

## **Special values:**

empty

Handles the NLRI as if there were a match with the AS-path list.

## Communities

Contains the corresponding entry from a communities list under **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Lists** > **Communities**.

## SNMP ID:

2.93.1.5.5.4

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Matches

## **Possible values:**

Max. 80 characters from  $[A-Z][a-z][0-9]-_$ ,

#### Default:

empty

## **Special values:**

empty

Handles the NLRI as if there were a match with the communities list.

## Comment

Comment on this entry.

#### SNMP ID:

2.93.1.5.5.5

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Matches

## **Possible values:**

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

#### Default:

empty

# **Filters**

This table contains filters that an NLRI to or from a BGP neighbor must pass through if the neighbor is configured with a corresponding policy.

For multiple filter entries with the same name, the device processes the filters according to the configured priority, until a filter matches the NLRI. The device then stops the filter pass.

#### SNMP ID:

2.93.1.5.6

## Telnet path:

Setup > Routing-Protocols > BGP > Policy

## Name

Contains the name of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value.

#### SNMP ID:

2.93.1.5.6.1

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

#### **Possible values:**

```
Max. 16 characters from [A-Z][a-z][0-9]-_
```

## Default:

empty

## Priority

Sets the priority of this entry.

Entries sharing the same name all belong to the same filter chain. The device processes the entries in this filter chain according to their priority value. A higher value means a higher priority.

#### SNMP ID:

2.93.1.5.6.2

```
Telnet path:
Setup > Routing-Protocols > BGP > Policy > Filters
Possible values:
Max. 5 characters from [0-9]
Default:
```

0

# **Address family**

Specifies the address family for which this filter applies.



If no option is selected, the entry is disabled.

## SNMP ID:

2.93.1.5.6.3

Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

**Possible values:** 

IPv4 IPv6

## Default:

IPv4

IPv6

## **Matches**

Specifies the name of an entry from the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Match**.

The device applies this filter if the NLRI matches the criteria.

() If this field indicates an invalid name, the device denies the NLRI and performs no further filters in the current filter chain.

## SNMP ID:

2.93.1.5.6.4

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

#### **Possible values:**

Max. 80 characters from [0-9][A-Z][a-z]-, !

#### Default:

empty

## Special values:

## empty

The device treats the NLRI as if it did match the criteria.

# Policy

Specifies whether the device should further process the filtered NLRI in the case that the filter is valid for the NLRI.

## SNMP ID:

2.93.1.5.6.5

#### Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

## Possible values:

Deny No further processing.

#### Permit

The device processes the NLRI further.

## Default:

Deny

# Action

Specifies which of the actions from the table **Setup** > **Routing-Protocols** > **BGP** > **Policy** > **Actions** is applied by the device to the NLRI.



If this field is empty or refers to an invalid name, the device performs no action.

## SNMP ID:

2.93.1.5.6.6

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

## Possible values:

Max. 16 characters from [A-Z][a-z][0-9]-\_

#### Default:

empty

## Comment

Comment on this entry.

#### SNMP ID:

2.93.1.5.6.7

## Telnet path:

Setup > Routing-Protocols > BGP > Policy > Filters

#### **Possible values:**

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

## Default:

empty

## Networks

Use this directory to configure the networks that the device shares with the BGP neighbors.

The distribution of these networks depends on the setting under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4/IPv6** > **Operating**.

## SNMP ID:

2.93.1.6

Telnet path: Setup > Routing-Protocols > BGP

## IPv4

Use this directory to configure the IPv4 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**.



The minimum specification for a valid new entry is one **IP address**.

## SNMP ID:

2.93.1.6.1

#### **Telnet path:**

Setup > Routing-Protocols > BGP > Networks

# **IP** address

Contains the IPv4 address or the prefix of the network.

#### SNMP ID:

2.93.1.6.1.1

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv4

## Possible values:

Max. 15 characters from [0-9].

## Default:

empty

# Netmask

Includes the IPv4 netmask of the network.

(f) The route is the default route for this address family if this entry contains the default setting 0.0.0.0.

## SNMP ID:

2.93.1.6.1.2

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv4

## Possible values:

Max. 15 characters from [0-9].

#### Default:

0.0.0.0

# **Rtg-Tag**

Contains the routing tag for this network.

The table under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4** uses this entry to filter the communication with BGP neighbors.

#### SNMP ID:

2.93.1.6.1.3

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv4

#### **Possible values:**

Max. 5 characters from [0-9]

#### Default:

0

## Туре

This item specifies whether the device advertises this network always or only when it appears in the active routing table.

#### SNMP ID:

2.93.1.6.1.4

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv4

#### **Possible values:**

Static

The network is always selected for advertisement.

#### Dynamic

The network is only selected for advertisement when it appears in the active routing table.

## Default:

Static

## Comment

Comment on this entry.

#### SNMP ID:

2.93.1.6.1.5

#### **Telnet path:**

Setup > Routing-Protocols > BGP > Networks > IPv4

## **Possible values:**

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

#### IPv6

Use this directory to configure the IPv6 networks that the device shares with the BGP neighbors.

Whether these networks are distributed depends upon the restrictions under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**.

The minimum specification for a valid new entry is one prefix.

#### SNMP ID:

2.93.1.6.2

## Telnet path:

Setup > Routing-Protocols > BGP > Networks

# Prefix

Contains the prefix (IPv6 address portion) of the network.

## SNMP ID:

2.93.1.6.2.1

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv6

## **Possible values:**

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

## Default:

empty

## **Prefix-Length**

Contains the prefix length of the IPv6 network.

(f) The route is the default route for this address family if this entry contains the default setting 0.

#### SNMP ID:

2.93.1.6.2.2

#### Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv6

# Possible values:

Max. 3 characters from [0-9]

#### Default:

0

# **Rtg-Tag**

Contains the routing tag for this network.

The table under **Setup** > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6** uses this entry to filter the communication with BGP neighbors.

## SNMP ID:

2.93.1.6.2.3

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv6

#### **Possible values:**

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

## Default:

0

# Туре

This item specifies whether the device always advertises this network, or only when the network appears in the active routing table.

## SNMP ID:

2.93.1.6.2.4

## Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv6

## Possible values:

Static

The device always uses this network in advertisements.

## Dynamic

The device only uses this network in advertisements when it appears in the active routing table.

## Default:

Static

## Comment

Comment on this entry.

## SNMP ID:

2.93.1.6.2.5

#### Telnet path:

Setup > Routing-Protocols > BGP > Networks > IPv6

#### **Possible values:**

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

## Operating

 $(\mathbf{i})$ 

Enables or disables BGP in the device.



#### SNMP ID:

2.93.1.7

# Telnet path:

Setup > Routing-Protocols > BGP

## Possible values:

Yes

BGP is enabled in the device.

No

BGP is disabled in the device.

## Default:

No

## Auto-Restart

Specifies whether a BGP neighbor automatically restarts after an error.

## SNMP ID:

2.93.1.8

## Telnet path:

Setup > Routing-Protocols > BGP

#### **Possible values:**

#### Yes

The automatic restart is enabled.

## No

The automatic restart is disabled.

## Default:

Yes

## Manual-Start

This action is used to start a BGP neighbor that was previously stopped by means of a manual stop.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from [A-Z][a-z][0-9]-).

If the arguments entered here match for several neighbors, the device establishes a connection to each one of them.

 $(\mathbf{i})$ 

The specified neighbors need to meet the following requirements:

• They must be fully configured for BGP.

For each one, the Connection mode setting under Setup > Routing-Protocols > BGP > Neighbors must not be set to "passive".

## SNMP ID:

2.93.1.9

## Telnet path:

Setup > Routing-Protocols > BGP

## Manual stop

With this action, you manually stop a BGP neighbor.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from [A-Z][a-z][0-9]-).

If the arguments entered here match for several neighbors, the device terminates all of these connections.

If multiple connections are opened to a neighbor, the device terminates all of these connections.

## SNMP ID:

2.93.1.10

Telnet path: Setup > Routing-Protocols > BGP

## Active start

Manually starts a BGP neighbor.

This function and its operating conditions are identical to Manual start, although in this case the device also connects to neighbors, for which the Connection mode under Setup > Routing-Protocols > BGP > Neighbors is set to "Passive".

## SNMP ID:

2.93.1.11

#### Telnet path:

Setup > Routing-Protocols > BGP

#### Reboot

With this action, you manually restart a BGP neighbor.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from [A-Z][a-z][0-9]-).

#### SNMP ID:

2.93.1.12

## Telnet path:

Setup > Routing-Protocols > BGP

#### Global-Read-Only-Timer

Time in seconds that the device remains in read-only mode after being started. As long as the device is in read-only mode, it receives routes from BGP neighbors but does not perform the "shortest-path algorithm" for route computation. This means that it does not send routes to BGP neighbors. This switch is used to optimize the performance of central-site devices where many routes are possible. This means that the device only performs a route computation once it has received all of the possible routes.

```
SNMP ID:
```

2.93.1.13

#### Telnet path:

Setup > Routing-Protocols > BGP

#### Possible values:

Max. 3 characters from [0-9]

#### Default:

0

#### Special values:

0

The timer is deactivated.

#### Peer-Read-Only-Timer

Time in seconds per individual neighbor that the device remains in read-only mode after being started. As long as the device is in read-only mode, it receives routes from this BGP neighbor but does not perform the "shortest-path algorithm" for route computation. This means that it does not send routes to this BGP neighbor. As soon as a BGP neighbor has sent its routes and issues an End-Of-RIB marker, the receiving device automatically exits the read-only mode and starts route computation. LANCOMRouters automatically send an End-Of-RIB marker after successfully transmitting its routes to a neighbor.

#### SNMP ID:

2.93.1.14

#### Telnet path:

Setup > Routing-Protocols > BGP

## Possible values:

Max. 3 characters from [0-9]

# Default: 0 Special values: 0 The timer is deactivated.

Send-Refresh-Request

This action sends a BGP-Route-Refresh message to a BGP neighbor. If this neighbor supports the Route-Refresh option, it sends its routes once again. The Route-Refresh option allows routes to be received from a neighbor again without having to restart the BGP connection.

The argument to be entered is the name of the neighbor indicated under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors** in the **Name** field (max 16 characters from [A-Z][a-z][0-9]-). Optionally specify the address family IPv4 or IPv6.

## SNMP ID:

2.93.1.15

#### Telnet path:

Setup > Routing-Protocols > BGP

# 5.1.8 Additions to the Status menu

## **Routing protocols**

This directory displays the statistics for BGP connections and the route monitor.

#### SNMP ID:

1.93

# Telnet path:

Status

# BGP

This directory displays the statistics for BGP connections.

#### SNMP ID:

1.93.1

## Telnet path:

Setup > Routing-Protocols

## Neighbors

This table contains the statistics for connections to the configured BGP neighbors.

The entries in the table are retained if you disable BGP.

## SNMP ID:

1.93.1.1

Telnet path:

Status > Routing-Protocols > BGP

# **IP** address

Contains the IPv4 or IPv6 address of the BGP neighbor.

The IP address is configured under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**.

## SNMP ID:

1.93.1.1.1

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

#### Port

Shows the port on which the BGP neighbor expects inbound BGP messages and, correspondingly, the port used by the device for outbound connections of the connection type "active" or "delayed".

The port is configured under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**.

## SNMP ID:

1.93.1.1.2

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Loopback address

Contains the sender address (IPv4 or IPv6) that the device uses when connecting to the BGP neighbor.

This loopback address is configured under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**.



If no loopback address is configured, this field contains the sender address.

#### SNMP ID:

1.93.1.1.3

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

# **Rtg-Tag**

Contains the routing tag. The device denies the connection if the routing tag does not match with the incoming connection. This routing tag is configured under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**.

#### SNMP ID:

1.93.1.1.4

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

# **Remote AS**

Contains the AS number of the BGP neighbor.

If the AS number of the BGP neighbor is identical to the AS number of the device's own BGP instance, then this neighbor is an iBGP peer (internal BGP) within the AS.

This remote AS is configured under **Setup** > **Routing-Protocols** > **BGP** > **Neighbors**.

#### SNMP ID:

1.93.1.1.5

#### Telnet path:

Status > Routing-Protocols > BGP > Neighbors

#### **Router ID**

Contains the router ID (IPv4 address) of this particular BGP neighbor. The BGP neighbor communicates its router ID in the OPEN message when connecting. If a BGP connection is to be operated via IPv6, it is essential that a unique 32-bit number is used as the router ID (e.g. a fictional IPv4 address). The router ID between BGP neighbors must be unique to each device.

## SNMP ID:

1.93.1.1.6

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## State

Contains the current state of the connection to the BGP neighbor.

#### SNMP ID:

1.93.1.1.7

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Possible values:**

#### Idle

In this state, no connections are established to the neighbors or accepted from them. No resources are made available to establish a connection.

## Connect

The device is connecting to the neighbor and is waiting for the completion of the TCP handshake.

## Active

The device accepts incoming connections from the neighbor.

## Open sent

The device sent an OPEN message to the neighbor and is waiting for its OPEN message.

#### Open confirmed

The device has accepted the OPEN message from the neighbor, has sent a keepalive message to the neighbor, and is waiting for its keepalive message.

## Established

The device and BGP neighbor are exchanging BGP messages.

#### Default:

Active

# **Previous state**

Contains the previous state of the connection to the BGP neighbor.

#### SNMP ID:

1.93.1.1.8

#### Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Possible values:**

#### Idle

In this state, no connections are established to the neighbors or accepted from them. No resources are made available to establish a connection.

#### Connect

The device is connecting to the neighbor and is waiting for the completion of the TCP handshake.

## Active

The device accepts incoming connections from the neighbor.

#### Open sent

The device sent an OPEN message to the neighbor and is waiting for its OPEN message.

## **Open confirmed**

The device has accepted the OPEN message from the neighbor, has sent a keepalive message to the neighbor, and is waiting for its keepalive message.

## Established

The device and BGP neighbor are exchanging BGP messages.

## Default:

Active

## Inbound updates

Contains the number of BGP UPDATE messages sent from this BGP neighbor.



Also counted are any invalid or empty BGP UPDATE messages.

## SNMP ID:

1.93.1.1.9

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Outbound updates

Contains the number of BGP-UPDATE messages sent to this BGP neighbor.

#### SNMP ID:

1.93.1.1.10

# Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Inbound messages

Contains the number of BGP messages sent from this BGP neighbor.



The display includes all types of BGP messages.

#### SNMP ID:

1.93.1.1.11

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Outbound messages**

Contains the number of BGP messages sent to this BGP neighbor.

## SNMP ID:

1.93.1.1.12

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Last error

Contains the last error message detected.

## SNMP ID:

1.93.1.1.13

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

# **Establish transitions**

This value indicates how often the device has established a connection to the BGP neighbors. Repeated attempts to establish the connection could be due to connect errors or the re-configuration of the BGP neighbor.

#### SNMP ID:

1.93.1.1.14

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Connection time**

Contains the time in seconds that the current connection exists to this BGP neighbor (state "connected").

(f) The display starts from "0" when the device establishes a new connection to the BGP neighbor.

#### SNMP ID:

1.93.1.1.15

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Keepalive

Contains the current value of the keepalive timer. If the device and the BGP neighbor have not yet negotiated this value (connection state "connected" not yet reached), this field contains the keepalive time configured for this BGP neighbor under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

If the device and the BGP neighbor negotiate the value "0", they do not exchange periodic keepalive messages.

#### SNMP ID:

1.93.1.1.16

#### Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Holdtime

Contains the current value of the hold-time timer. If the device and the BGP neighbor have not yet negotiated this value (connection state "connected" not yet reached), this field contains the hold-time configured for this BGP neighbor under **Setup** > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**.

With this value set to "0", the device assumes that the connection is in the "established" state even if it does not receive any messages.

(f) If the device receives no messages within the time specified here, it assumes that the connection has failed.

#### SNMP ID:

```
1.93.1.1.17
```

Telnet path:

**(i)** 

Status > Routing-Protocols > BGP > Neighbors

## Accepted prefixes

Contains the number of prefixes that the device has accepted from this BGP neighbor.

The displayed value is independent of the number of BGP-UPDATE messages from this BGP neighbor, as UPDATE messages can be sent with no prefixes or with several prefixes.

#### SNMP ID:

1.93.1.1.18

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Denied inbound prefixes**

Shows the number of prefixes from this BGP neighbor that were denied by the device. Prefixes are denied either by the local policy or if the prefix limit has been reached.

## SNMP ID:

1.93.1.1.19

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Inbound withdrawn prefixes

Contains the number of prefixes withdrawn by the BGP neighbor.

#### SNMP ID:

1.93.1.1.20

#### Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## **Advertised prefixes**

Contains the number of prefixes advertised by the device.



The displayed value is independent of the number of BGP-UPDATE messages, because an UPDATE message can advertise no prefixes or several prefixes.

## SNMP ID:

1.93.1.1.21

## Telnet path:

Status > Routing-Protocols > BGP > Neighbors

# **Denied outbound prefixes**

Contains the number of outbound prefixes denied by the device for this BGP neighbor.

The displayed value depends solely upon the policy applied to outbound BGP messages.

# SNMP ID:

 $\bigcirc$ 

1.93.1.1.22

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

## Outgoing withdrawn prefixes

Contains the number of outbound prefixes withdrawn by the device for this BGP neighbor.

#### SNMP ID:

1.93.1.1.23

Telnet path:

Status > Routing-Protocols > BGP > Neighbors

# 5.2 Route monitor

As of LCOS version 9.20, a route monitor checks the network connections to a specified prefix. This prefix is learned, for example as the result of a dynamic routing protocol such as BGP.

In case of a faulty connection, the route monitor opens a backup connection, if required.

# 5.2.1 Route monitor

The route monitor observes the connections to the networks of different providers and establishes a backup connection in case of failure. The monitoring makes use of a trigger prefix, which providers supply in their routing protocol, for example with the Border Gateway Protocol (BGP). As soon as a route to a provider's network becomes unavailable, the route monitor declares the relevant trigger prefix to be invalid for its network and opens a backup connection to the provider's network.

# Configuring the route monitor with LANconfig

To activate the route monitor, switch to the view **Communication** > **Call management** and check the option **Route monitor active**.

To configure the route monitor, open the **Route monitor table**.

Route Monitor Table - New	w Entry	? <b>×</b>
Active		
Remote site:	•	Select
Prefix:		
Routing tag:	0	
Up delay:	20	seconds
Down delay:	0	seconds
Comment:		
	OK	Cancel

#### Operating

Specifies whether this backup connection is enabled.

#### **Remote site**

Contains the name of the backup remote station.

## Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

## **Routing tag**

Contains the routing tag of the prefix being monitored.

## Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

## Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

The value "0" causes the device to disconnect from the backup peer immediately after the prefix arrives (no delay).

## Comment

Comment on this entry.

# 5.2.2 Additions to the Setup menu

# **Route monitor**

In this directory, you configure the route monitor.

#### SNMP ID:

2.93.2

## Telnet path:

Setup > Routing-protocols

#### Monitor table

In this table, you configure the route monitor.

## SNMP ID:

2.93.2.1

## Telnet path:

Setup > Routing-protocols > Route-monitor

## Backup peer

Contains the name of the backup remote station.

#### SNMP ID:

2.93.2.1.1

Telnet path:

## Setup > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

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

## Default:

empty

## Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

## SNMP ID:

2.93.2.1.2

## Telnet path:

Setup > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

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

## Default:

empty

## Rtg-Tag

Contains the routing tag of the prefix being monitored.

#### SNMP ID:

2.93.2.1.3

## Telnet path:

#### Setup > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

Max. 5 characters from [0-9]

## Default:

0

## Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

#### SNMP ID:

2.93.2.1.4

## Telnet path:

Setup > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

20

## Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

## SNMP ID:

2.93.2.1.5

## **Telnet path:**

Setup > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

Max. 10 characters from [0-9]

## Default:

0

## **Special values:**

0

No delay: The device immediately closes the connection to the backup peer when the prefix arrives.

## Operating

Specifies whether this backup connection is enabled.

## SNMP ID:

2.93.2.1.6

## Telnet path:

Setup > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

Yes

The backup connection is enabled.

## No

The backup connection is disabled.

## Default:

No

## Comment

Comment on this entry.

#### SNMP ID:

2.93.2.1.7

## Telnet path:

Setup > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

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

## Default:

empty

## Operating

This action is used to enable or disable the route monitor.

## SNMP ID:

2.93.2.2

#### Telnet path:

Setup > Routing-protocols > Route-monitor

**Possible values:** 

No

The route monitor is disabled.

Yes

The route monitor is enabled.

## Default:

No

# 5.2.3 Additions to the Status menu

## **Route monitor**

This directory shows the route monitor statistics.

## SNMP ID:

1.93.2

# Telnet path: Setup > Routing-Protocols

## Monitor table

This table shows the route monitor statistics.

## SNMP ID:

1.93.2.1

## Telnet path:

Status > Routing-protocols > Route-monitor

## Backup peer

Contains the name of the backup remote station.

## SNMP ID:

1.93.2.1.1

## Telnet path:

Status > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

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

#### Prefix

Contains the prefix (IPv4 or IPv6 address) of the backup peer.

## SNMP ID:

1.93.2.1.2

## Telnet path:

Status > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

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

# Rtg-Tag

Contains the routing tag for the backup connection.

#### SNMP ID:

1.93.2.1.3

## **Telnet path:**

Status > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

Max. 5 characters from [0-9]

## Default:

0

## **Prefix state**

Contains the prefix state of the backup connection.

## SNMP ID:

1.93.2.1.4

## **Telnet path:**

Status > Routing-protocols > Route-monitor > Monitor-table

# Possible values:

Available

The prefix of this backup connection is stored in the routing table.

## Unavailable

The prefix of this backup connection is not stored in the routing table.

#### Unknown

The prefix of this backup connection is unknown.

## **Backup-Status**

Contains the status of the backup connection.

## SNMP ID:

1.93.2.1.5

## Telnet path:

Status > Routing-protocols > Route-monitor > Monitor-table

#### **Possible values:**

## Unknown

The backup status is unknown.

## Down

There is no backup connection.

## Up

There is a backup connection.

## Wait down

The device terminates the backup connection after the specified delay.

#### Wait up

The device starts the backup connection after the specified delay.

## Peer state

Contains the status of the backup peer.

## SNMP ID:

1.93.2.1.6

## Telnet path:

Status > Routing-protocols > Route-monitor > Monitor-table

## **Possible values:**

#### Connected

The peer is configured correctly, the backup connection is established.

## Disconnected/unknown

Either the peer is not configured correctly, or the backup connection has not been established.

# 5.3 DiffServ field enabled by default

As of LCOS version 9.20, the routing method observes the DiffServ field in IP packets by default.

- Pouting options		
Housing options		
Use Proxy ARP to tie remote stations into the LAN		
Send ICMP redirects		
Transfer ICMP packets secured		
Pass on TCP SYN and ACK packets preferentially		
Transfer packets from internal services via the router		
Consider the Type-Of-Service field in IP packets		
Consider the DiffServ field in IP packets		
Copy DiffServ tags from Layer-3 to Layer-2		
DiffServ tags from Layer-2:		

## Consider the DiffServ field in IP packets

If the router considers the DiffServ field in IP packets, it applies preferential transmission according to the standardized DSCP (DiffServ code point) AFxx (Assured Forwarding) for secured transmission and EF (Expedited Forwarding). All other IP packets will be transmitted normally. This option is enabled by default.

This option cannot be used in combination with ToS since the DiffServ field replaces the ToS field within the IP packet.

For more information about DiffServ, see the chapter Quality-of-Service.

# 5.3.1 Additions to the Setup menu

# **Routing method**

Controls the analysis of ToS or DiffServ fields.

#### SNMP ID:

2.8.7.1

#### Telnet path:

Setup > IP-Router > Routing-Method

## Possible values:

#### Normal

The TOS/DiffServ field is ignored.

## Type of service

The TOS/DiffServ field is regarded as a TOS field; the bits "low delay" and "high reliability" will be evaluated.

## DiffServ

The TOS/DiffServ field is regarded as a DiffServ field and evaluated as follows.

- CSx (including CS0 = BE): Normal transmission
- AFxx: Secure transmission
- **EF:** Preferred transmission

## Default:

DiffServ

# 5.4 iPerf-compliant server/client

As of LCOS version 9.20, LCOS features the tool "iPerf" for performance measurements over network routes. It performs bandwidth measurements either one-way or two-way. Iperf can be started directly from any LANCOM device. The LANCOM device is able to act as a client and as a server (UDP/TCP). The LCOS implementation is based on iPerf2.

iPerf can be configured either via LANconfig or via the command-line console.

# 5.4.1 Bandwidth measurements with iPerf

Measurements of network performance determine values such as the throughput, latency, jitter and error rates over a network connection. The measured values are used, among other things, for network optimization, error detection and troubleshooting, and for assessing the performance of network infrastructures.

iPerf has become established as a free program for generating and evaluating data streams over data connections. An iPerf server daemon receives TCP and UDP streams and measures the throughput for the corresponding applications along with the latency, jitter, packet loss and packet reordering over UDP connections.

To conduct a bandwidth measurement between two hosts, you start the iPerf server on one device and the iPerf client on the other one. The iPerf client then connects to the iPerf server. The server and client exchange data packets for a certain time or a certain amount of data and generate statistics about this. These statistics provide information about the quality of the connection between the two devices.

When measuring the quality of the TCP connection, the iPerf client transmits completely filled TCP data packets at the fastest speed possible. The average data rate of successful data transfer ("goodput") is the result of what the iPerf server received correctly.

When measuring UDP connection quality, the iPerf client transmits data over a specified bandwidth (1 Mbps by default), although this is without flow or performance control. The "goodput" relates to the maximum bandwidth with which the client's transmission buffer remains permanently filled without data packets being lost.

LANCOM devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

**()** 

Measurements can be carried out between two LANCOM devices or between a LANCOM device and another iPerf2 instance.

# 5.4.2 Setting up iPerf with LANconfig

In LANconfig, you configure iPerf under Log & Trace > General and clicking on iPerf settings.

iP	erf settings		? 💌
	iPerf settings		
	iPerf server daemon active		
	Transport protocols:	TCP+UDP 🔻	
	Port:	5.001	
	Testing on WAN:	denied 💌	
	Here you configure the networks from which an iPerf test may be initiated.		
		Access stations	
		OK	Cancel

## iPerf server daemon active

Activates or deactivates the iPerf server daemon.

Rather than setting up the iPerf server to run permanently at this point, you can optionally start a one-off test by accessing the command-line console via SSH and starting a temporary iPerf server.

## **Transport protocols**

Here you set which transport protocols are to be measured for bandwidth.

#### Port

This port is used for communications between the iPerf client and server ("5001" by default).

#### **Testing on WAN**

Here you determine whether measurements are also permitted over a WAN connection.



Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

## Access stations

In order restrict iPerf access to certain stations only, enter the connection data into this table.

Access stations - New Entry		? 🗙
IP address:	0.0.0.0	
Netmask:	255.255.255.255	
Routing tag:	0	
Comment:		
	OK	Cancel

#### **IP** address

Enter the IPv4 address of the remote station.

#### Netmask

Enter the netmask of the remote station.

## **Routing tag**

Enter the routing tag that specifies the connection to the remote station.

#### Comment

Enter a descriptive comment for this entry.

# 5.4.3 Temporary iPerf server and client

If you configure iPerf with LANconfig, the iPerf function remains permanently active. You can optionally start a temporary iPerf daemon, which remains active for just one test, by using SSH to connect to the command-line console.

To do this, start a terminal program (e.g. PuTTY) and open a connection to the device where you want to perform the iPerf test. Use the console command *iperf* and the appropriate option switches to start the temporary iPerf daemon. The following examples illustrate some standard commands.

() More information about the option switches for iperf is available in the section *Commands for the console*.

#### Running the iPerf server in TCP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s
[Iperf-TCP-Server|1526] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

## Running the iPerf server in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s -u
[Iperf-UDP-Server|1524] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

#### Running the iPerf client in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -u -c 172.16.30.23
WARN: Using default UPD bandwidth limitation of 1 MBit/s
WARN: Using default UDP payload length of 1472 bytes (for matching Ethernet MTU
via IPv4)
[Iperf-UDP-Client|2100] Connecting to server...
[Iperf-UDP-Client|2100] Connection established to 172.16.30.23:5001
root@device:/
```

Press the Enter key to exit the test.

```
[Iperf-UDP-Client|2100] Connection closed actively
[Iperf-UDP-Client|2100] Sent 1249728 bytes within 10s (10000ms) -> 0 Mbit/s (999
Kbit/s)
[Iperf-UDP-Client|2100] Server reports 1249728 bytes received within 9s (9985ms)
-> 1 Mbit/s (1001 Kbit/s)
[Iperf-UDP-Client|2100] Server received 849 packets (0 lost / 0 out-of-order) with
62us jitter
root@device:/
>
```

# 5.4.4 Analyzing iPerf results with LANmonitor

LANCOM devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.
(i) For more information on iPerf, see the section *Bandwidth measurements with iPerf*.

The last iPerf test result can also be viewed in LANmonitor under "iPerf". In this case it is unimportant whether the device initiated a connection or was contacted externally. The connection type "Test mode" displays the mode accordingly:

E LANmonitor	
<u>F</u> ile <u>D</u> evice <u>V</u> iew <u>T</u> ools <u>H</u> elp	
🗣 🔍 🙀 💷 🗉 🔯 🖼 🗊 🛙 🗐 🖉 🔎	
Steff-1780EW-4G	
▶ 🖷 WAN connections: 1	
VPN: 5 connected	
EoGRE tunnel	
▷ · ·)) Wireless LAN	
Public spot	
Border Gateway Protocol	
Rapid Spanning Tree	
Certificates	
P are IPv6 firewall: 03/07/2016 14:01:16 intruder detection - Packet	dropped
P IPv4 firewall: 03/03/2016 10:37:51 intruder detection - Packet	dropped
b dia SLA monitoring	
⊿ 💌 iPerf	
▲ ↓ Last test result (TCP)	
Local IP: 172.16.30.1	
Test mode: Unidirectional server daemon	
▲ U Server report	
Start of test: 07.03.2016 13:54:03	
End of test: 07.03.2016 13:54:13	
T for the second	
Transferred data: 28960Kbytes	
Measured bandwidth: 23062Mbit/s	
Start of test: 07.05.2010 13:34:05	
Test duration: 10000mm	
Transforred data 50007/bittor	
Massured bandwidth: 40646Mbit/s	
Budget	
System information	
GPS: Disabled	
Monitoring: SNMPv3 (encrypted)	
- montering on an is (encrypted)	

LANmonitor displays the test results stored in the device under **Status** > **Iperf** > **Last results**.

# 5.4.5 iPerf commands on the command line

Table 2: Overview of iPerf options

Command	Description				
iperf [-s -c <host>] [-u] [-p <port>] [-B</port></host>	arts iPerf on the device in order to perform a bandwidth measurement with an erf2 remote station. Possible arguments are:				
<interface>] [-c] [-b</interface>	Client/server				
[ <bandw>/]<bandw>[KKmM]] [-1 <length>] [-t <time>]</time></length></bandw></bandw>	-u,udp: Uses UDP instead of TCP.				
[-d] [-r] [-L <port>] [-h]</port>	<ul> <li>-p,port <port>: Connects with or expects data packets on this port (default: 5001).</port></li> </ul>				
	<ul> <li>-B,bind <interface>: Permits the connection only via the specified interface (IP address or interface name).</interface></li> </ul>				
	Server specific				
	<ul> <li>-s,server: Starts iPerf in server mode and waits for an iPerf client to contact it.</li> </ul>				

Command	Description
	Client specific
	<ul> <li>-c,client <host>: Starts iPerf in client mode and connects with the iPerf server <host> (IP address or DNS name).</host></host></li> <li>-b,bandwidth [<bandw>/]<bandw>{kKmM}: Limit the [down]/up-stream bandwidth when analyzing a UDP connection. This Is specified as kilobytes (kK) or megabytes (mM) per second (default: 1 Mbps).</bandw></bandw></li> </ul>
	I,len <length>: Sets the length of the UDP data packets.</length>
	<ul> <li>-t,time <time>: Sets the duration of the connection in seconds (default: 10 seconds).</time></li> </ul>
	<ul> <li>-d,dualtest: The test is bidirectional: the iPerf server and client send and receive at the same time.</li> </ul>
	-r,tradeoff: The test is sequential: the iPerf server and client send and receive one after the other.
	<ul> <li>-L,listenport <port>: Specifies the port where the device in bidirectional mode expects to receive data packets from the remote iPerf server (default: 5001).</port></li> </ul>
	<ul> <li>Miscellaneous</li> </ul>
	-h,help: Outputs the help text.

# 5.4.6 Additions to the Setup menu

# Iperf

iPerf measures the throughput for TCP and UDP applications, as well as latency, jitter, packet loss or packet reordering for UDP connections.

Use this menu to configure the iPerf settings.

### SNMP ID:

2.96

# Telnet path:

Setup

# Server daemon

This menu contains the configuration for the iPerf server daemon.

### SNMP ID:

2.96.1

# Telnet path:

Setup > Iperf

### Operating

This entry is used to enable or disable the iPerf server daemon.

# SNMP ID:

2.96.1.1

### Telnet path:

Setup > Iperf > Server-Daemon

### **Possible values:**

No

The iPerf server daemon is not active.

# Yes

The iPerf server daemon is active.

# Default:

No

# Transport

Use this entry to set the transfer protocol used by the iPerf server daemon.

### SNMP ID:

2.96.1.2

Telnet path:

Setup > Iperf > Server-Daemon

Possible values:

UDP TCP

### Default:

UDP

# Port

Here you specify a port on which the iPerf server expects packets to arrive.

# SNMP ID:

2.96.1.3

Addendum

5 Routing and WAN connections

### Telnet path:

Setup > Iperf > Server-Daemon

## **Possible values:**

Max. 5 characters from [0-9]

# Default:

5001

### **IPv4-WAN-Access**

Here you determine whether measurements are also permitted over a WAN connection.

 $(\mathbf{i})$ 

Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

#### **SNMP ID:**

2.96.2

### Telnet path:

Setup > Iperf

# **Possible values:**

#### No

Bandwidth measurements are not permitted over a WAN connection.

#### VPN

The bandwidth measurements are permitted over a WAN connection, but only if it is protected by a VPN tunnel.

### Yes

Bandwidth measurements are also permitted over a WAN connection.

#### Default:

No

### IPv4-Access-List

In order restrict iPerf access to certain stations only, enter the connection data into this table.

#### **SNMP ID:**

2.96.3

Telnet path:

Setup > Iperf

#### **IP** address

Enter the IPv4 address of the remote station.

### SNMP ID:

2.96.3.1

### Telnet path:

Setup > Iperf > IPv4-Access-List

### **Possible values:**

Max. 15 characters from [0-9].

### Default:

empty

# Netmask

Enter the netmask of the remote station.

### SNMP ID:

2.96.3.2

# Telnet path:

Setup > Iperf > IPv4-Access-List

### **Possible values:**

Max. 15 characters from [0-9].

### Default:

255,255,255,255

# **Rtg-Tag**

Enter the routing tag that specifies the connection to the remote station.

# SNMP ID:

2.96.3.3

### Telnet path:

Setup > Iperf > IPv4-Access-List

#### **Possible values:**

Max. 5 characters from [0-9]

### Default:

0

#### Comment

Enter a descriptive comment for this entry.

#### SNMP ID:

2.96.3.4

Telnet path:

Setup > Iperf > IPv4-Access-List

### Possible values:

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

#### Default:

empty

# 5.4.7 Additions to the Status menu

### Iperf

Measurements of network performance determine values such as the throughput, latency, jitter and error rates over a network connection. The measured values are used, among other things, for network optimization, error detection and troubleshooting, and for assessing the performance of network infrastructures. Measurements can be performed automatically, periodically or manually on demand.

Iperf has become established as free software for generating and evaluating data streams over data connections. Iperf measures the throughput for TCP and UDP applications, as well as latency, jitter, packet loss and packet reordering for UDP connections.

LANCOM-devices include an iPerf-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

This directory contains an overview of WAN bandwidth measurements.

#### SNMP ID:

1.96

Telnet path:

Status

### Last-Results

This menu contains the tables with the results of WAN bandwidth measurements for TCP and UDP.

### SNMP ID:

1.96.1

# Telnet path:

Status > Iperf

#### UDP

This menu contains the table with the results of WAN bandwidth measurements for UDP.

In order to analyze the measurements on the client side as well, the iPerf server sends the data back to the iPerf client. These data appear in separate columns of the table.

# SNMP ID:

1.96.1.1

Telnet path: Status > Iperf > Last-Results

# Index

This column contains the sequential number of each entry.

#### SNMP ID:

1.96.1.1.1

### Telnet path:

Status > Iperf > Last-Results > UDP

## Local-IP

This column contains the local IP of the measured interface.

### SNMP ID:

1.96.1.1.2

### Telnet path:

Status > Iperf > Last-Results > UDP

# **Remote-IP**

This column contains the remote IP of the measured interface.

### SNMP ID:

1.96.1.1.3

### Telnet path:

Status > Iperf > Last-Results > UDP

# Mode

This column contains the mode of the measured interface.

### SNMP ID:

1.96.1.1.4

### Telnet path:

Status > Iperf > Last-Results > UDP

# Connections

This column contains the current connections at the measured interface.

#### SNMP ID:

1.96.1.1.5

### Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Start

This column contains the time when the iPerf server started.

### SNMP ID:

1.96.1.1.6

# Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Stop

This column contains the time when the iPerf server stopped.

### SNMP ID:

1.96.1.1.7

### Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Duration-ms

This column contains the transmission time of data packets from the server to the client in milliseconds.

#### SNMP ID:

1.96.1.1.8

# Telnet path:

Status > Iperf > Last-Results > UDP

### Server-Bytes

This column contains the number of bytes that the server transmitted during the connection.

### SNMP ID:

1.96.1.1.9

# Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Bandwidth-kbps

This column contains the server bandwidth during the connection.

# SNMP ID:

1.96.1.1.10

#### Telnet path:

Status > Iperf > Last-Results > UDP

# **Server-Packets**

This column contains the number of data packets that the server transmitted during the connection.

#### SNMP ID:

1.96.1.1.11

#### Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Lost-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

This column contains the difference between the number of data packets that the server sent and the number the client reported as received.

#### SNMP ID:

1.96.1.1.12

# Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Out-Of-Order-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

This column contains the number of data packets that the server sent and that were reported by the client as being received in a different order.

#### SNMP ID:

1.96.1.1.13

### Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Jitter-us

The client inserts a timestamp into the header of every packet it sends, so enabling the server to measure the latency of this data transfer.

This column contains the latency of the data packets in microseconds.

#### **SNMP ID:**

1.96.1.1.14

### Telnet path:

Status > Iperf > Last-Results > UDP

# Server-Error

Should an error occur, this column contains the error reported by the server during the connection.

#### SNMP ID:

1.96.1.1.15

### Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Start**

This column contains the time when the iPerf client started.

#### SNMP ID:

1.96.1.1.16

Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Stop**

This column contains the time when the iPerf client stopped.

#### SNMP ID:

1.96.1.1.17

# Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Duration-ms**

This column contains the transmission time of data packets from the client to the server in milliseconds.

### SNMP ID:

1.96.1.1.18

### Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Bytes**

This column contains the quantity of data packets in bytes that the client received during the connection.

### SNMP ID:

```
1.96.1.1.19
```

### Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Bandwidth-kbps**

This column contains the client bandwidth during the connection.

#### SNMP ID:

1.96.1.1.20

# Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Packets**

This column contains the quantity of data packets that the client received during the connection.

### SNMP ID:

1.96.1.1.21

# Telnet path:

Status > Iperf > Last-Results > UDP

# **Client-Error**

Should an error occur, this column contains the error reported by the client during the connection.

### SNMP ID:

1.96.1.1.22

#### Telnet path:

Status > Iperf > Last-Results > UDP

# **Remote-Server-Duration-ms**

This column contains the transmission time of data packets in milliseconds that the server reported back to the client.

This value appears only when the device is in the iPerf-client mode.

### SNMP ID:

1.96.1.1.23

Telnet path:

Status > Iperf > Last-Results > UDP

# **Remote-Server-Bytes**

This column contains the number of bytes that the server reported to the client.

(i) This value appears only when the device is in the iPerf-client mode.

#### SNMP ID:

1.96.1.1.24

Telnet path:

Status > Iperf > Last-Results > UDP

### Remote-Server-Bandwidth-kbps

This column contains the server bandwidth during the connection that the server reported back to the client.

(f) This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.25

Telnet path:

Status > Iperf > Last-Results > UDP

# **Remote-Server-Packets**

This column contains the number of data packets that the server reports to the client as being sent.



This value appears only when the device is in the iPerf-client mode.

### SNMP ID:

1.96.1.1.26

Telnet path:

Status > Iperf > Last-Results > UDP

# **Remote-Server-Lost-Packets**

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

The server uses this to find the difference between the number of data packets that it sent and the number the client reports as received.

This column contains the value that the server reports to the client.

(1) This value appears only when the device is in the iPerf-client mode.

#### SNMP ID:

1.96.1.1.27

Telnet path:

Status > Iperf > Last-Results > UDP

# Remote-Server-Out-Of-Order-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

The server uses this to calculate the number of data packets that the it sent and that were reported by the client as being received in a different order.

This column contains the value that the server reports to the client.

This value appears only when the device is in the iPerf-client mode.

### SNMP ID:

1.96.1.1.28

#### Telnet path:

Status > Iperf > Last-Results > UDP

### **Remote-Server-Jitter-us**

The client inserts a timestamp into the header of every packet it sends, so enabling the server to measure the latency of this data transfer.

The server uses this to calculate the latency of the data packets in microseconds.

This column contains the value that the server reports to the client.

This value appears only when the device is in the iPerf-client mode.

#### SNMP ID:

1.96.1.1.29

#### Telnet path:

Status > Iperf > Last-Results > UDP

# тср

This menu contains the table with the results of WAN bandwidth measurements for TCP.

#### SNMP ID:

1.96.1.2

# Telnet path:

Status > Iperf > Last-Results

# Index

This column contains the sequential number of each entry.

#### SNMP ID:

1.96.1.2.1

# Telnet path:

Status > Iperf > Last-Results > TCP

# Local-IP

This column contains the local IP of the measured interface.

### SNMP ID:

1.96.1.2.2

# Telnet path:

Status > Iperf > Last-Results > TCP

# **Remote-IP**

This column contains the remote IP of the measured interface.

### SNMP ID:

1.96.1.2.3

# Telnet path:

Status > Iperf > Last-Results > TCP

# Mode

This column contains the mode of the measured interface.

### SNMP ID:

```
1.96.1.2.4
```

### Telnet path:

Status > Iperf > Last-Results > TCP

# Connections

This column contains the current connections at the measured interface.

#### SNMP ID:

1.96.1.2.5

# Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Start

This column contains the time when the iPerf server started.

# SNMP ID:

1.96.1.2.6

# Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Stop

This column contains the time when the iPerf server stopped.

# SNMP ID:

1.96.1.2.7

### Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Duration-ms

This column contains the transmission time of data packets from the server to the client in milliseconds.

### SNMP ID:

1.96.1.2.8

### Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Bytes

This column contains the number of bytes that the server transmitted during the connection.

### SNMP ID:

1.96.1.2.9

Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Bandwidth-kbps

This column contains the server bandwidth during the connection.

SNMP ID:

1.96.1.2.10

Telnet path:

Status > Iperf > Last-Results > TCP

# Server-Error

Should an error occur, this column contains the error reported by the server during the connection.

### SNMP ID:

1.96.1.2.11

# Telnet path:

Status > Iperf > Last-Results > TCP

# **Client-Start**

This column contains the time when the iPerf client started.

#### SNMP ID:

1.96.1.2.12

# Telnet path:

Status > Iperf > Last-Results > TCP

# **Client-Stop**

This column contains the time when the iPerf client stopped.

# SNMP ID:

1.96.1.2.13

# Telnet path: Status > Iperf > Last-Results > TCP

# **Client-Duration-ms**

This column contains the transmission time of data packets from the client to the server in milliseconds.

#### SNMP ID:

1.96.1.2.14

Telnet path:

Status > Iperf > Last-Results > TCP

# **Client-Bytes**

This column contains the quantity of data packets in bytes that the client received during the connection.

#### SNMP ID:

1.96.1.2.15

### Telnet path:

Status > Iperf > Last-Results > TCP

# **Client-Bandwidth-kbps**

This column contains the client bandwidth during the connection.

### SNMP ID:

1.96.1.2.16

# Telnet path:

Status > Iperf > Last-Results > TCP

### **Client-Error**

Should an error occur, this column contains the error reported by the client during the connection.

#### SNMP ID:

1.96.1.2.17

### Telnet path:

Status > Iperf > Last-Results > TCP

# 5.5 SLA monitor

As of LCOS version 9.20, an SLA monitor checks the network connections and the available services. The device performs this by sending data packets over the Internet Control Message Protocol (ICMP) and using ping commands, among other things, to query the accessibility of remote stations.

Information about packet transmission times and the number of lost packets can be inspected via SYSLOG or LANmonitor.

# 5.5.1 SLA monitoring

SLA monitoring is used to monitor the connections to remote stations within a network infrastructure. Ping tests to specified targets provide information about peer availability, packet transmission times and the number of lost packets. You can optionally define alerts that are issued when certain threshold values are exceeded, and to output these with SYSLOG or LANmonitor. The history of past checks is also stored, so helping administrators to stay up to date about the quality of the connections.

A corresponding SYSLOG client or daemon is required to receive the SYSLOG messages. Logging under UNIX/Linux is generally performed by the SYSLOG daemon that is set up as standard in these operating systems. The daemon either establishes contact with the console or writes its log to an appropriate SYSLOG file.

Under Linux, the file /etc/syslog.conf contains a definition of which facilities should be written to which log file. Please check your daemon's configuration to see if it explicitly listens to network connections.

Windows does not provide a corresponding system function. You require special software to provide the functionality of a SYSLOG daemon.

# 5.5.2 Configuring SLA monitoring with LANconfig

For configuration with LANconfig, the SLA monitor is located under **Log & Trace** > **General** on the **SLA monitoring** pane.

SLA monitoring		
Through SLA monitoring you can to device.	est the accessibility of remote sit	es and services from this
	ICMP tests	

Click the button ICMP tests, add new queries and set guideline values for the connection tests.

IC	CMP tests													
	Test active	Name	IP version	Destination	Tag	Source address (optional)	Interval	Offset	Count	Delay	Size	RTT max. w.	RTT max. C.	RTT avg. w
	On	CENTRAL	Auto	132.168.1.120	0		30 seconds	0 seconds	5	1.000 milliseconds	56 byte	100 milliseconds	200 milliseconds	80 millisecor
	•													
	R QuickFir	nder										Add	Edit	Copy

Click the Add button, or select an existing entry and click Edit.

ICMP tests - New Entry					? <mark>×</mark>
V Test active			Result evaluation		
Name:	CENTRAL	]	RTT max. warning:	100	milliseconds
IP version:	Auto -		RTT max. Critical:	200	milliseconds
Destination:	192.168.1.120	]	RTT avg. warning:	80	milliseconds
Routing tag:	0	]	RTT avg. Critical:	170	milliseconds
Source address (optional):		Select	Packet loss warning:	10	percent
Test interval:	30	seconds	Packet loss critical:	20	percent
Start offset:	0	seconds		_	
Count per test:	5	]	Comment:		
Packet delay:	1.000	milliseconds			
Packet size:	56	byte			
			,		
					OK Cancel

#### Test active

With this check box enabled, the device uses the specified settings for the connectivity test.

#### Name

Name of connection

# **IP** version

Specifies the use of IPv4 or IPv6.

The setting "Auto" is selected by default.

### Destination

Specifies the destination for testing (ICMP/PING destination).

# **Routing tag**

Specify a routing tag if a particular route is to be used.

# Source address (optional)

You can optionally configure a source address if you want to use a specific network as the source interface.

### Test Interval:

Specifies the time interval in which the device sends ICMP packets (default: 30 seconds).

### Start offset

Set a delay time before ICMP packets are sent.

# Count per test

Specifies how many ICMP packets are sent per test (default: 5).

# Packet delay

Set a delay before packets are sent.

### Packet size

Sets the packet size for the ICMP message.

### **Result evaluation**

In this section, you specify the threshold limits for packet handling.

#### RTT max. warning

Specify a maximum packet transmission time (**R**ound **T**rip **T**ime). A warning message is generated if an ICMP packet takes longer than the transmission time specified here.

#### RTT max. critical

An error message is generated if an ICMP packet takes longer than the transmission time specified here.

#### RTT avg. warning

Specify an average packet transmission time here. A warning message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

#### RTT avg. critical

Specify an average packet transmission time here. An error message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

#### Packet loss warning

A warning message is generated if the percentage of lost packets reaches the value specified here.

### Packet loss critical

An error message is generated if the percentage of lost packets reaches the value specified here.

### Comment

Enter a descriptive comment for this entry.

# 5.5.3 Displaying the SLA monitoring results in LANmonitor

LANmonitor displays the configured tests under SLA monitoring.

It shows the results of the most recently collected information from the connection test.



You also have the option to display the history of the connection tests. Click with the right mouse button on the entry **SLA monitoring**. In the following dialog, select **SLA monitoring history**.

ring testresults of Steff	-1780EW-4G		-		- A Lotte Land			
ng <u>V</u> iew								
Timestamp	Name	Destination	Packetloss	Minimal round trip time	Maximum round trip time	Average round trip time	Warning due to	Critical due to
03/07/2016 15:33:07	ZENTRALE	172.16.10.1	0	224.869000	256.337000	238.560000	Maximum round	Maximum rou
03/07/2016 15:33:37	ZENTRALE	172.16.10.1	0	224.867000	272.290000	238.726000	Maximum round	Maximum rou
03/07/2016 15:34:07	ZENTRALE	172.16.10.1	0	225,852000	289.624000	254.387000	Maximum round	Maximum rou
03/07/2016 15:34:37	ZENTRALE	172.16.10.1	0	225.658000	294.184000	245.789000	Maximum round	Maximum rou
03/07/2016 15:35:07	ZENTRALE	172.16.10.1	0	225.040000	280.097000	246.493000	Maximum round	Maximum rou
03/07/2016 15:35:37	ZENTRALE	172.16.10.1	0	225.196000	361.272000	259.568000	Maximum round	Maximum rou
03/07/2016 15:36:07	ZENTRALE	172.16.10.1	0	226.290000	295.104000	248.344000	Maximum round	Maximum rou
03/07/2016 15:36:37	ZENTRALE	172.16.10.1	0	224.919000	377.248000	271.943000	Maximum round	Maximum rou
03/07/2016 15:37:07	ZENTRALE	172.16.10.1	0	225.174000	285.583000	243.667000	Maximum round	Maximum rou
03/07/2016 15:37:37	ZENTRALE	172.16.10.1	0	224.845000	237.954000	228.928000	Maximum round	Maximum rou
03/07/2016 15:38:07	ZENTRALE	172.16.10.1	0	224.027000	232.320000	226.219000	Maximum round	Maximum rou
03/07/2016 15:38:37	ZENTRALE	172.16.10.1	0	224.437000	283.768000	242.988000	Maximum round	Maximum rou
03/07/2016 15:39:07	ZENTRALE	172.16.10.1	0	225.133000	273.192000	247.214000	Maximum round	Maximum rou
03/07/2016 15:39:37	ZENTRALE	172.16.10.1	0	224.352000	243.303000	232.394000	Maximum round	Maximum rou
03/07/2016 15:40:07	ZENTRALE	172.16.10.1	0	226.346000	272.141000	246.442000	Maximum round	Maximum rou
03/07/2016 15:40:37	ZENTRALE	172.16.10.1	60	225.465000	386.022000	305.743000	Maximum round	Maximum rou
03/07/2016 15:41:07	ZENTRALE	172.16.10.1	0	225.130000	250.071000	234.968000	Maximum round	Maximum rou
03/07/2016 15:41:37	ZENTRALE	172.16.10.1	0	224.692000	257.372000	239.098000	Maximum round	Maximum rou
03/07/2016 15:42:07	ZENTRALE	172.16.10.1	0	223.870000	233.671000	227.234000	Maximum round	Maximum rou
03/07/2016 15:42:37	ZENTRALE	172.16.10.1	0	225.082000	390.594000	265.369000	Maximum round	Maximum rou
03/07/2016 15:43:07	ZENTRALE	172.16.10.1	0	225.358000	241.393000	231.379000	Maximum round	Maximum rou
	nig textensits of Steff ig View Timestamp 03/07/2016 153337 03/07/2016 153337 03/07/2016 153437 03/07/2016 153437	Inimite testinution         Steff-1780EW-4G           ig         Yiew           Timestamp         Name           03/07/2016 153307         ENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153337         ZENTRALE           03/07/2016 153377         ZENTRALE           03/07/2016 153378         ZENTRALE           03/07/2016 153370         ZENTRALE           03/07/2016 153370         ZENTRALE           03/07/2016 153370         ZENTRALE           03/07/2016 153370         ZENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153307         ZENTRALE           03/07/2016 153407         ZENTRALE           03/07/2016 153407         ZENTRALE           03/07/2016 1534307         ZENT	wine testerals of Steff-1780EW-46           gr Vew         Destination           03/07/2016 15:33:07         ZENTRALE         1722.63.0.1           03/07/2016 15:33:07         ZENTRALE         1723.63.0.1           03/07/2016 15:33:07         ZENTRALE         1723.63.0.1           03/07/2016 15:35:07         ZENTRALE         1723.63.0.1           03/07/2016 15:36:07         ZENTRALE         1723.63.0.1           03/07/2016 15:36:07         ZENTRALE         1723.63.0.1           03/07/2016 15:36:07         ZENTRALE         1723.63.0.1           03/07/2016 15:36:07         ZENTRALE         1723.63.0.1           03/07/2016 15:37         ZENTRALE         1723.63.0.1           03/07/2016 15:38:07         ZENTRALE         1723.63.0.1           03/07/2016 15:39:07         ZENTRALE         1723.63.0.1           03/07/2016 15:37         ZENTRALE         1723.63.0.1           03/07/2016 15:37         ZENTRALE         1723.63.0.1	origo Estere         TORRALE         TORESTING         Name         Declination         Packetlost           0.007/2016 15:3307         ZENTRALE         17/216:101         0 <td>Operation         Name         Destination         Packetions         Minimal round trip time           0.307/2016 153307         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153337         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153337         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153367         EVIFRALE         172.16.10.1         0         225.85000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         225.45000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         225.45000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         224.95000           0.307/2016 153377         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153377         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153837         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153807         ZVIFRALE         172.16.10.1         0         224.85000           &lt;</td> <td>Operation         Control         Packettors         Maximum round trip time           19         Yew         Tenestamp         Name         Destination         Packettors         Minimal round trip time         Maximum round trip time           0.107/2016 15:33.07         ZENTRALE         1721.61.01         0         224.869000         272.25000           0.007/2016 15:33.07         ZENTRALE         1721.61.01         0         225.852000         286.63000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.65000         280.97000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.40000         280.97000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.40000         281.49000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.49000         293.14000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         272.59000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         273.49000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         273.49000      <tr< td=""><td>Unique texture         Server           grag         Server           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         256.37000         228.50000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         272.29000         228.5000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         228.58000         272.29000         228.75000           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.68000         246.49300         246.49300           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.94000         255.19400         228.48400           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         226.49000         272.4900         228.48400           0.0107/2016 15:36:07         ZENTRALE         172.16:10.1         0         226.49000         271.48400         271.48400           0.0107/2016 15:36:37         ZENTRALE         172.16:10.1         0         224.491000         223.29000         228.28000         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100</td><td>Unique texturals of Steff-1702FW-46           y Lew         Transtamp         Name         Destination         Packetios         Minimal round trip time         Average round trip time         Average round trip time         Warning due to           0.107/2016 153:307         ZENTRALE         172.16.10.1         0         224.469000         256.3700         228.5000         Maimum round         0.307/2016 153:370         ZENTRALE         172.16.10.1         0         224.469000         225.2000         228.7000         Maimum round         0.307/2016 153:370         PKINE         172.16.10.1         0         225.542000         226.04200         226.43200         Maimum round         0.307/2016 153:577         ZENTRALE         172.16.10.1         0         225.542000         226.04200         226.54200</td></tr<></td>	Operation         Name         Destination         Packetions         Minimal round trip time           0.307/2016 153307         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153337         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153337         EVIFRALE         172.16.10.1         0         224.86000           0.307/2016 153367         EVIFRALE         172.16.10.1         0         225.85000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         225.45000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         225.45000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153537         EVIFRALE         172.16.10.1         0         224.95000           0.307/2016 153377         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153377         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153837         EVIFRALE         172.16.10.1         0         224.85000           0.307/2016 153807         ZVIFRALE         172.16.10.1         0         224.85000           <	Operation         Control         Packettors         Maximum round trip time           19         Yew         Tenestamp         Name         Destination         Packettors         Minimal round trip time         Maximum round trip time           0.107/2016 15:33.07         ZENTRALE         1721.61.01         0         224.869000         272.25000           0.007/2016 15:33.07         ZENTRALE         1721.61.01         0         225.852000         286.63000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.65000         280.97000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.40000         280.97000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.40000         281.49000           0.007/2016 15:35.07         ZENTRALE         1721.61.01         0         225.49000         293.14000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         272.59000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         273.49000           0.007/2016 15:36.07         ZENTRALE         1721.61.01         0         224.49000         273.49000 <tr< td=""><td>Unique texture         Server           grag         Server           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         256.37000         228.50000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         272.29000         228.5000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         228.58000         272.29000         228.75000           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.68000         246.49300         246.49300           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.94000         255.19400         228.48400           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         226.49000         272.4900         228.48400           0.0107/2016 15:36:07         ZENTRALE         172.16:10.1         0         226.49000         271.48400         271.48400           0.0107/2016 15:36:37         ZENTRALE         172.16:10.1         0         224.491000         223.29000         228.28000         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100</td><td>Unique texturals of Steff-1702FW-46           y Lew         Transtamp         Name         Destination         Packetios         Minimal round trip time         Average round trip time         Average round trip time         Warning due to           0.107/2016 153:307         ZENTRALE         172.16.10.1         0         224.469000         256.3700         228.5000         Maimum round         0.307/2016 153:370         ZENTRALE         172.16.10.1         0         224.469000         225.2000         228.7000         Maimum round         0.307/2016 153:370         PKINE         172.16.10.1         0         225.542000         226.04200         226.43200         Maimum round         0.307/2016 153:577         ZENTRALE         172.16.10.1         0         225.542000         226.04200         226.54200</td></tr<>	Unique texture         Server           grag         Server           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         256.37000         228.50000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         224.86000         272.29000         228.5000           0.0107/2016 15:33:07         ZENTRALE         172.16:10.1         0         228.58000         272.29000         228.75000           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.68000         246.49300         246.49300           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         225.94000         255.19400         228.48400           0.0107/2016 15:35:07         ZENTRALE         172.16:10.1         0         226.49000         272.4900         228.48400           0.0107/2016 15:36:07         ZENTRALE         172.16:10.1         0         226.49000         271.48400         271.48400           0.0107/2016 15:36:37         ZENTRALE         172.16:10.1         0         224.491000         223.29000         228.28000         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100         224.49100	Unique texturals of Steff-1702FW-46           y Lew         Transtamp         Name         Destination         Packetios         Minimal round trip time         Average round trip time         Average round trip time         Warning due to           0.107/2016 153:307         ZENTRALE         172.16.10.1         0         224.469000         256.3700         228.5000         Maimum round         0.307/2016 153:370         ZENTRALE         172.16.10.1         0         224.469000         225.2000         228.7000         Maimum round         0.307/2016 153:370         PKINE         172.16.10.1         0         225.542000         226.04200         226.43200         Maimum round         0.307/2016 153:577         ZENTRALE         172.16.10.1         0         225.542000         226.04200         226.54200

# 5.5.4 Additions to the Status menu

# **SLA** monitor

This menu contains the status values for the SLA monitor.

SNMP ID:

1.36

Telnet path:

Status

# ICMP

This menu contains the history log and the recent results of the ICMP.

### SNMP ID:

1.36.1

Telnet path: Status > SLA-Monitor

# **History** log

This entry contains the history table.

# SNMP ID:

1.36.1.1

Telnet path: Status > SLA-Monitor > ICMP

# Index

Consecutive numbering of entries.

SNMP ID:

1.36.1.1.1

# Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Timestamp

Exact time when the entry was created.

# SNMP ID:

1.36.1.1.2

# Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Name

Name of the ICMP configuration.

### SNMP ID:

1.36.1.1.3

# Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Destination

This entry contains the destination of the check.

# SNMP ID:

1.36.1.1.4

# Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# **Pkt-Loss-Percent**

This entry shows the number of lost data packets in percent.

### SNMP ID:

1.36.1.1.5

### Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# **RTT-Min**

This entry shows the minimum round-trip time of the ICMP packets.

### SNMP ID:

1.36.1.1.6

### Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# **RTT-Max**

This entry shows the maximum round-trip time of the ICMP packets.

### SNMP ID:

1.36.1.1.7

### Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# **RTT-Avg**

This entry shows the average round-trip time of the ICMP packets.

### SNMP ID:

```
1.36.1.1.8
```

### Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Warning

This entry contains the number of reported warnings.

#### SNMP ID:

1.36.1.1.9

# Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Critical

This entry contains the number of reported errors.

### SNMP ID:

1.36.1.1.10

## Telnet path:

Status > SLA-Monitor > ICMP > History-Log

# Last-Result

This entry contains the table with the results of the last check.

# SNMP ID:

1.36.1.2

# Telnet path: Status > SLA-Monitor > ICMP

# Name

Name of the ICMP configuration.

# SNMP ID:

1.36.1.2.1

# Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# Destination

This entry contains the destination of the last check.

### SNMP ID:

1.36.1.2.2

Telnet path: Status > SLA-Monitor > ICMP > Last-Result

# Timestamp

Exact time when the entry was created.

SNMP ID:

1.36.1.2.3

# Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# **Pkt-Loss-Percent**

This entry shows the number of lost data packets in percent.

### SNMP ID:

1.36.1.2.4

Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# **RTT-Min**

This entry shows the minimum round-trip time of the ICMP packets.

### SNMP ID:

1.36.1.2.5

# Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# **RTT-Max**

This entry shows the maximum round-trip time of the ICMP packets.

#### SNMP ID:

1.36.1.2.6

## Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# RTT-Avg

This entry shows the average round-trip time of the ICMP packets.

#### SNMP ID:

1.36.1.2.7

## Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# Warning

This entry contains the number of reported warnings.

#### SNMP ID:

1.36.1.2.8

# Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# Critical

This entry contains the number of reported errors.

### SNMP ID:

1.36.1.2.9

# Telnet path:

Status > SLA-Monitor > ICMP > Last-Result

# **Delete-Values**

This entry give you the option to delete all values.

### SNMP ID:

1.36.1.3

Telnet path:

Status > SLA-Monitor > ICMP

# 5.5.5 Additions to the Setup menu

# **SLA** monitor

This menu contains the settings for the SLA monitor.

SNMP ID:

2.45

Telnet path:

Setup

### ICMP

This menu is used to configure the Internet Control Message Protocol (ICMP).

### SNMP ID:

2.45.1

# Telnet path:

Setup > SLA-Monitor

# Name

Contains the name of the ICMP configuration.

### SNMP ID:

2.45.1.1

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

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

### Default:

empty

# Active

This entry controls whether the ICMP profile is actually used.

### SNMP ID:

2.45.1.2

# Telnet path:

Setup > SLA-Monitor > ICMP

**Possible values:** 

Yes No

# Default:

Yes

### Destination

Set an IPv4 address to which the ICMP sends diagnostic and error messages.

#### SNMP ID:

2.45.1.3

### Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 40 characters from [0-9].

# Default:

0.0.0.0

# Rtg-Tag

Enter the routing tag for setting the route to the relevant remote gateway.

### SNMP ID:

2.45.1.4

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 5 characters from [0-9]

### Default:

0

# Loopback address

The device sees this address as its own address, which is also available even if a physical interface is disabled, for example.

#### SNMP ID:

2.45.1.5

# Telnet path:

### Setup > SLA-Monitor > ICMP

### Possible values:

Max. 56 characters from [0-9]

### Default:

empty

### Interval

The interval in seconds in which the ICMP sends diagnostic or error messages to the specified destination.

#### SNMP ID:

2.45.1.6

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 6 characters from [0-9]

#### Default:

30

### Start offset

Here you specify a startup delay for the ICMP transmissions in milliseconds.

## SNMP ID:

2.45.1.7

### Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 6 characters from [0-9]

# Default:

0

#### Count

Set the number of ICMP packets to be transmitted at the same time.

#### SNMP ID:

2.45.1.8

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 3 characters from [0-9]

### Default:

5

# Packet delay

Sets delay before the ICMP packets are transmitted. Delay in milliseconds.

#### SNMP ID:

2.45.1.9

# Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 4 characters from [0-9]

### Default:

1000

### Packet size

Sets the packet size for ICMP messages. The value is set in bytes.

#### SNMP ID:

2.45.1.10

### Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 5 characters from [0-9]

### Default:

56

#### Warn-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor emits a warning.

#### SNMP ID:

2.45.1.11

# Telnet path: Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 4 characters from [0-9]

### Default:

100

# Crit-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor reports an error.

#### SNMP ID:

2.45.1.12

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

200

### Warn-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor emits a warning.

#### SNMP ID:

2.45.1.13

### Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

80

### Crit-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor reports an error.

#### SNMP ID:

2.45.1.14

# Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

170

# Warn-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before a warning is issued.

#### SNMP ID:

2.45.1.15

### Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 3 characters from [0-9]

### Default:

10

### Crit-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before an error message is issued.

## SNMP ID:

2.45.1.16

### Telnet path:

Setup > SLA-Monitor > ICMP

### **Possible values:**

Max. 3 characters from [0-9]

### Default:

20

#### **IP-Version**

Specifies the IP standard used for the Internet Control Message Protocol.

#### SNMP ID:

2.45.1.17

# Telnet path:

Setup > SLA-Monitor > ICMP

# Possible values:

Auto IPv4 IPv6

### Default:

Auto

# Comment

Comment about this ICMP configuration.

### SNMP ID:

2.45.1.19

### Telnet path:

Setup > SLA-Monitor > ICMP

#### **Possible values:**

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

# Default:

empty

### **Event count**

Number of events to be logged by the SLA monitor.

### SNMP ID:

2.45.2

### **Telnet path:**

Setup > SLA-Monitor

### Possible values:

Max. 3 characters from [0-9]

# Default:

100

#### Startup delay

Delay time in milliseconds before monitoring is started.

# SNMP ID: 2.45.3 Telnet path: Setup > SLA-Monitor Possible values: Max. 3 characters from [0-9] Default:

10

# 5.6 Additional DSL-modem status values

As of version 9.20, LCOS provides additional status values for DSL connections, i.e. the duration and number of connections.

# 5.6.1 Read out DSL modem status values with LANmonitor

LANmonitor can be used to read out the status values for each registered device with an ADSL/VDSL modem in the section **System information** > **Interfaces** > **ADSL modem: <Status**>.



# 5.6.2 Additions to the Status menu

# **Connection count**

This entry contains the number of DSL connections since the last system reboot.

SNMP ID:

1.75.53

Telnet path: Status > VDSL

# **Connection duration**

This entry contains the duration of the DSL connection since the last synchronization.

# SNMP ID:

1.75.54

Telnet path: Status > VDSL

# **Connection count**

This entry contains the number of DSL connections since the last system reboot.

### SNMP ID:

1.75.25.53

Telnet path: Status > VDSL > Advanced

# **Connection duration**

This entry contains the duration of the DSL connection since the last synchronization.

### SNMP ID:

1.75.25.54

# Telnet path:

Status > VDSL > Advanced
# 5.7 Displaying the mobile/cellular standards

As of LCOS version 9.20, LANconfig displays the names of mobile/cellular standards along with the corresponding generation numbers:

- GPRS: 2G
- GSM: 2G
- EDGE: 2.5G
- UMTS: 3G
- HSPA: 3.5G
- HSDPA: 3.5G
- HSUPA: 3.5G
- HSPA+: 3.5G
- LTE: 4G

# 5.7.1 Additions to the Setup menu

# Mode

Select the mobile networking transmission mode here.

### SNMP ID:

2.23.41.1.6

# Telnet path:

Setup > Interfaces > Mobile > Profiles

### **Possible values:**

#### Auto

Automatic selection of transmission mode

# 3G

UMTS operation only

# 2G

GPRS operation only

# 3G-2G

Combined UMTS-GPRS operation

## 4G

LTE operation only

### 4G-3G

Combined LTE-UMTS operation

### 4G-2G

Combined LTE-GPRS operation

# Default:

Auto

5 Routing and WAN connections

# 5.7.2 Additions to the Status menu

# Mode

This entry shows the mobile/cellular mode.

# SNMP ID:

1.49.9.3

# Telnet path:

Status > Modem-Mobile > Network-List

**Possible values:** 

Unknown 2G 3G 4G

# Mode

This entry contains the mobile/cellular mode.

### SNMP ID:

1.49.12

### Telnet path:

Status > Modem-Mobile

Possible values:

```
Unknown
UMTS(3G)
GPRS(2G)
GSM(2G)
EDGE(2.5G)
HSDPA(3.5G)
HSDPA(3.5G)
HSPA+(3.5G)
LTE(4G)
HSPA(3.5G)
```

# Default:

Unknown

# Mode

This entry contains the status values for Mode.

5 Routing and WAN connections

#### SNMP ID:

1.49.16.5

Telnet path:

Status > Modem-Mobile > History

Possible values:

Unknown UMTS(3G) GPRS(2G) GSM(2G) EDGE(2.5G) HSDPA(3.5G) HSDPA(3.5G) HSPA+(3.5G) LTE(4G) HSPA(3.5G)

### Default:

Unknown

# AcT

This entry contains the status values for AcT.

#### SNMP ID:

1.49.47.5

### Telnet path:

Status > Modem-Mobile > Network-List

**Possible values:** 

Unknown 2G 3G

4G

# 6 IPv6

# 6.1 IPv6 support for (S)NTP client and server

LCOS version 9.20 supports IPv6 for the (S)NTP client and server.

# 6.1.1 Configuring the time server under LANconfig

In order for a device to broadcast the current time on the network, go to **Date & Time > Synchronization** and enable the regular synchronization with a time server.

Select the adjustment method	for the implemented realtime clock	:
No regular adjustment of the second secon	ne device time	
Adjustment whenever a co	nnection is made to ISDN	
Synchronize to a time serv	er using NTP at regular intervals	
NTP client settings		
	Time server	
Request interval:	86.400	seconds
Number of tries:	4	

### **Request interval**

Specify the time interval in seconds after which the internal clock of the device is re-synchronized with the specified time server (NTP).

### Number of tries

Enter the number of times that the device should try to synchronize with the time server. By setting this value to zero, the device attempts to connect until it achieves a valid synchronization.

Then go to the section **NTP settings** and, under **Time server**, configure the settings for synchronizing the time with the server.

Time server - New Entry	? 💌
Name or address: Source address (opt.):	▼ ▼ Select
	OK Cancel

### Name or address

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.



If you specify more than one time server in the list, you set the order in which they are queried in the overview of entries.

#### Source address (optional)

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- 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 (caution: If there is an interface called "DMZ", then the device takes its address).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Any valid IPv4 or IPv6 address

With these settings, the device initially retrieves the time from the public time servers for its own use only. To broadcast the current time to other devices in the LAN, go to **Date & Time** > **Synchronization** and, in the section **NTP server settings**, enable the time server on the device.

NTP server settings		
Your device can serve as a local synchronize. Additionally, it can se local network.	time server to which other device end the time in constant intervals	es or stations can to all of the stations on your
📝 Time server enabled		
📝 Broadcast mode (IPv4 only)		
Broadcast interval:	60	seconds

#### Time server enabled

Enable this option if the device is to work as a time server on the network.

### Broadcast mode (IPv4 only)

If the device should regularly operate as a time server and send the current time to all stations in the network, enable the "send mode" here.



The send mode of the device only supports IPv4 addresses.

### **Broadcast interval**

Specify the time interval in seconds after which the time server broadcasts the current time to the accessible stations on the network.

# 6.1.2 Additions to the Setup menu

### BC-Mode

If the device should regularly operate as a time server and send the current time to all stations in the network, enable the "send mode" here.



The send mode of the device only supports IPv4 addresses.

6 IPv6

#### SNMP ID:

2.26.3

Telnet path:

Setup > NTP

# Possible values:

No

The send mode is disabled.

### Yes

The send mode is enabled.

### Default:

No

# **RQ-Address**

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.

### SNMP ID:

2.26.11.1

# Telnet path:

Setup > NTP > RQ-Address

### **Possible values:**

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

#### Default:

empty

# Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

() If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- 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 (caution: If there is an interface called "DMZ", then the device takes its address).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Any valid IPv4 or IPv6 address

# SNMP ID:

2.26.11.2

# Telnet path:

Setup > NTP > RQ-Address

# Possible values:

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

# Default:

empty

# 7 VPN

# 7.1 IKEv2 support

As of LCOS version 9.20, LCOS supports IKEv2.

# 7.1.1 Functions of the VPN module

This section lists all of the functions and properties of the LCOS VPN module. Experts of the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the VPN, this information is non-essential.

- VPN tunnel via leased lines, switched connections and IP networks
- LANCOMDynamic VPN: Public IP addresses can be static or dynamic (establishing a connection with remote sites using dynamic IP addresses requires ISDN)
- VPN in accordance with IPSec standard
- IPSec protocols ESP, AH and IPCOMP in tunnel mode
- Hash algorithms:
  - □ HMAC-MD5-96, hash length 128 bits
  - □ HMAC-SHA-1-96, hash length 160 bits
  - HMAC-SHA-1-256, hash length 256 bits
  - □ HMAC-SHA-1-384, hash length 384 bits
  - □ HMAC-SHA-1-512, hash length 512 bits
- Compression with "Deflate" (ZLIB)
- Key management as per ISAKMP (IKEv1, IKEv2)
- Symmetrical encryption methods
  - □ AES, key lengths of 128, 192 and 256 bits
  - □ Triple-DES (3DES), key length 168 bit
  - Blowfish, key length 128 448 bits
  - CAST, key length 128 bits
  - DES, key length 56 bits
- IKEv1 main and aggressive mode
- IKEv1/IKEv2 config mode
- IKEv1 with pre-shared keys and IKEv2
- IKEv1 and IKEv2 with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bits, 1024 bits, 1536 bits, 2048 bits, 3072 bits and 4096 bits (well-known groups 1, 2, 5, 14, 15 and 16)

# 7.1.2 IKEv2

LANCOM devices are capable of VPN with IKEv1 and IKEv2.

IKEv2 facilitates a fast and secure establishment of VPN tunnels. For the first time it is now possible to operate encrypted networking between IPv6-based sites and IPv4-based sites by means of the mixed mode.

Manually configuring a VPN connection that uses IKEv1 is complex and error prone. Consequently, many IPSec implementations have incompatible configurations, which causes the VPN connections between the devices to fail. The IKEv2 configuration in LCOS gives administrators a reliable method of setting up a configuration that matches that of the remote station. For example, administrators have a choice of several Diffie-Hellman groups. At the same time, the revised user interface presents recommended default values for many of the configuration parameters. The simplified configuration with IKEv2 eliminates sources of error, which results in a lower administrative overhead. Further, VPN connection establishment with IKEv2 offers better performance, because IKEv2 only exchanges 4 packets when negotiating a VPN tunnel (one REQUEST per VPN partner and one REPLY), rather than the 6 required by IKEv1 in the "aggressive/quick mode" or 12 in "main mode". The standard of security is just as high with IKEv2 as with IKEv1.

Operating IKEv2 supports RFC 7296, RFC 7427 and, in the IKEv2 client mode, RFC 5685.

# 7.1.3 Configuring IKEv2 with LANconfig

IKEv2 is configured under VPN > IKEv2/IPSec.

	v/ deneralj.	
Conr	ection list	Connection parameters
Authentication		
Define identities for these tables.	VPN connections as well a	s the associated profiles for digital signatures in
Auth	entication	Digital signature profile
Use this table to del	ine the IKEv2 crypto param	eters.
Use this table to del	ine the IKEv2 crypto param	eters.
Use this table to del	ine the IKE v2 crypto param	reters.
Use this table to del Addresses for in-dial Here you define the	ine the IKE v2 crypto param En ing access (CFG-Mode serv parameters the dial-in clien	ieters. cryption ver) ts are assigned by CFG-Mode.
Use this table to def Addresses for in-dial Here you define the	ine the IKE v2 crypto param En ing access (CFG-Mode serv parameters the dial-in clien addresses	ieters. cryption /er) ts are assigned by CFG-Mode. IPv6 addresses
Use this table to del Addresses for in dial Here you define the IPv4 Extended settings	ine the IKEv2 ctypto param En ing access (CFG-Mode ser parameters the dial-in clien addresses	ieters. cryption ver) ts are assigned by CFG-Mode. IPv6 addresses
Use this table to def Addresses for in-dial Here you define the IPv4 Extended settings	ine the IKEv2 ctypto param En ing access (CFG-Mode serv parameters the dial-in clien addresses	ieters. cryption /er) ts are assigned by CFG-Mode. IPv6 addresses ded settings
Use this table to def Addresses for in-dial Here you define the IPv4 Extended settings Fragmentation	ine the IKEv2 ctypto param En ing access (CFG-Mode serv parameters the dial-in clien addresses Extend	ieters. cryption /er) ts are assigned by CFG-Mode. IPv6 addresses

#### VPN connections

In this section, you configure the IKEv2 VPN connections and the connection parameters.

#### Authentication

This table is used to define the identities for your VPN connections.

### **Digital signature profile**

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

### Encryption

This table is used to set the encryption parameters.

#### Addresses for dial-in access (CFG mode server)

Use this table to specify the parameters that the device CFG mode assigns to the dial-in clients.

### **Extended settings**

This section is used to configure the settings for the authentication of other remote identities, the IKEv2 rekeying parameters, and the prefixes for IKEv2 routing.

In order to configure an IKEv2 connection, you first need to make an entry in the **Connection list**. LCOS contains default entries in order to minimize the effort of configuration. Most of these entries contain default parameters with common settings for strong encryption algorithms, dead-peer-detection, and lifetimes. All you need to do is specify the address of the VPN remote peer, the authentication parameters (under **Authentication**), and the VPN rules (under **VPN** > **General** > **Network rules**).



The console command show vpn displays whether the VPN connection was established successfully.

# **Connection list**

In this table, you configure the IKEv2 connections to VPN partners.

Connection list - New Ent	try	? 💌
🔽 Entry active		
Name of connection:		
Short hold time:	0	seconds
Gateway:		]
Routing tag:	0	
Encryption:	DEFAULT -	Select
Authentication:	DEFAULT -	Select
Connection parameters:	DEFAULT -	Select
Lifetimes:	DEFAULT -	Select
IKE-CFG:	Off 🗸 🗸	]
IPv4 address pool:	•	Select
IPv6 address pool:	•	Select
Rule Creation:	Manual 👻	]
IPv4 rules:	•	Select
IPv6 rules:	•	Select
Routing:	•	Select
RADIUS auth. server:	•	Select
RADIUS acc. server:	•	Select
Comment:		]
	OK	Cancel

### **Entry active**

Enables or disables the connection to this VPN peer.

### Name of connection

Contains the name of the connection to the remote station.

### Short hold time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

### Gateway

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

### **Routing tag**

Contains the routing tag for this VPN connection.

### Encryption

Specifies the encryption used for the VPN connection. The corresponding entry is located in the **Encryption** table.

### Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the **Authentication** table.

### **Connection parameters**

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the **Connection parameters** table.

### Validity period

Specifies the lifetime of the key used for the VPN connection. The corresponding entry is located in the **Extended settings** > **Lifetimes** table.

### **IKE-CFG**

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

Possible values are:

- Off: IKEv2 config mode is disabled
- Server: The router distributes configuration parameters (such as addresses or the DNS server) to VPN clients. The parameters to be distributed are configured in the IPv4 or IPv6 address pool.
- Client: The router requests the server for configuration parameters (e.g. addresses or the DNS server).

# IPv4 address pool

IPv4 addresses and DNS server for dial-in access in the IKE CFG mode Server.

#### IPv6 address pool

IPv6 addresses and DNS server for dial-in access in the IKE CFG mode Server.

### **Rule creation**

Specifies how VPN rules are created.

Possible values:

### Automatic

The local intranet serves as the source network (private IP address range that the local VPN gateway itself belongs to). For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

When two simple local networks are connected, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.

### Manual

Rules are created for the network relationships in the same way as rules are defined manually for IPv4 or IPv6.

### **IPv4-Rules**

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table **VPN** > **Network rules**.

# **IPv6-Rules**

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table VPN > Network rules.

### Routing

Specifies the routes that the remote site should transmit dynamically via IKE-CFG mode. This function is only available in the IKEv2 CFG mode for the client and server.

The routes for IPv4 and IPv6 connections are located in the **Extended settings** > **IPv4 routing/IPv6 routing** tables.

### **RADIUS** auth. server

Specifies the RADIUS server for the VPN peer authorization. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPSec** under **Extended settings**.

### **RADIUS** auth. server

Specifies the RADIUS server for the VPN peer accounting. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPSec** under **Extended settings**.

### Comment

Enter a descriptive comment here.

# **Connection parameters**

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

Connection parameters	- New Entry	? 💌
Name:	I	
Dead Peer Detection:	30	seconds
IPSec-over-HTTPS:	Off	•
IPCOMP:	No	•
Mode:	Tunnel	•
	OK	Cancel

### Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Connection parameters" field.

### **Dead peer detection**

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

### **IPSec-over-HTTPS**

Specifies whether the connection uses IKEv2 over HTTPS.

### IPCOMP

Specifies whether the devices transmit compressed IKEv2 data packets.

# Mode

Specifies the mode of transmission.

# Authentication

In this table, you configure the parameters for IKEv2 authentication of the local and at least one remote identifier.

Name:			
Local authentication:	PSK	•	
Local dig. signature profile:	DEFAULT	•	Select
Local identifier type:	No identity	•	
Local identifier:			
Local password:			Show
	Generate password	•	
Remote authentication:	RSA signature	•	
Remote dig. signature profil	DEFAULT	•	Select
Remote identifier type:	No identity	•	
Remote identifier:			
Remote password:			Show
	Generate password	•	
Addit, remote identities list;		•	Select
Local certificate:		•	
Remote cert. ID check:	Yes	•	
OCSP check:	No	•	

### Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Authentication" field.

### Local authentication

Sets the authentication method for the local identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per *RFC 7427*. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

### Local digital signature profile

The profile name of the local digital signature profile that is used.

### Local identifier type

Displays the ID type of the local identity. The device interprets the entry under "Local identifier" accordingly. Possible entries are:

- No identity: No identity is transmitted.
- IPv4 address: The device uses an IPv4 address as a local ID.
- IPv6 address: The device uses an IPv6 address as a local ID.
- Domain name (FQDN): The device uses a domain name as a local ID.

- E-mail address (FQUN): The device uses an e-mail address as a local ID.
- ASN.1 Distinguished Name: The device uses a distinguished name as a local ID (e.g. "CN=client01.example.com,O=test,C=DE").
- Key ID (group name): The device uses the group name as a local ID. You can set any group name.

### Local identifier

Contains the local identity. The significance of this entry depends on the setting under "Local identifier type".

#### Local password

Contains the password of the local identity. The device uses this password to authenticate at the remote site. The local and remote password can be identical or different.

### **Remote authentication**

Sets the authentication method for the remote identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per *RFC 7427*. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

#### Remote digital signature profile

The profile name of the remote digital signature profile.

#### Remote identifier type

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under "Remote identifier" accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the "Remote identifier" field.
- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as a remote ID (e.g. "CN=client01.example.com,O=test,C=DE").
- Key ID (group name): The device expects the group name as the remote ID.

### **Remote identifier**

Contains the remote identity. The significance of this entry depends on the setting under "Remote identifier type".

#### Remote password

Contains the password of the remote identity.

#### Addit. remote identities list

Redundant VPN scenarios allow the use of alternative remote identities.

Here you configure additional remote identities from the table **Extended settings** > **Identity list**.

# Local certificate

Displays the local certificate.

## Remote certificate check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

# **Digital signature profile**

In this table, you configure the parameters for IKEv2 authentication of the local and at least one remote identifier.

Name:			
Authentication method:	RSASSA-PSS	•	
SHA1	📝 SHA-256		
🔽 SHA-384	V SHA-512		

### Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Authentication" field.

### Authentication method

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

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1\_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)

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

# Encryption

This table is used to configure the encryption parameters. An entry named "DEFAULT" is provided with common settings.

Multiple parameters can be selected. The device propagates these parameter lists in the IKE protocol and in CHILD SAs. The two VPN partners agree to use one of the algorithms in the propagated lists. While they are establishing the first IKE SA, the VPN partners agree to use the highest of the mutually propagated DH groups. The VPN partners use this DH group when they renew the IKE SAs, or when they create or renew the CHILD SAs (if PFS is enabled). A connection will be established between the VPN partners if there are sets of encryption parameters that agree at both ends. If none of the parameters match, no connection can be established.

Encryption - New Entry			8 <del>x</del>
Name:		Child-SA	
Permitted DH groups DH16 DH14 DH2	DH15	Cipher list	AES-CBC-192 3DES
PFS: IKE-SA Cipher list	Yes 🔻	<ul> <li>SHA-512</li> <li>✓ SHA-256</li> <li>MD5</li> </ul>	I SHA-384 I SHA1
AES-CBC-256	AES-CBC-192	_	
Digest list SHA-512 SHA-256 MD5	I SHA-384 I SHA1		
		· · · · · · · · · · · · · · · · · · ·	OK Cancel

### Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** by selecting it from the "Encryption" field.

### **Permitted DH groups**

Contains the selection of Diffie-Hellman groups used by the VPN partners to create a key for exchanging data. The higher the DH group selected, the more complex is the key that is generated. The following groups are currently supported:

- DH-2 (1024-bit modulus)
- DH-5 (1536-bit modulus)
- DH-14 (2048-bit modulus)
- DH-15 (3072-bit modulus)
- DH-16 (4096-bit modulus)

### PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

## **Cipher list**

Specifies which encryption algorithms are enabled.

# **Digest list**

Specifies which hash algorithms are enabled.

# **IPv4** addresses

Use this table to configure the IPv4 parameters that the device CFG mode assigns to the VPN clients.

IPv4 addresses - New Entry	/	? ×
Name:		
Address pool		
First address:	0.0.0.0	
Last address:	0.0.0.0	
Name server addresses		
Primary DNS:	0.0.0.0	
Secondary DNS:	0.0.0.0	
	OK	Cancel

### Name

Contains the name of the interface for the dial-in access.

### Address pool

### **First address**

Here you enter the first IPv4 address of the pool of addresses that you want to provide to VPN clients.

## End address

Here you enter the last IPv4 address of the pool of addresses that you want to provide to VPN clients.

### Name server addresses

### **DNS default**

Contains the primary DNS address.

# **DNS backup**

Contains the secondary DNS address.

# **IPv6 addresses**

If the device operates as a "CFG-mode server", it uses the IKEv2 configuration payload to assign an address from a local address pool to clients. Also, it can assign up to two DNS servers to the client.

To operate this, you use the VPN connection list to enable the CFG mode "Server" on the server and the CFG mode "Client" on the client.

Use this table to configure the IPv6 parameters that the device in the CFG mode "Server" assigns to VPN clients.

IP∨6 addresses - New Entry	,	? <mark>×</mark>
Name:		
Address pool		
First address:		
Last address:	::	
Name server addresses		
Primary DNS:		
Secondary DNS:		
	ОК	Cancel

### Name

Contains the name of the interface for the dial-in access.

# Address pool

### **First address**

Here you enter the first IPv6 address of the pool of addresses that you want to provide to VPN clients.

# End address

Here you enter the last IPv6 address of the pool of addresses that you want to provide to VPN clients.

# Name server addresses

## **DNS default**

Contains the primary DNS address.

# **DNS backup**

Contains the secondary DNS address.

# **Extended settings**

Use this dialog to configure the settings for the authentication of other remote identities, the IKEv2 rekeying parameters, the prefixes for IKEv2 routing, and the RADIUS server for IKEv2.

Extended settings			? <mark>×</mark>
Authentication Additional remote identitie: Identity list	s	Identities	
Lifetime			
The lifetimes table defines	IKEv21	ekeying timeouts.	
		Lifetimes	
IKEv2 routing			
Here you define the prefix routing IKE v2.	es that a	are propagated by dynam	ic
IPv4 routing		IPv6 routing	
RADIUS authentication			
Define here what RADIUS	server:	s to use for authentication	r. –
		RADIUS server	
Password:	Gener	ate password 💌	w
RADIUS accounting			
Define here what RADIUS	server:	s to use for accounting.	
		RADIUS server	
Update cycle:	0	secon	ds
		ОК Са	ancel

# Lifetimes

Use this table to specify the IKEv2 rekeying parameters. An entry named "DEFAULT" is provided with common settings.

Depending on the phase, the device discriminates according to time or the amount of transmitting data. The parameter that reaches its limit first triggers the renewal of the corresponding IKEv2 key.



The value "0" means that the device sets no limit on the corresponding key.

Lifetimes - New Entry		? 🔀
Name:		
Phase 1:	10.800	seconds
	0	kBytes
Phase 2:	28.800	seconds
	2.000.000	kBytes
	OK	Cancel

### Name

Contains the unique name of this entry.

### Phase 1:

Contains the time in seconds or the data volume in kilobytes until the IKE SA key is renewed.

### Phase 2:

Contains the time in seconds or the data volume in kilobytes until the CHILD SA key is renewed.

### **IPv4** routing

Use this table to configure the IPv4 networks that the device propagates via dynamic routing as per IKEv2.

IPv4 routing - New Entry	? 💌
Name:	
Network:	Select
Send IKE-CFG-Address	

### Name

Contains the unique name of this entry.

### Network

Contains the comma-separated list of IP subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix length
- IP interface name

The IP subnets are configured under IPv4 > General in the section Own addresses.

# Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

# **IPv6** routing

Use this table to configure the IPv6 networks that the device propagates via dynamic routing as per IKEv2.

IPv6 routing - New Entry	? 💌
Name:	
Network:	Select
🔄 Send IKE-CFG-Address	
	OK Cancel

### Name

Contains the unique name of this entry.

### Network

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 interface name

The IP subnets are configured under IPv6 > General in the section IPv6 networks.

# Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

# 7.1.4 Tutorial: Setting up IKEv2 under LANconfig

**Initial situation:** Two LANCOM routers are connected via a WAN link. The requirement is to establish a secure VPN connection between them by means of IKEv2/IPSec VPN. The routers are a LANCOM 1781AW at the main office and a LANCOM 1781VA-4G at the branch office.



1. Enabling VPN: For both of the routers, open the menu item VPN > General and, under Virtual Private Network, select the option Activated. This enables VPN on that specific device.

Virtual Private Network:	Activated
Simplified RAS with certificates a	activated
Allow peer to select remote netw	ork
📝 NAT traversal activated	
Accept IPSec-over-HTTPS	
Establ. of net relationships (SAs):	Collectively with KeepAlive 💌
VPN connections	
In this table, you can define the V Specify additional net relationship	PN connections that are to be established by your device. settings in the configuration section 'Firewall/QoS'.
	Connection list
Remote gateways	
In this table, you can specify a list	of possible redundant gateways for each remote site.
	Further remote gateways
Connection parameters	
Define other parameters for the in	dividual VPN connections here.
	Connection parameters

2. Configuration of the establishment of net relations (SAs): In order for net relations to be established correctly and according to the same schema, on each of the routers you should navigate to Establishment of net relations (SAs) and enable the option Collectively with KeepAlive.

Virtual Private Network:	Activated
Simplified RAS with certificates a	activated
Allow peer to select remote netw	vork
🔽 NAT traversal activated	
Accept IPSec-over-HTTPS	
Establ. of net relationships (SAs):	Collectively with KeepAlive 💌
VPN connections	
In this table, you can define the V Specify additional net relationship	PN connections that are to be established by your device. settings in the configuration section 'Firewall/QoS'.
	Connection list
Remote gateways	
In this table, you can specify a list	of possible redundant gateways for each remote site.
	Further remote gateways
Connection parameters	
Define other parameters for the in	dividual VPN connections here.
	Connection parameters

**3.** Configuring the authentication: Specify the type of authentication for the VPN connection. To do this, open the menu item VPN > IKEv2/IPSec and click the button Authentication.

Connection list	Connection parameters
Authentication	
Define in this table identities for V	/PN connections.
	Authentication
Encryption	
Use this table to define the IKE v	2 crypto parameters.
	Encryption
Addresses for in-dialing access (0	CFG-Mode server)
Here you define the parameters t	the dial-in clients are assigned by CFG-Mode.
	IPv6 addresses
Extended settings	
-	

**4.** Click on the **Add** button to configure a new authentication type. Enter the information for the authentication of the VPN connection into the configuration window.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

Authentication - New Entr	У	? <mark>- x -</mark>	Authentication - New Ent	у	? 💌
Name:	ID-IKEV2-DEM0		Name:	ID-IKEV2-DEMO	
Local authentication:	PSK 🔻	]	Local authentication:	PSK 🔹	
Local identifier type:	Email address (FQU) 🔻	]	Local identifier type:	Email address (FQU) 🔻	
Local identifier:	head office	]	Local identifier:	branch	
Local password:	•	Show	Local password:	•	📄 Show
	Generate password			Generate password 💌	
Remote authentication:	RSA signature 🔹 👻	]	Remote authentication:	RSA signature 🔹	
Remote identifier type:	No identity 🔹 👻	]	Remote identifier type:	No identity 🔹	
Remote identifier:	branch	]	Remote identifier:	head office	
Remote password:	•	Show	Remote password:	•	Show
	Generate password 🖛			Generate password 💌	
Additional remote identities	i 👻	Select	Additional remote identities	i 🔹 👻	Select
Local certificate:	VPN-1	]	Local certificate:	VPN-1	
Remote certificate check:	No 👻	]	Remote certificate check:	No 💌	
OK Cancel				ОК	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

Parameter	Description
Name	Enter the name for the authentication here. In this example, <b>ID-IKEV2-DEMO</b> was entered on both devices. This entry is used later in the VPN connection list.
Local authentication	Select the authentication type used on this router. This example uses authentication by pre-shared key (PSK).
Local identifier type	Select the identifier type used on this router. In this example, the identity type was set to <b>E-mail</b> address (FQUN).
Local identifier	Set the local identifier. In this example, the local identifier was set to <b>Main</b> on the 1781AW and <b>Branch</b> on the 1781VA-4G.
Local password	The pre-shared key required to successfully authenticate at this router.
Remote authentication	Select the authentication type used by the remote router. On the 1781AW, this entry corresponds to the entry for "Local authentication" on the 1781VA-4G.
Remote identifier type	Select the type of the remote identifier (used by the remote router). On the 1781AW, this entry corresponds to the entry for Local identifier on the 1781VA-4G.
Remote identifier	Enter the identifier of the remote station. On the 1781AW, this entry corresponds to the entry for "Local identifier" on the 1781VA-4G.
Remote password	The pre-shared key required to successfully authenticate at the remote station. On the 1781AW, this entry corresponds to the entry for Local password on the 1781VA-4G.

5. Configuring the Connection list: Configure the connection lists on each individual router. To carry out the configuration, open the menu item VPN > IKEv2/IPSec and click the button Connection list.

VPN connections	
Configure in this table IKEv2 VPN connections. Th Network Rules (VPN/General).	ne net relationships are defined in the VPN
Connection list	Connection parameters
Authentication	
Define in this table identities for VPN connections.	
Authent	ication
Encryption	
Use this table to define the IKEv2 crypto parameter	ers.
Encry	ption
Addresses for in-dialing access (CFG-Mode server)	ļ
Here you define the parameters the dial-in clients a	are assigned by CFG-Mode.
IPv6 ad	dresses
Extended settings	
Extended	settings

6. Create a new VPN connection by clicking the button Add.

() The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

Connection list - New Ent	try	? 💌	Connection list - New Ent	iry	? 💌
🔽 Entry active			🔽 Entry active		
Name of connection:	IKEV2-DEM0	]	Name of connection:	IKEV2-DEM0	
Short hold time:	0	seconds	Short hold time:	9.999	seconds
Gateway:	1.1.1.2		Gateway:	1.1.1.1	
Routing tag:	0		Routing tag:	0	
IKE-CFG:	Off 🗸		IKE-CFG:	Off 🗸	]
Encryption:	DEFAULT -	<u>S</u> elect	Encryption:	DEFAULT -	Select
Authentication:	ID-IKEV2-DEM0 -	<u>S</u> elect	Authentication:	ID-IKEV2-DEMO -	Select
Connection parameters:	DEFAULT -	Select	Connection parameters:	DEFAULT -	Select
Lifetimes:	DEFAULT -	Select	Lifetimes:	DEFAULT -	Select
Rule Creation:	Auto -		Rule Creation:	Auto 👻	]
IPv4 rules:		Select	IPv4 rules:	-	Select
IPv6 rules:	-	<u>S</u> elect	IPv6 rules:	-	Select
Routing:	-	<u>S</u> elect	Routing:	•	Select
	OK	Cancel		ОК	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

Parameter	Description
Entry active	Set a check mark in the check box to activate the connection.
Name of connection	Enter a name for the VPN connection. This name is used later in the routing table.
Short hold time	Specify the short-hold time in seconds for the VPN connection. In this example, the value for the 1781AW is set to $0$ . This means that this router will not actively establish the VPN

Parameter	Description
	connection. The value for the 1781VA-4G is set to <b>9999</b> . This value means that the router will not actively disconnect and, in case the connection is lost, it reconnects immediately.
Gateway	Specify the IP address of the remote station. In this example, the IP address of the WAN interface of the 1781AW is 1.1.1.1 and that of the 1781VA-4G is 1.1.1.2.
Authentication	Select the authentication. The entry here corresponds to the name of the authentication that you set in <b>step 3</b> .

7. Configuring the Routing table: Configuring the routes here ensures that packets can be sent from the router through the VPN tunnel to the VPN remote station. To do this, open the menu item IP router > Routing and click the button IPv4 routing table.

Routing table	
Use this table to spec	ify the remote sites to be used to access different remote IP networks.
	IPv4 routing table
	IPv6 routing table
Time-dependent cont	rol
Time-dependent cont on the time and day o	rol can be used to specify various destinations for the default route based if the week.
🔲 Time-dependent o	control of the default route enabled
	Time control table
Load balancing	
If your Internet provid connections with a lo	er does not support real channel bundling, it is possible to combine several ad balancer.
🔲 Load balancing er	nabled
	Load balancing
For connections that WAN connection is u addresses.	fit certain protocol/port criteria, client binding ensures that only a single sed for each target address. This avoids the occurence of multiple source
Binding minutes:	30 Balance seconds: 10
	Client binding protocols

8. Create an additional route by clicking the button Add. Information about the route is entered into the configuration window for each router.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.

IPv4 routing table - New Entry		IPv4 routing table - New E	ntry	? 🗙	
IP address: Netmask: Routing tag:	192.168.2.0 255.255.255.0 0		IP address: Netmask: Routing tag:	192.168.1.0 255.255.255.0 0	
Enable state:		Enable state:			
OROUTE IS ENABLED AND WILL ALWAYS BE PROPAGATED VIA RIP (sticky)		O Houte is enabled and will always be propagated via RIP (sticky)			
Route is enabled and will be propageted via RIP if the target network is reachable (conditional)		Route is enabled and will be propageted via RIP if the target network is reachable (conditional)			
This route is disabled		This route is disabled			
Router:	IKEV2-DEMO -	Select	Router:	IKEV2-DEMO 👻	Select
Distance:	0		Distance:	0	
IP masquerading:			IP masquerading:		
IP Masquerading switched off		IP Masquerading switched off			
<ul> <li>masking Intranet and DMZ (default)</li> </ul>		masking Intranet and DMZ (default)			
🔘 masking Intranet only			🔘 masking Intranet only		
Comment:			Comment:		
	ОК	Cancel		ОК	Cancel

The left half of the images shows the LANCOM 1781AW, and the right half shows the parameters of the LANCOM 1781VA-4G.

Parameter	Description
IP address	Enter the IP network to be accessed via the VPN tunnel. In this example, the IP network 192.168.2.0 should be accessed from the 1781AW and the IP network 192.168.1.0 should be accessed from the 1781VA-4G.
Netmask	Specify the netmask of the IP network named above.
Enable state	Select the option <b>Route is enabled and will always be propagated by RIP</b> . This activates the entry and makes it available for use.
Router	For the router, enter the name of the VPN connection that you entered in <b>step 4</b> .
IP masquerading	Select <b>IP masquerading switched off</b> so that the router does not conceal the other network behind its own IP address.

9. Write the respective configurations back to the two devices.

**10.** Use LANmonitor to check the VPN connection. LANmonitor displays the status of the VPN connection.

# 7.1.5 Additions to the Setup menu

# IKEv2

In this directory you configure the IKEv2 parameters.

### SNMP ID:

2.19.36

Telnet path:

Setup > VPN

# remote sites

In this table, you configure the IKEv2 connections to VPN partners.

(f) The console command show vpn shows whether the connection is successful.

# SNMP ID:

2.19.36.1

Telnet path:

Setup > VPN > IKEv2

# Peer

Contains the name of the connection to the remote station. Subsequently, this name appears in the routing table.

#### SNMP ID:

2.19.36.1.1

### Telnet path:

Setup > VPN > IKEv2 > Peers

#### **Possible values:**

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

# Default:

DEFAULT

### Active

Specifies whether the VPN peer is enabled.

#### SNMP ID:

2.19.36.1.2

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

Yes

The VPN connection is enabled.

# No

The VPN connection is disabled.

7 VPN

#### Default:

Yes

# SH time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

#### SNMP ID:

2.19.36.1.3

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

0

0 ... 9999

### **Special values:**

# 0

The device does not actively establish a connection, but waits for data packets to arrive.

# 9999

Keepalive: The device establishes a permanent connection.

### **Remote gateway**

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

# SNMP ID:

2.19.36.1.4

### Telnet path:

Setup > VPN > IKEv2 > Peers

# **Possible values:**

Max. 40 characters from [A-Z][a-z][0-9]@{|}~!\$%&'()+-,/:;<=>?[\]^\_.`

# Default:

empty

### **Rtg-Tag**

Contains the routing tag for this VPN connection.

### SNMP ID:

2.19.36.1.5

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

Max. 5 characters from [0-9]

### Default:

0

# Encryption

Specifies the encryption method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Encryption**.

### SNMP ID:

2.19.36.1.6

### Telnet path:

Setup > VPN > IKEv2 > Peers

#### **Possible values:**

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

### Default:

DEFAULT

### Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

#### SNMP ID:

2.19.36.1.7

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

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

### Default:

empty

7 VPN

### General

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **General**.

### SNMP ID:

2.19.36.1.8

## Telnet path:

Setup > VPN > IKEv2 > Peers

# **Possible values:**

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

### Default:

DEFAULT

# Lifetimes

Specifies the lifetimes of the key used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Lifetimes**.

### SNMP ID:

2.19.36.1.9

#### Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

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

#### Default:

DEFAULT

# IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

### SNMP ID:

2.19.36.1.10

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

Off

RAS services are disabled.

### Client

The device works as a RAS client and dials-in to a server.

### Servers

The device works as a server. RAS clients can dial-in to it.

### Default:

Off

# **Rule creation**

Specifies how VPN rules are created.

#### **SNMP ID:**

2.19.36.1.11

### Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

# Auto

The device creates the VPN rules automatically.

## Manual

The device uses manually created rules.

#### Default:

Auto

# IPv4-Rules

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table Setup > VPN > Networks > IPv4-Rule-Lists.

### SNMP ID:

2.19.36.1.12

### Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

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

### Default:

empty

7 VPN

### **IPv6-Rules**

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table Setup > VPN > Networks > IPv6-Rule-Lists.

### SNMP ID:

2.19.36.1.13

### Telnet path:

Setup > VPN > IKEv2 > Peers

### Possible values:

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

### Default:

empty

### Comment

Enter a comment about this entry.

### SNMP ID:

2.19.36.1.17

### Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

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

# Default:

empty

# IPv4-CFG-Pool

Use this entry to specify an IPv4 address pool for the IKEv2 peer.

### SNMP ID:

2.19.36.1.18

### Telnet path:

Setup > VPN > IKEv2 > Peers

# Possible values:

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

# Default:

empty

# IPv6-CFG-Pool

Use this entry to specify an IPv6 address pool for the IKEv2 peer.

### SNMP ID:

2.19.36.1.19

# Telnet path:

Setup > VPN > IKEv2 > Peers

### **Possible values:**

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

# Encryption

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

### SNMP ID:

2.19.36.2

### Telnet path:

Setup > VPN > IKEv2

### Name

Contains the name of this configuration.

### SNMP ID:

2.19.36.2.1

# Telnet path:

Setup > VPN > IKEv2 > Encryption

### **Possible values:**

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

### Default:

DEFAULT

# **DH-Groups**

Contains the selection of Diffie-Hellman groups.

### SNMP ID:

2.19.36.2.2

Addendum

7 VPN

Telnet path: Setup > VPN > IKEv2 > Encryption

Possible values:

DH16 DH15 DH14 DH5 DH2

# Default:

DH14

# PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

## SNMP ID:

2.19.36.2.3

# Telnet path:

Setup > VPN > IKEv2 > Encryption

# Possible values:

Yes No

# Default:

Yes

# **IKE-SA cipher list**

Specifies which encryption algorithms are enabled.

# SNMP ID:

2.19.36.2.4

# Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

AES-CBC-256	
AES-CBC-192	
AES-CBC-128	
3DES	

# Default:

AES-CBC-256

# IKE-SA-Integ-Alg-List

Specifies which hash algorithms are enabled.

## SNMP ID:

2.19.36.2.5

# Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

SHA-512 SHA-384 SHA-256 SHA1 MD5

### Default:

SHA-256

SHA1

# Child-SA-Cipher-List

Specifies which encryption algorithms are enabled in the Child-SA.

### SNMP ID:

2.19.36.2.6

# Telnet path:

Setup > VPN > IKEv2 > Encryption

# 7 VPN

### **Possible values:**

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES

# Default:

AES-CBC-256

# Child-SA-Integ-Alg-List

Specifies which hash algorithms are enabled in the Child-SA.

# SNMP ID:

2.19.36.2.7

# Telnet path:

Setup > VPN > IKEv2 > Encryption

Possible values:

SHA-512 SHA-384 SHA-256 SHA1 MD5

### Default:

SHA-256

SHA1

# Auth

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

### SNMP ID:

2.19.36.3

# Telnet path:

Setup > VPN > IKEv2
## Parameter

Use this table to configure the local and a corresponding remote identity for the IKEv2 authentication.

### SNMP ID:

2.19.36.3.1

## Telnet path:

Setup > VPN > IKEv2 > Auth

## Name

Contains the name of this entry.

### SNMP ID:

2.19.36.3.1.1

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### **Possible values:**

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

## Default:

DEFAULT

# Local-Auth

Sets the authentication method for the local identity.

## SNMP ID:

2.19.36.3.1.2

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### **Possible values:**

RSA-Signature

Authentication by RSA signature.

## PSK

Authentication by pre-shared key (PSK).

# **Digital signature**

Use of configurable authentication methods with digital certificates as per RFC 7427.

## Default:

PSK

# Local-ID-Type

Displays the ID type of the local identity. The device interprets the entry under Local-ID accordingly.

## SNMP ID:

2.19.36.3.1.3

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

### No-Identity

The ID is the local gateway address.

(f) If this option is selected, the entry under **Local-ID** has no effect.

IPv4 address IPv6 address Domain name E-mail address Distinguished name Key ID

## Default:

E-mail address

# Local-ID

Contains the local identity. The significance of this entry depends on the setting under Local-ID-Type.

### SNMP ID:

2.19.36.3.1.4

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

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

## Default:

empty

# Local-Password

Contains the password of the local identity.

### SNMP ID:

2.19.36.3.1.5

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

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

## Default:

empty

# **Remote-Auth**

Sets the authentication method for the remote identity.

### SNMP ID:

2.19.36.3.1.6

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### **Possible values:**

## **RSA-Signature**

Authentication by RSA signature.

## PSK

Authentication by pre-shared key (PSK).

## **Digital signature**

Use of configurable authentication methods with digital certificates as per RFC 7427.

### Default:

PSK

# **Remote-ID-Type**

Displays the ID type of the remote identity. The device interprets the entry under Remote-ID accordingly.

### SNMP ID:

2.19.36.3.1.7

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### **Possible values:**

## No-Identity

The device accepts all connections from remote IDs.

(i) If this option is selected, the entry under **Remote-ID** has no effect.

IPv4 address IPv6 address Domain name E-mail address Distinguished name Key ID

## Default:

E-mail address

# **Remote-ID**

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

### SNMP ID:

2.19.36.3.1.8

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### **Possible values:**

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

## Default:

empty

# **Remote-Password**

Contains the password of the remote identity.

## SNMP ID:

2.19.36.3.1.9

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

### Possible values:

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

### Default:

empty

# Local-Certificate

Contains the local VPN certificate used by the device for outbound connections.

The corresponding VPN certificates "VPN1" to "VPN9" are configured under **Setup** > **Certificates** > **SCEP-Client** > **Certificates**.

# SNMP ID:

2.19.36.3.1.11

Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

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

### Default:

empty

# Remote-Cert-ID-Check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

## SNMP ID:

2.19.36.3.1.12

### Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

Yes

The device checks that the remote identity exists in the certificate.

## No

The device does not check that the remote identity exists in the certificate.

### Default:

Yes

# Local-Dig-Sig-Profile

Contains the profile name of the local digital signature profile being used.

## SNMP ID:

2.19.36.3.1.13

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## **Possible values:**

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

### Default:

empty

# **Remote-Dig-Sig-Profile**

Contains the profile name of the remote digital signature profile.

### SNMP ID:

2.19.36.3.1.14

## Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

## Possible values:

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

## Default:

empty

# **OCSP-Check**

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

### SNMP ID:

2.19.36.3.1.15

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

Possible values:

Yes No

## Default:

No

### General

Use this table to configure the general IKEv2 parameters.

## SNMP ID:

2.19.36.4

## Telnet path:

Setup > VPN > IKEv2

### Name

Contains the name of this entry.

#### SNMP ID:

2.19.36.4.1

### Telnet path:

Setup > VPN > IKEv2 > General

## **Possible values:**

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

# Default:

DEFAULT

## **DPD-Inact-Timeout**

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

### SNMP ID:

2.19.36.4.2

# Telnet path: Setup > VPN > IKEv2 > General

## **Possible values:**

Max. 4 characters from [0-9]

## Default:

30

## SSL-Encaps.

Specifies whether the connection uses IKEv2 over HTTPS.

### SNMP ID:

2.19.36.4.4

Telnet path: Setup > VPN > IKEv2 > General

## **Possible values:**

Yes No

....

# Default:

No

# IPCOMP

Specifies whether the devices transmit compressed IKEv2 data packets.

#### SNMP ID:

2.19.36.4.5

# Telnet path:

Setup > VPN > IKEv2 > General

# Possible values:

Yes No

# Default:

No

# Encaps-Mode

Specifies the mode of transmission.

# SNMP ID:

2.19.36.4.6

# Telnet path:

Setup > VPN > IKEv2 > General

## Possible values:

Tunnel

# Default:

Tunnel

# Lifetimes

Use this table to configure the lifetimes of the IKEv2 keys.

## SNMP ID:

2.19.36.5

# Telnet path:

Setup > VPN > IKEv2

## Name

Contains the name of this entry.

# SNMP ID:

2.19.36.5.1

## Telnet path:

Setup > VPN > IKEv2 > Lifetimes

### Possible values:

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

## Default:

DEFAULT

# IKE-SA-Sec

Contains the time in seconds until the IKE SA key is renewed.

## SNMP ID:

2.19.36.5.2

# Telnet path:

Setup > VPN > IKEv2 > Lifetimes

## **Possible values:**

Max. 10 characters from [0-9]

Default: 108000 Special values: 0 No key renewal.

# IKE-SA-KB

Contains the data volume in kilobytes until the IKE SA key is renewed.

## SNMP ID:

2.19.36.5.3

Telnet path: Setup > VPN > IKEv2 > Lifetimes

**Possible values:** 

Max. 10 characters from [0-9]

# Default:

0

## Special values:

0

No key renewal.

# Child-SA-Sec

Contains the time in seconds until the CHILD SA key is renewed.

# SNMP ID:

2.19.36.5.4

## Telnet path:

Setup > VPN > IKEv2 > Lifetimes

## **Possible values:**

Max. 10 characters from [0-9]

## Default:

28800

## Special values:

0

No key renewal.

### Child-SA-KB

Contains the data volume in kilobytes until the CHILD SA key is renewed.

### SNMP ID:

2.19.36.5.5

## Telnet path:

Setup > VPN > IKEv2 > Lifetimes

## **Possible values:**

Max. 10 characters from [0-9]

## Default:

2000000

### Special values:

0

No key renewal.

## IKE-CFG

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the IKE-CFG mode "Server" is specified for the entries in the connection list.

Use this menu to configure the address pool that the device in CFG mode "Server" passes to the clients.

### SNMP ID:

2.19.36.7

## Telnet path:

Setup > VPN > IKEv2

## IPv4

In this table, you configure the IPv4 addresses of the address pool for the IKEv2-CFG mode "Server".

### SNMP ID:

2.19.36.7.1

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG

### Name

Contains the name of the IPv4 address pool.

### SNMP ID:

2.19.36.7.1.1

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv4

## Possible values:

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

# Start-Address-Pool

Here you enter the first IPv4 address of the pool of addresses that you want to provide to dial-in clients.

#### **SNMP ID:**

2.19.36.7.1.2

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv4

## **Possible values:**

Max. 15 characters from [0-9]./

### Default:

empty

## **End-Address-Pool**

Here you enter the last IPv4 address of the pool of addresses that you want to provide to dial-in clients.

### SNMP ID:

2.19.36.7.1.3

### Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv4

# Possible values:

Max. 15 characters from [0-9]./

## Default:

empty

# **Primary-DNS**

Specify here the address of a name server to which DNS requests are to be forwarded.

### SNMP ID:

2.19.36.7.1.4

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv4

## Possible values:

Max. 15 characters from [0-9].

# Default:

0.0.0.0

# Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

### SNMP ID:

2.19.36.7.1.5

### Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv4

### **Possible values:**

Max. 15 characters from [0-9].

## Default:

empty

## IPv6

In this table, you configure the IPv6 addresses of the address pool for the IKEv2-CFG mode "Server".

### SNMP ID:

2.19.36.7.2

### Telnet path:

Setup > VPN > IKEv2 > IKE-CFG

# Name

Contains the name of the IPv6 address pool.

### SNMP ID:

2.19.36.7.2.1

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

## Possible values:

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

# Start-Address-Pool

Here you enter the first IPv6 address of the pool of addresses that you want to provide to dial-in clients.

### SNMP ID:

2.19.36.7.2.2

## Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

## **Possible values:**

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

# **End-Address-Pool**

Here you enter the last IPv6 address of the pool of addresses that you want to provide to dial-in clients.

### SNMP ID:

2.19.36.7.2.3

### Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

## **Possible values:**

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

# **Primary-DNS**

Specify here the address of a name server to which DNS requests are to be forwarded.

### SNMP ID:

2.19.36.7.2.4

### Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

## **Possible values:**

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

# Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

## SNMP ID:

2.19.36.7.2.5

Telnet path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

### **Possible values:**

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

# 7.2 IKEv2 fragmentation support

As of LCOS version 9.20, LCOS supports IKEv2 fragmentation.

# 7.2.1 IKEv2 fragmentation

The fragmentation of data packets is controlled by the maximum transmission unit (MTU). The MTU is the maximum size that a packet may have in order to be sent as payload over a channel. The two communication partners negotiate this during connection establishment in order to optimize data transmission by avoiding any additional fragmentation of the data packets.

In LCOS, IKEv2 fragmentation is enabled automatically. You can manually specify a maximum MTU if you wish.

To do this in LANconfig, go to VPN > IKEv2/IPSec.

Fragmentation		
MTU:	0	

Enter the maximum IP packet length/size in bytes into the **MTU** field in the **Fragmentation** section. Smaller values lead to greater fragmentation of the payload data.

# 7.2.2 Additions to the Setup menu

## MTU

This entry contains the maximum transmission unit (MTU) for IKEv2.

## SNMP ID:

2.19.36.8

Telnet path:

Setup > VPN > IKEv2

### **Possible values:**

Max. 5 characters from [0-9] 0...65535 Default: 0 Special values:

0

The MTU setting is disabled. The two IKEv2 endpoints negotiate the MTU between themselves.

# 7.3 RADIUS support for IKEv2

As of LCOS version 9.20, RADIUS supports the IKEv2 protocol for authorization and accounting.

# 7.3.1 RADIUS support for IKEv2

LCOS enables the configuration of IKEv2 for authorization and accounting of VPN peers to be performed by an external RADIUS server.

In medium- to large-scale VPN scenarios, the tables for VPN configurations are generally rather large and complex. If multiple VPN gateways are operated for redundancy, it is important to ensure that the configuration is identical on all VPN gateways.

Operating a central RADIUS server allows the configuration of the VPN parameters on the VPN gateways to be almost completely outsourced to one or more RADIUS servers. When a device receives an incoming connection from a VPN peer, the device attempts to authenticate the incoming connection via RADIUS and to retrieve other necessary connection parameters, such as VPN network relationships, CFG-mode address or DNS server, from the RADIUS server.

The VPN configuration may be either completely or only partially retrieved from the RADIUS server, in which case it is combined with parameters stored locally. This mechanism works for incoming connections only.

Optional RADIUS accounting allows information about VPN connections to be stored centrally on a RADIUS server. This information may consist of the duration of the connection to the client, the time when the connection is established, or the transmitted data volume.

The RADIUS server is configured in LANconfig under VPN > IKEv2/IPSec > Extended settings.

# **RADIUS** authorization

When authenticating a VPN peer, the LANCOM gateway transmits the following RADIUS attributes to the RADIUS server in the Access-Request:

ID :	Name	Meaning
1	User name	The remote ID of the VPN peers sent in the AUTH negotiation with the LANCOM gateway.
2	User-Password	The dummy password as configured in LANconfig under <b>VPN</b> > <b>IKEv2/IPSec</b> > <b>Extended settings</b> > <b>Password</b> .
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute "95" instead (see below).
6	Service type	The service type is always "Outbound (5)" or "Dialout-Framed-User".
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).

ID :	Name	Meaning
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv4 connection, the gateway transmits the attribute "4" instead (see above).

Of the attributes contained in the Access-Accept response from the RADIUS server, the LANCOM gateway evaluates the following, in part vendor-specific attributes:

ID :	Name	Meaning	
8	Framed-IP-Address	IPv4 address for the client (in IKE CFG-mode "Server").	
22	Framed-Route	IPv4 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client).	
39	Tunnel-Password	Sets the passwords on the local and remote identity to the same value when using synchronous PSKs.	
88	Framed-Pool	Name of the IPv4 address pool from which the client retrieves its IP address and the DNS server.	
		The values in "Framed-IP-Address" and "LCS-DNS-Server-IPv4-Address" take precedence over this attribute.	
99	Framed-IPv6-Route	IPv6 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client).	
168	Framed-IPv6-Address	IPv6 address for the client (in IKE CFG-mode "Server").	
169	DNS-Server-IPv6-Address	IPv6 DNS server for the client (in IKE CFG-mode "Server").	
172	Stateful-IPv6-Address-Pool	Name of the IPv6 address pool (in IKE CFG-mode "Server").	
Lancom 19	LCS-IKEv2-Local-Password	Local IKEv2 PSK	
Lancom 20	LCS-IKEv2-Remote-Password	Remote IKEv2 PSK	
Lancom 21	LCS-DNS-Server-IPv4-Address	IPv4 DNS server for the client (in IKE CFG-mode "Server").	
Lancom 22	LCS-VPN-IPv4-Rule	Contains the IPv4 network rules (examples below)	
Lancom 23	LCS-VPN-IPv6-Rule	Contains the IPv6 network rules (examples below)	
Lancom 24	LCS-Routing-Tag	Routing tag to be configured for the client (IPv4/IPv6).	
Lancom 25	LCS-IKEv2-IPv4-Route	Routes in prefix notation (e.g. "192.168.1.0/24") that the LANCOM gateway transfers to the client via INTERNAL_IP4_SUBNET. Multiple attributes can be analyzed.	
Lancom 26	LCS-IKEv2-IPv6-Route	Routes in prefix notation (e.g. "2001:db8::/64") that the LANCOM gateway transfers to the client via INTERNAL_IP6_SUBNET. Multiple attributes can be analyzed.	

## **Examples of network rules**

The format for a network rule on the RADIUS server takes the form <local networks> \* <remote networks>.

The entries for <local networks> and <remote networks> are comma-separated lists.

# Example 1: 10.1.1.0/24,10.2.0.0/16 \* 172.32.0.0/12

The result is the following network rules:

```
10.2.0.0/255.255.0.0 <-> 172.16.200.0/255.255.255.255
10.1.1.0/255.255.255.0 <-> 172.16.200.0/255.255.255.255
```

## Example 2: 10.1.1.0/24 \* 0.0.0.0/0

This results in the following network rule:

10.1.1.0/255.255.255.0 <-> 0.0.0.0/0.0.0.0

Here, 0.0.0.0/0 means "ANY", i.e. any network. 0.0.0/32 can be used to restrict a CFG-mode client to its own (as yet unknown) config-mode address. This address could come from an address pool on the device or from the RADIUS server.

# Example 3: 2001:db8:1::/48 \* 2001:db8:6::/48

### **RADIUS** accounting

The LANCOM gateway counts the transmitted data packets and octets and sends this information as regular Accounting-Request messages to the RADIUS accounting server. The RADIUS server answers this message with an Accounting-Response message.

The Accounting-Request messages have the following status types:

### Home

As soon as a VPN peer contacts the LANCOM gateway, the gateway starts an accounting session via IKEv2 and sends a Start status message with the appropriate RADIUS attributes to the RADIUS accounting server.

## Interim-Update

During an ongoing accounting session, the gateway sends Interim-Update status messages at specified time intervals to that RADIUS accounting server, which gave a valid response to the Start status message. The gateway ignores any backup servers that may have been configured.

## Stop

After the end of a session, the LANCOM gateway sends a Stop status message to the RADIUS accounting server. This message is also sent only to that RADIUS accounting server, which gave a valid response to the Start status message. The gateway ignores any backup servers that may have been configured.

ID :	Name	Meaning	Status-Type
1	User name	The remote ID of the VPN peers sent in the AUTH negotiation with the LANCOM gateway.	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute "95" instead (see below).	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
8	Framed-IP-Address	IP4 address of the VPN client.	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
32	NAS identifier	The device name of the gateway.	<ul> <li>Home</li> </ul>

In the Access-Request message, the gateway transmits the following RADIUS attributes to the RADIUS server:

ID :	Name	Meaning	Status-Type
			Interim-Update
			<ul> <li>Stop</li> </ul>
40	Acct-Status-Type	Contains the status type "Start" (1).	<ul> <li>Home</li> </ul>
40	Acct-Status-Type	Contains the status type "Interim-Update" (3).	<ul> <li>Interim-Update</li> </ul>
40	Acct-Status-Type	Contains the status type "Stop" (2).	<ul> <li>Stop</li> </ul>
42	Acct-Input-Octets	Contains the number of octets received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	<ul><li>Interim-Update</li><li>Stop</li></ul>
43	Acct-Output-Octets	Contains the number of octets sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	<ul><li>Interim-Update</li><li>Stop</li></ul>
44	Acct-Session-Id	The name of the VPN peer and the timestamp at the start of the session form the unique session ID.	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
46	Acct-Session-Time	Contains the elapsed time in seconds since the start of the session.	<ul><li>Interim-Update</li><li>Stop</li></ul>
47	Acct-Input-Packets	Contains the current number of data packets received from the direction of the VPN peer.	<ul><li>Interim-Update</li><li>Stop</li></ul>
48	Acct-Output-Packets	Contains the current number of data packets sent to the VPN peer.	<ul><li>Interim-Update</li><li>Stop</li></ul>
49	Acct-Terminate-Cause	Contains the reason for terminating the session.	<ul> <li>Stop</li> </ul>
52	Acct-Input-Gigawords	Contains the number of gigawords received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	<ul><li>Interim-Update</li><li>Stop</li></ul>
53	Acct-Input-Gigawords	Contains the number of gigawords sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	<ul><li>Interim-Update</li><li>Stop</li></ul>
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute "4" instead (see above).	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>
168	Framed-IPv6-Address	IP6 address of the VPN client.	<ul><li>Home</li><li>Interim-Update</li><li>Stop</li></ul>

# **RADIUS** authentication

In the **RADIUS authentication** section you configure the settings for the RADIUS server used for VPN client authentication.

In the **Password** field you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the LANCOM gateway after this receives the corresponding authorization in the access-accept message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

Just click on RADIUS server to open the configuration dialog of the RADIUS server.

RADIUS server - New Entry	/	? <mark>×</mark>
Name:		]
Server address:		
Port:	1.812	
Secret:		Show
	Generate password 🖛	
Protocols:	RADIUS -	]
Source address (opt.):	-	Select
Attribute values:		
Backup profile:	-	Select
	ОК	Cancel

### Name

Specify an identifier for this entry.

# Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Server address

## Port

Specify the UDP port of the RADIUS server. The value "1812" is preset as the default value.

## Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.



Confirm the secret by entering it again into the field that follows.

### Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

### Source address (optional)

Enter the loopback address of the device, where applicable.

### Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <a href="https://www.commons.com">https://www.commons.com</a> <a href="https://www.commons.com">com</a> <a href="https://www.commons.com"/>com</a> <a href="https://www.com"/>com</a> <a href="https://www.commons.com"/>com</a> <a href="https://www.commons.com"/>com</a> <a href="https://www.commons.com"/>com</a> <a href="https://www.com"/>com</a

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

Addendum

7 VPN

The following variables are permitted as values:

%n

Device name

%**e** 

Serial number of the device

%%

Percent sign

## %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

## Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPSec** > **Connection list** in the **RADIUS auth. server** field.

# **RADIUS** accounting

In the RADIUS accounting section you configure the settings for the RADIUS server used for VPN client accounting.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.

The **Update cycle** field is used to set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of  $\pm 10\%$  to keep the update messages of parallel accounting sessions separate from one another.

Just click on RADIUS server to open the configuration dialog of the RADIUS server.

RADIUS server - New Entr	у	? <b>X</b>
Name:		]
Server address:		
Port:	1.813	
Secret:		Show
	Generate password 🖛	
Protocols:	RADIUS -	]
Source address (opt.):	•	Select
Attribute values:		
Backup profile:	-	Select
	OK	Cancel

## Name

Specify an identifier for this entry.

# Server address

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

## Port

Specify the UDP port of the RADIUS server. The value "1813" is preset as the default value.

### Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.



Confirm the secret by entering it again into the field that follows.

### Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

### Source address (optional)

Enter the loopback address of the device, where applicable.

### Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <Attribute\_1>=<Value\_1>;<Attribute\_2>=<Value\_2>.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

#### %n

Device name

%e

Serial number of the device

88

Percent sign

## %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

## **Backup profile**

From the list of RADIUS server profiles, select a profile as the backup server.

The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPSec** > **Connection list** in the **RADIUS acc. server** field.

# 7.3.2 Additions to the Setup menu

# **RADIUS** authorization

Here you specify the RADIUS server that performs the authorization.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**.

(f) If you do not specify a RADIUS server for authorization, the device uses the local IKEv2 configuration.

### SNMP ID:

2.19.36.1.15

### Telnet path:

Setup > VPN > IKEv2 > Peers

#### **Possible values:**

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

## Default:

empty

# **RADIUS** accounting

Use this entry to specify the RADIUS server that is to be used for the accounting.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

(f) If you do not specify a RADIUS server, no accounting takes place for this VPN peer.

### SNMP ID:

2.19.36.1.16

## Telnet path:

Setup > VPN > IKEv2 > Peers

## **Possible values:**

Max. 31 characters from  $[A-Z][0-9]@{|} \sim !$ 

### Default:

empty

## RADIUS

This menu contains the RADIUS configuration for IKEv2.

#### SNMP ID:

2.19.36.9

# Telnet path:

Setup > VPN > IKEv2

## Authorization

This menu contains the configuration for the RADIUS authorization via IKEv2.

## SNMP ID:

2.19.36.9.1

## Telnet path:

Setup > VPN > IKEv2 > RADIUS

## Servers

This table contains the server configuration for the RADIUS authorization under IKEv2.

## SNMP ID:

2.19.36.9.1.1

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization

# Name

Specify an identifier for this entry.

# SNMP ID:

2.19.36.9.1.1.1

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

## Possible values:

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

# Default:

empty

# Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

### SNMP ID:

2.19.36.9.1.1.2

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

### **Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-:%

## Default:

empty

# Port

Specify the UDP port of the RADIUS server.

## SNMP ID:

2.19.36.9.1.1.3

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

## **Possible values:**

Max. 5 characters from [0-9]

## Default:

1812

# Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

() Confirm the secret by entering it again into the field that follows.

# SNMP ID:

2.19.36.9.1.1.4

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

## Possible values:

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

### Default:

empty

# Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

### SNMP ID:

2.19.36.9.1.1.6

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

## Possible values:

RADIUS RADSEC

## Default:

RADIUS

# Loopback address

This entry contains the loopback address of the LANCOM gateway that sent the request to the RADIUS server.

## SNMP ID:

2.19.36.9.1.1.7

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

### **Possible values:**

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

## Default:

empty

# **Attribute-Values**

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <Attribute\_1>=<Value\_1>;<Attribute\_2>=<Value\_2>.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

### %n

Device name

## %**e**

Serial number of the device

## 88

Percent sign

## %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

### SNMP ID:

2.19.36.9.1.1.8

### **Telnet path:**

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

### **Possible values:**

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

### Default:

empty

## Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

### SNMP ID:

2.19.36.9.1.1.9

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

### **Possible values:**

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

### Default:

empty

## Password

Here you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the LANCOM gateway after this receives the corresponding authorization in the access-accept message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

### SNMP ID:

2.19.36.9.1.2

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Authorization

## Possible values:

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

## Default:

empty

## Accounting

This menu contains the configuration for the RADIUS accounting via IKEv2.

## SNMP ID:

2.19.36.9.2

### Telnet path:

Setup > VPN > IKEv2 > RADIUS

### Server

This table contains the server configuration for the RADIUS accounting under IKEv2.

### SNMP ID:

2.19.36.9.2.1

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting

## Name

Specify an identifier for this entry.

### SNMP ID:

2.19.36.9.2.1.1

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## **Possible values:**

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

## Default:

empty

# Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

### SNMP ID:

2.19.36.9.2.1.2

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## **Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-:%

## Default:

empty

# Port

Specify the UDP port of the RADIUS server.

### SNMP ID:

2.19.36.9.2.1.3

# Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## **Possible values:**

Max. 5 characters from [0-9]

## Default:

1813

## Secret

This entry contains the shared secret used to authorize the LANCOM gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

### SNMP ID:

2.19.36.9.2.1.4

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## **Possible values:**

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

#### Default:

empty

## Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

### SNMP ID:

2.19.36.9.2.1.5

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

Possible values:

RADIUS RADSEC

Default:

RADIUS

# Loopback address

This entry contains the loopback address of the LANCOM gateway that sent the request to the RADIUS server.

### SNMP ID:

2.19.36.9.2.1.6

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## Possible values:

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

Default:

empty

# **Attribute-Values**

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <Attribute\_1>=<Value\_1>;<Attribute\_2>=<Value\_2>.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

%n

Device name

# %**e**

Serial number of the device

## %%

Percent sign

# %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

## SNMP ID:

2.19.36.9.2.1.7

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

### Possible values:

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

### Default:

empty

# Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

## SNMP ID:

2.19.36.9.2.1.8

## Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting > Server

## Possible values:

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

### Default:

empty

## Interim-Interval

Set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of  $\pm 10\%$  to keep the update messages of parallel accounting sessions separate from one another.

### SNMP ID:

2.19.36.9.2.2

### Telnet path:

Setup > VPN > IKEv2 > RADIUS > Accounting

### **Possible values:**

Max. 10 characters from [0-9] 0... 4294967295

### Default:

0

#### **Special values:**

0

The transmission of interim-update messages is disabled.

## Create-Routes-For-RAS-SAs

Specifies whether routes should be generated automatically from the VPN rules for dial-in (RAS) clients operating as CFG-mode servers. Disabling automatic route generation is useful when the routes are to be created by means of a routing protocol.

### SNMP ID:

2.19.36.10

## Telnet path:

Setup > VPN > IKEv2

# Possible values:

No

No routes are generated for RAS SAs.

Yes

Routes are generated for RAS SAs.

# Default:

Yes

# **Extended parameters**

This table contains extended parameters for IKEv2 remote stations.

## SNMP ID:

2.19.36.11

## Telnet path:

Setup > VPN > IKEv2

# Name

Name of the remote device.

## SNMP ID:

2.19.36.11.1

## Telnet path:

Setup > VPN > IKEv2 > Extended-Parameters

## **Possible values:**

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

## Default:

empty

## **PRF-as-Sig-Hash**

Specifies whether to use the PRF (pseudo-random function) of the IKEv2 negotiation as a signature hash with the RSA signature. This function should be used for compatibility with third-party products only. The setting must be configured identically at both ends of the VPN connection.

# SNMP ID:

2.19.36.11.2

Telnet path:

Setup > VPN > IKEv2 > Extended-Parameters

Possible values:

Yes No

Default:

No

# 7.3.3 Additions to the Status menu

# RADIUS

This menu contains status values for all of the current VPN peers being managed by a RADIUS server (authorization and accounting).

### SNMP ID:

1.26.39

Telnet path:

Status > VPN

### Authorization

This directory contains the status values for all of the current VPN peers that were authorized by a RADIUS server.

A new VPN peer appears in this table after the first access request at a RADIUS server. The entry for a VPN peer is removed from the table as soon as its IKE SA (phase 1) is deleted.

## SNMP ID:

1.26.39.1

## Telnet path:

Status > VPN > RADIUS

## Peer

This entry shows the name of the remote station.

## SNMP ID:

1.26.39.1.1

Telnet path:

Status > VPN > RADIUS > Authorization

### Remote-ID

This entry shows the remote ID of the VPN peer as forwarded by the device to the RADIUS server.

#### SNMP ID:

1.26.39.1.2

## Telnet path:

Status > VPN > RADIUS > Authorization

## Local-Gateway

This entry contains the IPv4 or IPv6 address of the LANCOM gateway that the VPN peer sent its VPN request to. The LANCOM gateway transmits this address as the RADIUS attribute "NAS-IP-Address" or "NAS-IPv6-Address" in the access request sent to the RADIUS server.

### SNMP ID:

1.26.39.1.3

## Telnet path:

Status > VPN > RADIUS > Authorization

## **Remote gateway**

This entry contains the IPv4 or IPv6 address from which the VPN peer sent its VPN request to the LANCOM gateway. The LANCOM gateway transmits this address as the RADIUS attribute "Calling-Station-Id" in the access request sent to the RADIUS server.

## SNMP ID:

1.26.39.1.4

#### Telnet path:

Status > VPN > RADIUS > Authorization

### State

Displays the status of the VPN peer. The following states are possible:

### Running

The "Access-Request" was sent to the RADIUS server but there was no response yet.

### Succeeded

The "Access-Accept" message was received from the RADIUS server.

# Failed

The "Access-Request" to the RADIUS server or the configured backup RADIUS server failed.

### SNMP ID:

1.26.39.1.5

### Telnet path:

Status > VPN > RADIUS > Authorization

## Server-Hostname

Displays the host name of the requested RADIUS server if this has answered a request. The entry corresponds to the configuration under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**.

### SNMP ID:

1.26.39.1.6

### Telnet path:

Status > VPN > RADIUS > Authorization

## CFG-IPv4-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IP-Address". If the RADIUS server does not return a value, this entry remains blank.

# SNMP ID:

1.26.39.1.7

Telnet path:

Status > VPN > RADIUS > Authorization

### CFG-IPv4-DNS-Server

Displays a comma-separated list of IPv4 DNS servers reported by the RADIUS server in the vendor-specific RADIUS attribute "LCS-DNS-Server-IPv4-Address". This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

#### SNMP ID:

1.26.39.1.8
Telnet path:

Status > VPN > RADIUS > Authorization

#### CFG-IPv4-Pool

Displays the framed IPv4 address pool reported by the RADIUS server. If the RADIUS server does not return a value, this entry remains blank.

#### SNMP ID:

1.26.39.1.9

## Telnet path:

Status > VPN > RADIUS > Authorization

## CFG-IPv6-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IPv6-Address". If the RADIUS server does not return a value, this entry remains blank.

## SNMP ID:

1.26.39.1.10

## Telnet path:

Status > VPN > RADIUS > Authorization

# CFG-IPv6-DNS-Server

Displays a comma-separated list of IPv6 DNS servers reported by the RADIUS server in the vendor-specific RADIUS attribute "LCS-DNS-Server-IPv6-Address". This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

## SNMP ID:

1.26.39.1.11

## Telnet path:

Status > VPN > RADIUS > Authorization

## CFG-IPv6-Pool

Displays the framed IPv6 address pool reported by the RADIUS server. If the RADIUS server does not return a value, this entry remains blank.

#### SNMP ID:

1.26.39.1.12

## Telnet path:

Status > VPN > RADIUS > Authorization

## **Rtg-Tag**

This entry contains the IPv4 or IPv6 routing tag reported by the RADIUS server in the "Access-Accept" message (with the vendor-specific RADIUS attribute "LCS-Routing-Tag").

#### SNMP ID:

1.26.39.1.13

## Telnet path:

Status > VPN > RADIUS > Authorization

## Framed-IPv4-Routes

This entry contains a comma-separated list of IPv4 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the RADIUS attribute "Framed-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

## SNMP ID:

1.26.39.1.14

#### Telnet path:

Status > VPN > RADIUS > Authorization

## Framed-IPv6-Routes

This entry contains a comma-separated list of IPv6 prefixes reported by the RADIUS server in the "Access-Accept" message in the RADIUS attribute "Framed-IPv6-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

#### SNMP ID:

1.26.39.1.15

Telnet path:

Status > VPN > RADIUS > Authorization

## **IKE-IPv4-Routes**

This entry contains a comma-separated list of IPv4 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the vendor-specific RADIUS attribute "LCS-IKEv2-IPv4-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

#### SNMP ID:

1.26.39.1.16

## Telnet path:

Status > VPN > RADIUS > Authorization

### **IKE-IPv6-Routes**

This entry contains a comma-separated list of IPv6 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the vendor-specific RADIUS attribute "LCS-IKEv2-IPv6-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

## SNMP ID:

1.26.39.1.17

## Telnet path:

Status > VPN > RADIUS > Authorization

# **Other attributes**

This entry contains a comma-separated or space-separated list of additional attributes transferred by the RADIUS server in the "Access-Accept" message.

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

Possible values are:

#### Local password

The content of the attributes "LCS-IKEv2-Local-Password" or "Tunnel-Password".

## **Remote password**

The content of the attributes "LCS-IKEv2-Remote-Password" or "Tunnel-Password".

## IPv4-Rule

Content of the attribute "LCS-VPN-IPv4-Rule".

## IPv6-Rule

Content of the attribute "LCS-VPN-IPv6-Rule".

# SNMP ID:

1.26.39.1.18

## Telnet path:

Status > VPN > RADIUS > Authorization

## Accounting

This directory contains the status values for all of the current VPN peers whose accounting is handled by a RADIUS server.

# SNMP ID:

1.26.39.2

## Telnet path:

Status > VPN > RADIUS

## Peer

This entry shows the name of the remote station.

#### SNMP ID:

1.26.39.2.1

## Telnet path:

Status > VPN > RADIUS > Accounting

## Session-ID

The name of the VPN peer and the timestamp at the start of the session form the unique session ID.

#### SNMP ID:

1.26.39.2.2

#### Telnet path:

Status > VPN > RADIUS > Accounting

## **Remote-ID**

This entry shows the remote ID of the VPN peer as forwarded by the device to the RADIUS server.

## SNMP ID:

1.26.39.2.3

# Telnet path:

Status > VPN > RADIUS > Accounting

## Local-Gateway

This entry contains the IPv4 or IPv6 address of the LANCOM gateway that the VPN peer sent its VPN request to. The LANCOM gateway transmits this address as the RADIUS attribute "NAS-IP-Address" or "NAS-IPv6-Address" in the access request sent to the RADIUS server.

#### SNMP ID:

1.26.39.2.4

# Telnet path:

Status > VPN > RADIUS > Accounting

## **Remote gateway**

This entry contains the IPv4 or IPv6 address from which the VPN peer sent its VPN request to the LANCOM gateway. The LANCOM gateway transmits this address as the RADIUS attribute "Calling-Station-Id" in the access request sent to the RADIUS server.

## SNMP ID:

1.26.39.2.5

## Telnet path:

Status > VPN > RADIUS > Accounting

# CFG-IPv4-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IP-Address". If the RADIUS server does not return a value, this entry remains blank.

## SNMP ID:

1.26.39.2.6

Telnet path:

Status > VPN > RADIUS > Accounting

#### CFG-IPv6-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IPv6-Address". If the RADIUS server does not return a value, this entry remains blank.

## SNMP ID:

1.26.39.2.7

## Telnet path:

Status > VPN > RADIUS > Accounting

# State

Displays the status of the VPN peer. The following states are possible:

## Starting

There was no "Accounting-Response" message from the RADIUS server.

## Start-Failed

IKE did not transfer a valid "Start" message, or the VPN peer did not receive a valid "Accounting-Response" message from the RADIUS server.

## Running

The VPN peer received a valid "Accounting-Response" message and the last interim update was successful.

# **Update-Failed**

The last interim update was not successful.

## SNMP ID:

1.26.39.2.8

## Telnet path:

Status > VPN > RADIUS > Accounting

# Server host name

Displays the host name of the requested RADIUS server if this has answered a request. The entry corresponds to the configuration under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

#### SNMP ID:

1.26.39.2.9

## Telnet path:

Status > VPN > RADIUS > Accounting

# Session-Time

Displays the elapsed time in seconds since the start of the session.

## SNMP ID:

1.26.39.2.10

# Telnet path:

Status > VPN > RADIUS > Accounting

# Input-Octets

Shows the number of octets received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.

## SNMP ID:

1.26.39.2.11

# Telnet path:

Status > VPN > RADIUS > Accounting

# **Output-Octets**

Shows the number of octets sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.

### SNMP ID:

1.26.39.2.12

# Telnet path:

Status > VPN > RADIUS > Accounting

# Input-Packets

Shows the current number of data packets received from the direction of the VPN peer.

## SNMP ID:

1.26.39.2.13

## Telnet path:

Status > VPN > RADIUS > Accounting

# **Output-Packets**

Shows the current number of data packets sent to the VPN peer.

# SNMP ID:

1.26.39.2.14

# Telnet path:

Status > VPN > RADIUS > Accounting

# 7.4 IKEv2 routing support

As of version 9.20, LCOS supports the following functions for IKEv2-Config-Exchange

- CFG\_Request
- CFG\_Reply
- CFG\_Set
- CFG\_Ack

Configuring the prefixes for dynamic routing via IKEv2 in LANconfig is done under VPN > IKEv2/IPSec > Extended settings in the IKEv2 routing section.

# 7.4.1 IPv4 routing

IKEv2 routing uses an IKEv2 tunnel to propagate local networks or to learn about remote networks.

# 7.4.2 IPv6 routing

Use this table to configure the IPv6 networks that the device propagates via dynamic routing as per IKEv2.

IPv6 routing - New Entry	? 💌
Name:	Select
Send IKE-CFG-Address	
	OK Cancel

## Name

Contains the unique name of this entry.

# Network

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 interface name

The IP subnets are configured under IPv6 > General in the section IPv6 networks.

# Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

 $(\mathbf{I})$ 

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

# 7.4.3 Additions to the Setup menu

# Routing

Specifies the route used for the VPN connection.

The routes for IPv4 and IPv6 connections are located in the menu Setup > VPN > IKEv2 > Routing.

# SNMP ID:

2.19.36.1.14

# **Telnet path:**

Setup > VPN > IKEv2 > Peers

## **Possible values:**

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

## Default:

empty

# Routing

Use this menu to configure the routing table for the IKEv2 routing.

The routing tables specify IPv4/IPv6 routes used by the VPN connections if there is no corresponding route in the IPv4/IPv6 router.

# SNMP ID:

2.19.36.6

# Telnet path:

Setup > VPN > IKEv2

# IPv4

Use this table to configure the IPv4 tables for the IKEv2 routing.

## SNMP ID:

2.19.36.6.1

# Telnet path:

Setup > VPN > IKEv2 > Routing

# Name

Contains the name of this entry.

## SNMP ID:

2.19.36.6.1.1

# Telnet path:

Setup > VPN > IKEv2 > Routing > IPv4

# **Possible values:**

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

# Default:

DEFAULT

## Networks

Contains the comma-separated list of IPv4 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

# SNMP ID:

2.19.36.6.1.2

# Telnet path:

Setup > VPN > IKEv2 > Routing > IPv4

## **Possible values:**

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

# Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

## SNMP ID:

2.19.36.6.1.3

# Telnet path:

Setup > VPN > IKEv2 > Routing > IPv4

# **Possible values:**

No

The IPv4 address is not sent

Yes

The IPv4 address will be sent

# Default:

Yes

# IPv6

Use this table to configure the IPv6 tables for the IKEv2 routing.

# SNMP ID:

2.19.36.6.2

# Telnet path:

Setup > VPN > IKEv2 > Routing

## Name

Contains the name of this entry.

#### SNMP ID:

2.19.36.6.2.1

## Telnet path:

Setup > VPN > IKEv2 > Routing > IPv6

## **Possible values:**

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

## Default:

DEFAULT

## Networks

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

# SNMP ID:

2.19.36.6.2.2

## Telnet path:

Setup > VPN > IKEv2 > Routing > IPv6

## Possible values:

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

## Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. LANCOM routers generate the necessary routes automatically.

#### SNMP ID:

2.19.36.6.2.3

## Telnet path:

Setup > VPN > IKEv2 > Routing > IPv6

Possible values: No The IPv6 address is not sent Yes The IPv6 address will be sent

# Default:

Yes

# 7.5 "Match Remote Identity" for IKEv2

LCOS as of version 9.20 supports the configuration of multiple remote identities for IKEv2 connections. These identities can then be allocated to a VPN remote station.

The additional remote identities are configured in LANconfig under VPN > IKEv2/IPSec > Extended settings in the Authentication section.

The allocation of an additional remote identity to a VPN connection is done under VPN > IKEv2/IPSec > Authentication in the Additional remote identities section.

# 7.5.1 Identity list

Use this table to collect other remote identities into a group.

Identity list - New Entry		? 🗙
Name: Identities:		Select
	OK	Cancel

# Name

Contains the unique name of this entry.

# Identity

Lists the other identities that are collected into this group. Configure the identities under Identities.

# 7.5.2 Identities

Use this table to configure additional remote identities. You select this name when grouping remote identities in the **Identity list**.

Identities - New Entry	? 💌
Name:	
Remote authentication:	RSA signature 🔻
Remote identifier type:	No identity 🔹
Remote identifier:	
Remote password:	Show
	Generate password 💌
Remote certificate check:	No
	OK Cancel

### Name

Contains the unique name of this entry.

# **Remote authentication**

Sets the authentication method for the remote identity.

## **Remote identifier type**

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under "Remote identifier" accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the "Remote identifier" field.
- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as the remote ID.
- Key ID (group name): The device expects the group name as the remote ID.

## **Remote identifier**

Contains the remote identity. The significance of this entry depends on the setting under "Remote identifier type".

## **Remote password**

Contains the password of the remote identity.

## Remote certificate check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

# 7.5.3 Additions to the Setup menu

# Addit.-Remote-ID-List

Contains additional remote identities as specified in the table Setup > VPN > IKEv2 > Auth > Addit.-Remote-ID-List.

#### SNMP ID:

2.19.36.3.1.10

# Telnet path:

Setup > VPN > IKEv2 > Auth > Parameter

# Possible values:

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

## Default:

empty

# Addit.-Remote-ID-List

Use this table to configure lists of additional remote identities.

## SNMP ID:

2.19.36.3.2

# Telnet path:

Setup > VPN > IKEv2 > Auth

# Name

Sets the name of the ID list.

## SNMP ID:

2.19.36.3.2.1

#### Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-ID-List

## **Possible values:**

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

# Default:

empty

## Addit.-Remote-IDs

Contains the remote identities that you want to collect into this list. The IDs are located in the table Addit.-Remote-IDs.

Specify several IDs by separating them with a space character.

## SNMP ID:

2.19.36.3.2.2

## Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-ID-List

# **Possible values:**

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

## Default:

empty

# Addit.-Remote-IDs

Use this table to configure additional remote identities.

#### SNMP ID:

2.19.36.3.3

# Telnet path:

Setup > VPN > IKEv2 > Auth

# Name

Contains the name of this remote identity.

#### SNMP ID:

2.19.36.3.3.1

## Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

#### **Possible values:**

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

## Default:

empty

## **Remote-Auth**

Sets the authentication method for the remote identity.

## SNMP ID:

2.19.36.3.3.2

## Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

## **Possible values:**

# **RSA-Signature**

Authentication by RSA signature.

# PSK

Authentication by pre-shared key (PSK).

# **Digital signature**

Use of configurable authentication methods with digital certificates as per RFC 7427.

#### Default:

PSK

## **Remote-ID-Type**

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

### SNMP ID:

2.19.36.3.3.3

# Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

## **Possible values:**

#### **No-Identity**

The device accepts all connections from remote IDs. IPv4 address IPv6 address Domain name E-mail address Distinguished name Key ID

### Default:

E-mail address

# **Remote-ID**

Contains the remote identity. The significance of this entry depends on the setting under Remote-ID-Type.

# SNMP ID:

2.19.36.3.3.4

# Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

## **Possible values:**

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

## Default:

empty

# **Remote-Password**

Contains the password of the remote identity.

## SNMP ID:

2.19.36.3.3.5

# Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

## **Possible values:**

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

# Default:

empty

# Remote-Cert-ID-Check

This function checks whether the specified remote ID is also included in the certificate that was used by the peer to establish the connection.

## SNMP ID:

2.19.36.3.3.6

# Telnet path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

**Possible values:** 

Yes No

## Default:

Yes

# **Digital-Signature-Profiles**

Use this table to configure the profiles of the digital signature.

#### **SNMP ID:**

2.19.36.3.4

# Telnet path:

Setup > VPN > IKEv2

# Name

Name of the profile.

#### SNMP ID:

2.19.36.3.4.1

## Telnet path:

Setup > VPN > IKEv2 > Digital-Signature-Profiles

# **Possible values:**

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

# Default:

DEFAULT

# **Auth-Method**

Sets the authentication method for the digital signature.

## SNMP ID:

2.19.36.3.4.2

# Telnet path:

Setup > VPN > IKEv2 > Digital-Signature-Profiles

# **Possible values:**

RSASSA-PSS RSASSA-PKCS1-v1\_5

## Default:

**RSASSA-PSS** 

# Hash algorithms

Sets the hash algorithms for the digital signature.

### SNMP ID:

2.19.36.3.4.3

# Telnet path:

Setup > VPN > IKEv2 > Digital-Signature-Profiles

# Possible values:

SHA-512, SHA-384, SHA-256, SHA1

## Default:

SHA-512, SHA-384, SHA-256, SHA1

# 7.6 Redirect mechanism for IKEv2

As of LCOS version 9.20, LCOS supports the redirect mechanism as per RFC 5685 for VPN connections that use IKEv2. This is initially supported as a client only. This allows an IKEv2 server to redirect a client to a different gateway.

# 7.6.1 Additions to the Setup menu

# 7.7 VPN via IPv6 connections with IKEv1

As of LCOS version 9.20, current VPN devices support IKEv1 for VPN connections over IPv6.

# 7.7.1 Additions to the Setup menu

# 7.8 VPN network rules for IPv4 and IPv6

As of LCOS version 9.20, current VPN devices allow the flexible configuration of network rules for VPN connections over IPv4 and IPv6.

# 7.8.1 Additions to the Setup menu

# Networks

In this directory, you configure the VPN network rules for IPv4 and IPv6 connections.

SNMP ID:

2.19.35

Telnet path: Setup > VPN

## **IPv4-Rules**

In this table, you configure the VPN network rules for IPv4 connections.

# SNMP ID:

2.19.35.1

## Telnet path:

Setup > VPN > Networks

## Name

Contains the name of this rule.

#### SNMP ID:

2.19.35.1.1

#### Telnet path:

Setup > VPN > Networks > IPv4-Rules

## **Possible values:**

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

# Default:

empty

## Local-Networks

Contains the local networks to which this rule applies.

The following entries are valid:

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

(f) Specify multiple networks by separating them with a space character.

# SNMP ID:

```
2.19.35.1.2
```

Telnet path:

Setup > VPN > Networks > IPv4-Rules

## Possible values:

```
Max. 127 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `
```

### Default:

empty

#### **Remote-Networks**

Contains the remote networks to which this rule applies.

The following entries are valid:

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



Specify multiple networks by separating them with a space character.

#### SNMP ID:

2.19.35.1.3

## **Telnet path:**

Setup > VPN > Networks > IPv4-Rules

## **Possible values:**

```
Max. 127 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `
```

## Default:

empty

# IPv4-Rule-Lists

In this table, you collect the VPN network rules for IPv4 connections into a rule list.

## SNMP ID:

2.19.35.2

## Telnet path:

Setup > VPN > Networks

# Name

Contains the name of this rule list.

#### SNMP ID:

2.19.35.2.1

## Telnet path:

Setup > VPN > Networks > IPv4-Rules

# Possible values:

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

# Default:

empty

# Rules

Contains the rules that you want to collect into this rule list.

(f) Specify several rules by separating them with a space character.

# SNMP ID:

2.19.35.2.2

## Telnet path:

Setup > VPN > Networks > IPv4-Rules

#### **Possible values:**

Max. 127 characters from  $[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .$ 

## Default:

empty

# **IPv6-Rules**

In this table, you configure the VPN network rules for IPv6 connections.

## SNMP ID:

2.19.35.3

## Telnet path:

Setup > VPN > Networks

# Name

Contains the name of this rule.

# SNMP ID:

2.19.35.3.1

# Telnet path:

Setup > VPN > Networks > IPv6-Rules

## **Possible values:**

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

## Default:

empty

# Local-Networks

Contains the local networks to which this rule applies.

(f) Specify multiple networks by separating them with a space character.

# SNMP ID:

2.19.35.3.2

## Telnet path:

Setup > VPN > Networks > IPv6-Rules

## Possible values:

```
Max. 127 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `
```

## Default:

empty

# **Remote-Networks**

Contains the remote networks to which this rule applies.

(f) Specify multiple networks by separating them with a space character.

## SNMP ID:

2.19.35.3.3

## Telnet path:

Setup > VPN > Networks > IPv6-Rules

# **Possible values:**

```
Max. 127 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `
```

## Default:

empty

#### **IPv6-Rule-Lists**

In this table, you collect the VPN network rules for IPv6 connections into a rule list.

#### SNMP ID:

2.19.35.4

# Telnet path:

Setup > VPN > Networks

# Name

Contains the name of this rule list.

## SNMP ID:

2.19.35.4.1

# Telnet path:

Setup > VPN > Networks > IPv6-Rules

# **Possible values:**

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

# Default:

empty

# Rules

Contains the rules that you want to collect into this rule list.



Specify several rules by separating them with a space character.

## SNMP ID:

2.19.35.4.2

## Telnet path:

Setup > VPN > Networks > IPv6-Rules

# Possible values:

Max. 127 characters from  $[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .$ 

## Default:

empty

8 Virtual LANs (VLAN)

# 8 Virtual LANs (VLAN)

# 8.1 VLAN-tagging mode "ingress mixed" removed

As of LCOS version 9.20, the VLAN-tagging mode "ingress mixed" in the VLAN port table is deprecated.

This tagging mode is now automatically converted to "Hybrid (mixed)" mode. The default value for new configurations is also the mode "Hybrid (mixed)".

# 8.1.1 The port table

The port table is used to configure each of the device's ports that are used in the VLAN. The table has an entry for each of the device's ports with the following values.

VLAN port:	LAN-1: Local area network 1
VLAN tagging mode:	Hybrid (Mixed)
Accept frames on this	port that belong to other VLANs
Port VLAN ID:	1

LANconfig: Interfaces / VLAN / Port table

WEBconfig: LCOS menu tree / Setup / VLAN / Port-Table

- Port: The name of the port; this cannot be edited
- Tagging mode

Controls the processing and assignment of VLAN tags at this port.

- Access (never): Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.
- Trunk (always): Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they are dropped.
- Hybrid (mixed): Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.
- Default: Hybrid (mixed)

## Allow all VLANs (allows packets from other VLANs to enter this port)

This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.

# Port VLAN-ID

This port ID has two functions:

Untagged packets received at this port in "Hybrid (mixed)" mode are assigned to this VLAN, as are all ingress packets received in "Access (never)" mode. 8 Virtual LANs (VLAN)

In the "Hybrid (mixed)" mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port receive **no** VLAN tag; all others are given a VLAN tag.

# **9 WLAN**

# 9.1 Adaptive RF Optimization

Improved WLAN throughput due to dynamic selection of the best WLAN channel by the access point in case of interference.

Choosing a WLAN channel specifies which part of the frequency band is used by an access point for its logical WLANs. To ensure the flawless operation of a WLAN within range of another access point, each of the access points should be using a separate channel—otherwise the WLANs have to share the medium. For this purpose, LANCOM access points use the feature Adaptive RF Optimization: The access point permanently scans the radio field for interfering signals. If a threshold is exceeded on the current WLAN channel (by means of the "wireless quality indicators"), the access point automatically switches to a qualitatively better channel. This intelligent feature enables the access point to dynamically adapt to an ever-changing radio field in order to maximize the WLAN's stability.



In LANconfig you have the option to manually configure the different thresholds that are used as the basis for an automatic channel change.

With the current LCOS version **Adaptive RF Optimization** is available to the following devices: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

# 9.1.1 Setting up Adaptive RF Optimization with LANconfig

In order to use LANconfig to configure the function Adaptive RF Optimization, it is necessary for the devices that you want to configure to offer the feature "Wireless Quality Indicators". Further information about WQI is available in the reference manual.

# 9 WLAN

To configure Adaptive RF Optimization, open LANconfig and go to **Wireless LAN** > **General**. In the "Interfaces" section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure and go to the tab **Adaptive RF Optimization**.

Physical WLAN settings - WLAN	l interface	:1		? 🛛
Operation Radio Adaptive RF Op	timization	Performance	Client mode	
In case of bad WLAN ambiance im threshold values here, which can tri	pacting the gger a cha	WLAN signal nnel switch of g	ransmission noticably, your WLAN interface.	you can define
📝 Enable Adaptive RF Optimization	n			
Threshold values				
Minimum client signal strength:	15		%	
Minimum packet count to client:	30			
Packet retry rate to client:	70		%	
Upper noise limit:	-70		dBm	
Marked channel timeout:	20		minutes	
Minimal trigger timespan:	1		minutes	
			ΠΚ	Cancel

#### **Enable Adaptive RF Optimization**

To enable monitoring of the WLAN radio field via Adaptive RF Optimization, check the box **Enable Adaptive RF Optimization**.

You then configure the thresholds that trigger automatic channel changes.

#### Minimum client signal strength

Setting for the minimum client signal strength. Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change. The value is set in % with a default of 15).

#### Minimum packet count to client

Setting for the minimum number of packets sent to a client (TX). Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change (default value: 30).

#### Packet retry rate to client

Setting for the upper limit of packets that are resent to a client. If a client receives a proportion of resent packets that exceeds this percentage value, the device will consider this client the next time the need for a channel change is evaluated. The value is set in % with a default of 70).

#### Upper noise limit

Setting for the upper limit of acceptable noise on the channel. The value is set in dBm with a default of -70).

## Marked channel timeout

If a channel is considered unusable, it will be marked/blocked for the length of time specified here. This value also blocks the channel change trigger in case all channels have been blocked. The value is set in minutes (default value: 20).

## Minimal trigger timespan

Here you specify for how long a limit is exceeded continuously before an action is triggered. The timer is reset if no limits are exceeded for a period of 20 seconds. If a limit is exceeded for the entire time span, the current channel is blocked/marked. The value is set in minutes (default value: 1).



For this setting we recommend small single-digit values.

# 9.1.2 Additions to the Setup menu

# Adaptive-RF-Optimization

Adaptive RF Optimization constantly monitors the WLAN environment and evaluates the quality of the network based on the "Wireless Quality Indicators". If the quality drops, the Adaptive RF Optimization triggers a change to a better suited channel.

## SNMP ID:

2.23.20.23

Telnet path: Setup > Interfaces > WLAN

#### lfc

Shows the interface for the Adaptive RF Optimization.

#### SNMP ID:

2.23.20.23.1

# Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

## Operating

Activates or deactivates Adaptive RF Optimization for this interface.

## SNMP ID:

2.23.20.23.2

#### Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

#### Addendum

9 WLAN

**Possible values:** 

No Yes

# Default:

No

# **Min-Client-Phy-Signal**

Setting for the minimum signal strength of clients.

# SNMP ID:

2.23.20.23.3

## Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

## **Possible values:**

Max. 3 characters from [0-9]

# Default:

15

# **Min-Client-Tx-Packets**

Setting for the minimum number of packets sent to a client.

# SNMP ID:

2.23.20.23.4

# Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

# Possible values:

Max. 5 characters from [0-9]

# Default:

30

# **Tx-Client-Retry-Ratio-Limit**

In this field you specify how quickly a packet is resent to a client.

## SNMP ID:

2.23.20.23.5

# Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

# Possible values:

Max. 3 characters from [0-9]

## Default:

70

# Noise-Limit

Setting for the upper limit of acceptable noise on the channel.

## SNMP ID:

2.23.20.23.6

# Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

## **Possible values:**

Max. 6 characters from [0-9]-

## Default:

-70

# Marked-Channel-Timeout

When a channel is considered unusable it is marked/blocked for the time specified here.

### SNMP ID:

2.23.20.23.7

## Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

#### **Possible values:**

Max. 5 characters from [0-9]

# Default:

20

## **Trigger-Timespan**

The trigger timespan set here determines how long a limit is continuously exceeded before an action is triggered.

## 9 WLAN

# SNMP ID: 2.23.20.23.8 Telnet path: Setup > Interfaces > WLAN > Adaptive-RF-Optimization Possible values: Max. 5 characters from [0-9]

Default:

# 9.2 Managed RF Optimization

As of LCOS version 9.20, you have the option to allow the APs in your WLAN environment to perform automatic channel selection.

# 9.2.1 Managed RF Optimization

Automatic channel selection ensures that the devices always operate with the best available channels. Managed RF Optimization allows you to instruct an AP to find the appropriate channel with a simple press of a button. A prerequisite for this is the Inter Access Point Protocol (IAPP), which allows the APs to communicate with one another.

APs use the IAPP protocol to communicate and pass information about the handovers of associated WLAN clients which are roaming. APs regularly send out multicast announcements to inform the devices about the BSSIDs and IP addresses of the other APs. A roaming WLAN client informs a new AP about its former AP. The AP uses the information supplied by the IAPP protocol to inform the former AP to remove the WLAN client from its list of associated clients.

You can initiate channel selection either manually or you can let the devices perform it automatically.

After receiving the command to execute automatic channel selection, each AP performs the following actions:

- The relevant WLAN is disabled.
- The AP sets its priority based on the IAPP table.
- The AP waits for a specified period of time (priority \* waiting time (10 seconds)).
- The AP reactivates the relevant WLAN.
- The AP performs an automatic channel selection.

Each AP in the same network searches for the optimal channel in a particular order. This ensures that not all devices commence their channel selection at the same time.

# Enabling channel selection via the status menu

To enable channel selection via the status menu, use the LCOS menu tree to navigate to **Status** > **WLAN** > **Auto channel selection**.



Specify a WLAN interface (e.g. WLAN-1) that should select a new channel and then click **Execute**.

Please note that channel switching only takes place on this specific device!

Enter the parameter "\*" in order to prompt all interfaces to search for a new channel.

# Setting up Managed RF Optimization with LANconfig

To configure automatic channel selection, open LANconfig and go to **Date & Time** > **General**. In the "Cron table" section, click **Cron table** and add a new entry.

Cron table					
Define actions that are performed on a time basis:					
Cron table					
ron table	Cron table - New Entr	ry	8 23		
Active Time base Variation Minutes Hours Weekday	s 🔽 Entry active				
	Which time base should be used for the trigger:				
	Real time				
	Operation time				
<	- Variation:	0			
	Minutes:		Select		
& QuickFinder Add	Hours:		Select		
	Days of week:		Select		
	Days:		Select		
	Months:		Select		
	Commands:				
	Owner:	root	- Select		
	Comment:				
		ОК	Cancel		

Specify the properties of the new cron job.

# **Entry active**

Activates or deactivates the current entry.

# Real time

Select real time as the time base for the cron job.

The real time must be valid, otherwise the commands will not be executed.

# **Operation time**

Select operation time as the time base for the cron job.



If you select operation time, the only fields in the cron table that are evaluated are the hours and minutes.

# Variation

This setting is used to generate a random value by which the action is delayed in minutes.

If this value is left at the default setting of "0", the actions are performed at the specified time. There is no variation.

# Minutes

Specify the minutes of the time when the command is executed.

## Hours

Specify the hours of the time when the command is executed.

## Days of week

Specify the weekdays on which the command is executed.

## Days

Specify the all of the days of the month on which the command is executed.

## Months

Specify the all of the months of a year when the command is executed.

## Commands

Enter the command for the channel selection here.

do /Status/WLAN/Auto-Channel-Selection [Interface-Name]

The following interface names are available: "WLAN-1", "WLAN-2" or "\*" for both interfaces.

#### Owner

By specifying an owner, the action is executed with the associated rights.

## Comment

Enter a descriptive comment here.

Please note that channel switching only takes place on this specific device!

For multiple APs within a WLAN environment, channel optimization is best managed by means of a script on the WLC, which is rolled-out to the individual APs on the network.

# Manual channel change in LANmonitor

LANmonitor gives you the option to instruct each AP in the network to manually perform a channel change. Go to the **Wireless LAN** view. Right-click with the mouse on the interface that you want to perform a channel change and, in the submenu, select **Perform automatic channel selection**.





Please notice that you do not receive feedback about the channel change.

# 9.3 Airtime Fairness

 $(\mathbf{i})$ 

 $(\mathbf{D})$ 

By fairly sharing the WLAN transmission time between all of the active clients, the available bandwidth is used to maximum effect and WLAN performance is improved.

Especially in WLAN scenarios with a high client-density, the devices have to compete for the available bandwidth. Here, the AP offers transmission slots to each of the clients in turn—without any consideration for the necessary transmission times. Legacy clients end up slowing down faster clients, even though the faster ones could complete their data transmission more quickly. The feature "Airtime Fairness" ensures that the available bandwidth is used efficiently. To this end, the WLAN transmission time ("airtimes") is fairly distributed between the active clients. The consequence: Thanks to all clients being provided with the same airtime, faster clients can achieve more data throughput in the same amount of time.



"Airtime" refers to the WLAN transmission time. Airtime Fairness provides WLAN transmission time to all of the active clients according to the mode configured for the Airtime Fairness. This, for example, stops older clients from slowing down more modern clients.

For devices with WLAN modules supporting the IEEE 802.11ac standard, the **Airtime Fairness** feature is automatically enabled in the WLAN module.

With the current LANCOM version **Airtime Fairness** is available to the following devices: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

# 9.3.1 Setting up Airtime Fairness with LANconfig

Go to **Wireless LAN** > **General**. In the **Interfaces** section, click on **Physical WLAN** settings. Select the WLAN interface you want to configure, and go to the tab **Performance**.

🔄 Physical WLAN settings - WLAN interface 💦 💽	3
Operation Radio Adaptive RF Optimization Performance Client mode	
Use TX burst (Bundling of WLAN frames - not for 802.11n)	
Quality of Service Enable QoS according to 802.11e (WME)	
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.	
Airtime fairness	
Airtime fairness mode:	
The default value 'Equal time' is advisable in most scenarios. A deviation from it is rarely neccessary.	
OK Cancel	

In the section Airtime fairness mode you select the Airtime Fairness operating mode:

## **Round robin scheduling**

Each client receives a time slot for transmission, one after the other.

## Equal media time

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because they can transmit a greater amount of data to the access point in a given amount of time.

 $(\mathbf{i})$ 

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

## 802.11n preferred

This setting prefers clients using IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

## Equal media volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down the other clients.

(i)

This setting is only recommended where it is necessary for all clients to receive the same throughput.
# 9.3.2 Additions to the Setup menu

# Airtime-Fairness-Mode

**Airtime Fairness** is a feature that shares the available bandwidth fairly between all of the active clients. Especially useful in high-density environments, it results in an improvement to WLAN performance. **Airtime Fairness** is activated by default.

### SNMP ID:

2.23.20.9.6

#### Telnet path:

Setup > Interfaces > WLAN > Performance

#### **Possible values:**

# **Round-Robin**

Each client in turn receives a time slot for transmission.

# **Equal-Airtime**

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because the access point can send more data to the client in the same amount of time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

#### Pref.-11n-Airtime

This setting prefers clients that use IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent much faster to clients using IEEE 802.11n.

#### **Equal-Volume**

This setting distributes the airtime between the clients to ensure that all clients receive the same amount of throughput by the access point. However, slower clients will slow down all clients.



This setting is only recommended when it is necessary for all clients to receive the same throughput.

### Default:

Equal-Airtime

# 9.3.3 Additions to the Status menu

### **Powersave-Retransmits**

For each packet deferred by an Airtime Fairness mode the counter increases by 1.

### SNMP ID:

1.3.54.29

Telnet path:

Status > WLAN > Errors

# 9.4 Encrypted OKC via IAPP

As of LCOS version 9.20, it is possible to use OKC (opportunistic key caching) in networks that are managed by the LANCOM Large Scale Rollout & Management (LSR).

# 9.4.1 Encrypted OKC via IAPP

By setting an IAPP passphrase (PMK-IAPP secret) on an AP, it is possible to transfer the encrypted PMK (pairwise master key) to the other APs and store it there.

In LANconfig, the IAPP passphrase is entered under **Wireless LAN** > **802.11i/WEP** and clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.

🔁 WLAN encryption settings - Ed	it Entry	? 💌
General Advanced		
WPA rekeying cycle:	0	seconds
WPA2 key management:	Standard 🗸	
Client EAP method:	TLS -	
IAPP passphrase:		Show
	Generate password	]
📝 PMK caching		
Pre authentication		
Authentication:	Open system (recommende 🔻	]
Default key:	Key 1 🔹	]
Encrypt management frames:	No	]
		OK Cancel

# 9.4.2 Additions to the Setup menu

# **PMK-IAPP-Secret**

Networked APs exchange data about associated WLAN clients by means of the IAPP, so ensuring that the WLAN clients can roam securely in controller-less WLAN networks that are managed by the LANCOM LSR.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

#### SNMP ID:

2.23.20.3.20

### Telnet path:

Setup > Interfaces > WLAN > Encryption

# Possible values:

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

#### Default:

empty

Special values:

empty OKC via IAPP is disabled.

# 9.5 Fast roaming

As of LCOS version 9.20, it is possible to operate Fast Roaming (IEEE 802.11r) in networks that are managed by the LANCOM Large Scale Rollout & Management (LSR).

# 9.5.1 Fast roaming with IAPP

In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). APs that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between themselves and ensure uninterrupted connections.

In LANconfig, the IAPP passphrase is entered by navigating to **Wireless LAN** > **Encryption** and then clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.

🔄 WLAN encryption settings - Edit	Entry	? 💌
General Advanced		
WPA rekeying cycle:	0	seconds
WPA2 key management:	Standard 👻	
Client EAP method:	TLS 👻	
IAPP passphrase:		Show
	Generate password 🛛 🖛	]
☑ PMK caching ☑ Pre authentication		
Authentication:	Open system (recommende 💌	]
Default key:	Key 1 🔹	]
Encrypt management frames:	No 🔻	]
		OK Cancel

Please note the use of IEEE 802.11r requires **WPA2 key management** in the encryption settings to be set to "Fast roaming".

# 9.5.2 Additions to the Setup menu

# **PMK-IAPP-Secret**

Networked APs exchange data about associated WLAN clients by means of the IAPP, so ensuring that the WLAN clients can roam securely in controller-less WLAN networks that are managed by the LANCOM LSR.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

### SNMP ID:

2.23.20.3.20

### Telnet path:

Setup > Interfaces > WLAN > Encryption

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

Default:

empty

#### Special values:

empty

OKC via IAPP is disabled.

# 9.6 Wireless Intrusion Detection System (WIDS)

An Intrusion Detection System (IDS) recognizes attacks on a network and reports these attacks to a network management system. Especially in a professional environment, an IDS is essential for the detection and handling of potential attacks or interference.

The Wireless Intrusion Detection System (WIDS) in LCOS devices monitors the different WLANs by using a wide range of specified thresholds. If a potential attack is detected, the system reports it immediately via e-mail, SYSLOG, or SNMP traps.

Attacks are detected by monitoring for known or similar patterns.

The WIDS configuration is either done directly on the AP, or by means of a WIDS profile assigned to the AP by a WLC.

Please note that detection based on pattern recognition (heuristics) can lead to false alarms ("false positives").

# 9.6.1 Configuring WIDS on the AP with LANconfig

To configure the Wireless Intrusion Detection System (WIDS) open LANconfig and go to Wireless LAN > Security.

Wireless-IDS active	Promiscuous mode	
🗸 Messaging via SYSLOG	Messaging via SNMP traps	
Messaging via E-Mail		
E-Mail recipient:		
E-Mail addredate interval:	10	seconds

### Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

#### Promiscuous mode

With the ("promiscuous mode") enabled, the AP additionally receives packets that were not directed at it, but to other network participants.

This mode is necessary to be able to detect the attacks listed below. However, the promiscuous mode affects the performance. For this reason, activating the promiscuous mode automatically causes frame aggregation to be switched off.

#### Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

### Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

#### Messaging via e-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

#### E-mail recipient

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

#### E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

# Signatures

Here you configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

Signatures					? <b>×</b>
Attack szenarios:			Measuring interval:		
EAPOL start:	250	Packets	per interval of:	10	seconds
Broadcast probe:	1.500	Packets	per interval of:	10	seconds
Authentication request:	250	Packets	per interval of:	10	seconds
Deauthentication:	250	Packets	per interval of:	10	seconds
Broadcast deauthenticat.:	2	Packets	per interval of:	1	seconds
Association request:	250	Packets	per interval of:	10	seconds
Reassociation request:	250	Packets	per interval of:	10	seconds
Disassociation request:	250	Packets	per interval of:	10	seconds
Broadcast disassociate:	2	Packets	per interval of:	1	seconds
Out-of-window:	200	Packets	per interval of:	5	seconds
Block Ack after DelBA:	100	Packets	per interval of:	5	seconds
Null data flood:	500	Packets	per interval of:	5	seconds
Null data PS buffer overfl.:	200	Packets	per interval of:	5	seconds
Multi stream data:	100	Packets	per interval of:	5	seconds
Premature EAPOL success:	0	Packets	per interval of:	1	seconds
Premature EAPOL failure:	0	Packets	per interval of:	1	seconds
PS poll TIM interval:	100	Packets	per interval of:	5	seconds
Listen interval difference:	5				
				ОК	Cancel

The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

- EAPOL-Start
- Broadcast probe
- Authentication request
- Deauthentication request (\*)
- Broadcast deauthentication
- Association request

- Reassociation request
- Disassociation request (\*)
- Broadcast disassociate
- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (\*)
- Premature EAPOL failure (\*)
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.

(\*) These attacks are only detected if promiscuous mode is active.

# 9.6.2 Configuring WIDS profiles on the WLC with LANconfig

To configure a profile for the Wireless Intrusion Detection System (WIDS) with LANconfig, go to the view **WLAN** controller > Profiles and click on Advanced profiles.

Advanced Profiles	? ->
The following profiles which are assigned in the ) (()	
control the LEDs of the device.	an promes,
Device LED profiles	]
With the automatical wireless distribution system (Aut possible to automatically expand a WLAN network o radio links (point-to-point).	oWDS) it is n the basis of
AutoWDS	]
The following profiles control which Location Based (LBS server) is contacted by the access points (AP).	Services server
Here you define wireless ePaper profiles, that are to WLAN profiles table above, which specify the wirele information to be used by the access points.	be used in the ss ePaper
Wireless ePaper	profiles
With the Wireless Intrusion Detection System (Wirele identify specific attacks on your wireless LAN infrastr Wireless IDS profiles	ess IDS) you can ucture.
	Cancel

Create or edit the WIDS profiles under Wireless IDS profiles.

	, ? 💌
General Signatures Signatures	
Profile name:	
📝 Entry active	
With the Wireless Intrusion Detection your wireless LAN infrastructure.	n System (Wireless IDS) you can identify specific attacks on
☑ Wireless-IDS active	Promiscuous mode
✓ Messaging via SYSLOG Messaging via E-Mail	Messaging via SNMP traps
E-Mail recipient:	
E-Mail aggregate interval:	10 seconds

# Profile name

Enter an identifier for this profile. You allocate this profile name to a WLAN profile under **WLAN controller** > **Profiles > WLAN profiles.** 

 $\bigcirc$ 

You need to specify a profile name for the configuration of the WIDS signatures.

### Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

### **Promiscuous mode**

With the ("promiscuous mode") enabled, the AP additionally receives packets that were not directed at it, but to other network participants.

This mode is necessary to be able to detect the attacks listed below. However, the promiscuous mode affects the performance. For this reason, activating the promiscuous mode automatically causes frame aggregation to be switched off.

### Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

### Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

#### Messaging via e-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

# **E-mail recipient**

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

#### E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

The "Signatures" tabs are used to configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.



The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

EAPOL-Start

- Broadcast probe
- Authentication request
- Deauthentication request (\*)
- Broadcast deauthentication
- Association request
- Reassociation request
- Disassociation request (\*)
- Broadcast disassociate
- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (\*)
- Premature EAPOL failure (\*)
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.

(\*) These attacks are only detected if promiscuous mode is active.

Save the WIDS profile and then assign it to a WLAN profile under WLAN controller > Profiles > WLAN profiles.

WLAN profiles - New Entry	/	? 🔀
Profile name:		]
Specify in the following list u profile.	ip to 16 logical WLAN net	works for this
WLAN network list:		Select
Physic. WLAN parameters:	-	Select
List of alternative WLCs:		
802.11u venue profile:	-	Select
Configuration delay:	0	seconds
Device LED profile:	-	Select
LBS server profile:	-	Select
Wireless ePaper profile:	-	Select
Wireless IDS profile:	-	Select
	ОК	Cancel
	- On	00.1001

# 9.6.3 Additions to the Setup menu

# Wireless-IDS

In this directory, you configure the Wireless Intrusion Detection System (WIDS).

# SNMP ID:

2.12.248

Telnet path: Setup > WLAN

### **IDS-Operational**

Activates or deactivates the Wireless Intrusion Detection System (WIDS).

#### SNMP ID:

2.12.248.9

#### Telnet path:

Setup > WLAN > Wireless-IDS

### **Possible values:**

No

The Wireless Intrusion Detection System is deactivated.

#### Yes

The Wireless Intrusion Detection System is activated.

#### Default:

No

### Syslog-Operational

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

## SNMP ID:

2.12.248.10

### Telnet path:

Setup > WLAN > Wireless-IDS

#### **Possible values:**

#### No

WIDS messaging via SYSLOG is disabled.

### Yes

WIDS messaging via SYSLOG is enabled.

### Default:

Yes

#### **SNMPTraps-Operational**

Activates or deactivates the WIDS messaging via SNMP traps.

#### SNMP ID:

2.12.248.11

# Telnet path:

Setup > WLAN > Wireless-IDS

# Possible values:

No

Messaging via SNMP traps is disabled.

Yes

Messaging via SNMP traps is enabled.

# Default:

No

# E-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

#### SNMP ID:

2.12.248.12

### Telnet path:

Setup > WLAN > Wireless-IDS

# **Possible values:**

No

WIDS messaging via e-mail is disabled.

Yes

Messaging via e-mail is enabled.

# Default:

No

# **E-Mail-Receiver**

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

# SNMP ID:

2.12.248.13

#### Telnet path:

Setup > WLAN > Wireless-IDS

# **Possible values:**

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

#### E-Mail-Aggregate-Interval

This setting sets the delay in seconds before a new e-mail is sent in case the WIDS is triggered again. This prevents flooding by e-mail in case of extensive attacks.

#### SNMP ID:

2.12.248.14

#### Telnet path:

Setup > WLAN > Wireless-IDS

# Possible values:

Max. 4 characters from [0-9]

### Default:

10

#### Signatures

Here you configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

### SNMP ID:

2.12.248.50

#### Telnet path:

Setup > WLAN > Wireless-IDS

# AssociateReqFlood

Here you configure the threshold for attacks of the type AssociateReqFlood.

### SNMP ID:

2.12.248.50.1

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.1.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

### **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.1.2

### Telnet path:

# Setup > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

# **Possible values:**

Max. 4 characters from [0-9]

#### Default:

10

## ReassociateReqFlood

Here you configure the threshold for attacks of the type ReassociateReqFlood.

#### SNMP ID:

2.12.248.50.2

#### **Telnet path:**

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.2.1

### Telnet path:

### Setup > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

# Possible values:

Max. 4 characters from [0-9]

# Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.2.2

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

#### **Possible values:**

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

### Default:

10

#### AuthenticateReqFlood

Here you configure the threshold for attacks of the type AuthenticateReqFlood.

#### SNMP ID:

2.12.248.50.3

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.3.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

### **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.3.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

10

#### EAPOLStart

Here you configure the threshold for attacks of the type EAPOLStart.

### SNMP ID:

2.12.248.50.4

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.4.1

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > EAPOLStart

Addendum

9 WLAN

### **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

### SNMP ID:

2.12.248.50.4.2

Telnet path:

### Setup > WLAN > Wireless-IDS > Signatures > EAPOLStart

Possible values:

Max. 4 characters from [0-9]

# Default:

10

# ProbeBroadcast

Here you configure the threshold for attacks of the type ProbeBroadcast.

# SNMP ID:

2.12.248.50.5

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

### SNMP ID:

2.12.248.50.5.1

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

# Possible values:

Max. 4 characters from [0-9]

Default:

1500

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.5.2

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

#### **Possible values:**

Max. 4 characters from [0-9]

### Default:

10

## DisassociateBroadcast

Here you configure the threshold for attacks of the type DisassociateBroadcast.

### SNMP ID:

2.12.248.50.6

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.6.1

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

2

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.6.2

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast

# Possible values:

Max. 4 characters from [0-9]

# Default:

1

# DeauthenticateBroadcast

Here you configure the threshold for attacks of the type DeauthenticateBroadcast.

#### SNMP ID:

2.12.248.50.7

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.7.1

#### Telnet path:

### Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

### **Possible values:**

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

### Default:

2

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.7.2

### Telnet path:

#### Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

#### **Possible values:**

Max. 4 characters from [0-9]

### Default:

1

#### DisassociateReqFlood

Here you configure the threshold for attacks of the type DisassociateReqFlood.

#### SNMP ID:

2.12.248.50.8

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.8.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

## SNMP ID:

2.12.248.50.8.2

#### Addendum

9 WLAN

#### Telnet path:

#### Setup > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood

# **Possible values:**

Max. 4 characters from [0-9]

# Default:

10

# BlockAckOutOfWindow

Here you configure the threshold for attacks of the type BlockAckOutOfWindow.

## SNMP ID:

2.12.248.50.9

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.9.1

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

200

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.12.248.50.9.2

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

5

# BlockAckAfterDelBA

Here you configure the threshold for attacks of the type BlockAckAfterDelBA.

#### SNMP ID:

2.12.248.50.10

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.10.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

100

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

### SNMP ID:

2.12.248.50.10.2

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

### **Possible values:**

Max. 4 characters from [0-9]

Default:

5

## NullDataFlood

Here you configure the threshold for attacks of the type NullDataFlood.

#### SNMP ID:

2.12.248.50.11

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

# SNMP ID:

2.12.248.50.11.1

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > NullDataFlood

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

500

# CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.11.2

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > NullDataFlood

# **Possible values:**

Max. 4 characters from [0-9]

### Default:

5

# NullDataPSBufferOverflow

Here you configure the threshold for attacks of the type NullDataPSBufferOverflow.

#### SNMP ID:

2.12.248.50.12

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.12.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

200

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.12.2

#### Telnet path:

#### Setup > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

**Possible values:** 

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

# Default:

5

# **PSPollTIMInterval**

Here you configure the threshold for attacks of the type PSPollTIMInterval.

#### SNMP ID:

2.12.248.50.13

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.13.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

100

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.12.248.50.13.2

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

# Possible values:

Max. 4 characters from [0-9]

# Default:

5

# Interval-Diff

#### SNMP ID:

2.12.248.50.13.3

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

## **Possible values:**

Max. 4 characters from [0-9]

# Default:

5

# SMPSMUltiStream

Here you configure the threshold for attacks of the type SMPSMUltiStream.

### SNMP ID:

2.12.248.50.14

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.14.1

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > SMPSMUltiStream

### **Possible values:**

Max. 4 characters from [0-9]

### Default:

100

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

### SNMP ID:

2.12.248.50.14.2

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > SMPSMUltiStream

#### Addendum

#### 9 WLAN

Possible values:

Max. 4 characters from [0-9]

# Default:

5

# DeauthenticateReqFlood

Here you configure the threshold for attacks of the type DeauthenticateReqFlood.

#### SNMP ID:

2.12.248.50.15

# Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.15.1

#### Telnet path:

Setup > WLAN > Wireless - IDS > Signatures > DeauthenticateReqFlood

### Possible values:

Max. 4 characters from [0-9]

### Default:

250

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

### SNMP ID:

2.12.248.50.15.2

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

# Possible values:

Max. 4 characters from [0-9]

Default:

10

# PrematureEAPOLSuccess

Here you configure the threshold for attacks of the type PrematureEAPOLSuccess.

#### SNMP ID:

2.12.248.50.16

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

# SNMP ID:

2.12.248.50.16.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess

#### **Possible values:**

Max. 4 characters from [0-9]

#### Default:

2

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.16.2

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess

# **Possible values:**

Max. 4 characters from [0-9]

### Default:

1

#### PrematureEAPOLFailure

Here you configure the threshold for attacks of the type PrematureEAPOLFailure.

### SNMP ID:

2.12.248.50.17

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

# CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.12.248.50.17.1

#### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

2

# CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.12.248.50.17.2

#### Telnet path:

#### Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

**Possible values:** 

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

# Default:

1

# Promiscuous-Mode

Activates or deactivates the promiscuous mode. This mode handles also packets that were not sent to the device itself. These packets are forwarded to LCOS to allow an analysis by the WIDS.

This mode can be used to detect the following attacks:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess
- DeauthenticateReqFlood
- DisassociateReqFlood

Please note that the promiscuous mode has a significant impact on the performance. For example, frame aggregation is deactivated while it is in action. Only use this mode in case of a strong suspicion.

#### SNMP ID:

2.12.248.51

### Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

### **Possible values:**

No

Promiscuous mode is disabled.

Yes

Promiscuous mode is enabled.

#### Default:

No

# 9.6.4 Additions to the Status menu

# Wireless-IDS

In this directory, you find the statistics for the Wireless Intrusion Detection System (WIDS).

#### SNMP ID:

1.3.248

### Telnet path:

 ${\it Status} > {\it WLAN}$ 

#### **Event-Table**

The event table shows the details of the most recent attacks, including event type, event ID, and timestamp. The AP stores up to 100 entries.

#### SNMP ID:

1.3.248.1

### Telnet path:

Status > WLAN > Wireless-IDS

Addendum

#### 9 WLAN

# **Event-Type**

This entry shows the type of attack.

# SNMP ID:

1.3.248.1.1

# Telnet path:

Status > WLAN > Wireless-IDS > Event-Table

# ID :

Index to identify the events.

#### SNMP ID:

1.3.248.1.2

#### Telnet path:

Status > WLAN > Wireless-IDS > Event-Table

# **Event-Time**

Time when the attack took place.

#### SNMP ID:

1.3.248.1.3

#### Telnet path:

Status > WLAN > Wireless-IDS > Event-Table

# **Event-Rate**

This entry shows the number of attacks during the configured interval.

# SNMP ID:

1.3.248.1.4

# Telnet path:

Status > WLAN > Wireless-IDS > Event-Table

# Interface

This entry shows the interface on which the attack took place.

#### SNMP ID:

1.3.248.1.5

# Telnet path:

Status > WLAN > Wireless-IDS > Event-Table

### **Signatures**

This directory contains information about the different attacks.

#### SNMP ID:

1.3.248.2

# Telnet path:

Status > WLAN > Wireless-IDS

## AssociateReqFlood

In this directory, you find the statistics for the attack of the type AssociateReqFlood.

(i) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

### SNMP ID:

1.3.248.2.1.1

### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.1.2

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

### SNMP ID:

1.3.248.2.1.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

### ReassociateReqFlood

In this directory, you find the statistics for the attack of the type ReassociateReqFlood.

(i) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.2

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

#### **Possible values:**

max. 4 characters from [0-9]

# Default:

10

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.2.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.2.2

### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.2.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

# AuthenticateReqFlood

In this directory, you find the statistics for the attack of the type AuthenticateReqFlood.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.3.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

### SNMP ID:

1.3.248.2.3.2

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

### SNMP ID:

1.3.248.2.3.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

# EAPOLStart

In this directory, you find the statistics for the attack of the type EAPOLStart.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.4

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.4.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > EAPOLStart

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.4.2

### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > EAPOLStart

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.4.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > EAPOLStart

# ProbeBroadcast

In this directory, you find the statistics for the attack of the type ProbeBroadcast.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.5

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.5.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.5.2

### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

### SNMP ID:

1.3.248.2.5.3

### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

# DisassociateBroadcast

In this directory, you find the statistics for the attack of the type DisassociateBroadcast.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.6

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.6.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast
# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.6.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.6.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast

# DeauthenticateBroadcast

In this directory, you find the statistics for the attack of the type DeauthenticateBroadcast.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.7

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.7.1

# **Telnet path:**

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.7.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

## SNMP ID:

1.3.248.2.7.3

#### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

# DisassociateReqFlood

In this directory, you find the statistics for the attack of the type DisassociateReqFlood.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.8

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

## SNMP ID:

1.3.248.2.8.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.8.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.8.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood

# BlockAckOutOfWindow

In this directory, you find the statistics for the attack of the type BlockAckOutOfWindow.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.9

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.9.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.9.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.9.3

#### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

# BlockAckAfterDelBA

In this directory, you find the statistics for the attack of the type BlockAckAfterDelBA.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.10

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded Block-Ack-after-DelBA attacks.

# SNMP ID:

1.3.248.2.10.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.10.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.10.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

# NullDataFlood

In this directory, you find the statistics for the attack of the type NullDataFlood.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.11

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.11.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > NullDataFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

## SNMP ID:

1.3.248.2.11.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > NullDataFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

## SNMP ID:

1.3.248.2.11.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > NullDataFlood

# NullDataPSBufferOverflow

In this directory, you find the statistics for the attack of the type NullDataPSBufferOverflow.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.12

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.12.1

# Telnet path:

Status > WLAN > Wireless - IDS > Signatures > NullDataPSBufferOverflow

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.12.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.12.3

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

# PSPolITIMInterval

In this directory, you find the statistics for the attack of the type PSPolITIMInterval.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.13

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.13.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

## SNMP ID:

1.3.248.2.13.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PSPolITIMInterval

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

## SNMP ID:

1.3.248.2.13.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

# SMPSMUltiStream

In this directory, you find the statistics for the attack of the type SMPSMUltiStream.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.20.14

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.14.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > SMPSMUltiStream

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.14.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > SMPSMUltiStream

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.14.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > SMPSMUltiStream

# DeauthenticateReqFlood

In this directory, you find the statistics for the attack of the type DeauthenticateReqFlood.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.15

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.15.1

# **Telnet path:**

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

## SNMP ID:

1.3.248.2.15.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

## SNMP ID:

1.3.248.2.15.3

#### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

# PrematureEAPOLSuccess

In this directory, you find the statistics for the attack of the type PrematureEAPOLSuccess.

The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.16

Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.16.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

#### SNMP ID:

1.3.248.2.16.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

#### SNMP ID:

1.3.248.2.16.3

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess

# PrematureEAPOLFailure

In this directory, you find the statistics for the attack of the type PrematureEAPOLFailure.

(1) The display of the parameters may vary depending on the number of interfaces.

#### SNMP ID:

1.3.248.2.17

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures

# Counter

Number of recorded attacks.

# SNMP ID:

1.3.248.2.17.1

# Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

# Alarm-State-Ifc-1

Shows the alarm state of the 1st interface.

## SNMP ID:

1.3.248.2.17.2

## Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

# Alarm-State-Ifc-2

Shows the alarm state of the 2nd interface.

## SNMP ID:

1.3.248.2.17.3

#### Telnet path:

Status > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

# 9.7 Status counters for failed WPA-PSK/IEEE 802.1X login attempts

As of LCOS version 9.20, you have the option to display the number of failed login attempts for WPA and IEEE 802.1X.

# 9.7.1 Status counters for WPA-PSK login attempts

An overview of the number of failed WPA-PSK login attempts is located in the LCOS menu tree under **Status** > **WLAN** > **Encryption**.

There is also an overview of successful login attempts, as well as the number of authorizations rejected due to an incorrect passphrase.

Encryption													
Interface	Encryption	Method	WPA-Version	WPA1-Session- Keytypes	WPA2-Session- Keytypes	PMK-Caching	Pre-Authentication	окс	Prot Mgmt-Frames	WPA2-Key- Management	WPA-PSK- Num-Success	WPA-PSK- Num-Failures	WPA-PSK-Num-Wrong- Passphrase
WLAN-1	Yes	802.11i- WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-2	Yes	802.11i- WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-3	Yes	802.11i- WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-4	Yes	802.11i- WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-5	Yes	802.11i- WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-6	Yes	802.11i- WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0

Select an interface in the table (e.g. WLAN-1) to display the information for the selected interface.

Encryption	
Interface	WLAN-1
Encryption	Yes
Method	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Session-Keytypes	TKIP/AES
WPA2-Session-Keytypes	TKIP/AES
PMK-Caching	Yes
Pre-Authentication	Yes
OKC	No
ProtMgmt-Frames	No
WPA2-Key-Management	Standard
WPA-PSK-Num-Success	0
WPA-PSK-Num-Failures	0
WPA-PSK-Num-Wrong-Passphrase	0

# 9.7.2 Status counters for IEEE 802.1X login attempts

A table showing the number of accepted and rejected connect requests for each logical interface is located in the LCOS menu tree under **Status** > **IEEE802.1x** > **Ports**.

The overview also indicates the number of times the authorization limit was reached for each interface.

Ports			
Port	Num-Accept	Num-Reject	Num-ReauthMax-reached
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

# 9.7.3 Additions to the Status menu

# Encryption

This table contains information about the encryption on each interface.

# SNMP ID:

1.3.64

Telnet path:

 ${\sf Status} > {\sf WLAN}$ 

## WPA-PSK-Num-Wrong-Passphrase

Displays the number of WPA requests that failed on this interface due to an incorrect passphrase.

## SNMP ID:

1.3.64.20

Telnet path: Status > WLAN > Encryption

## WPA-PSK-Num-Success

Displays the number of successful WPA requests on this interface.

#### SNMP ID:

1.3.64.21

Telnet path: Status > WLAN > Encryption

#### WPA-PSK-Num-Failures

Displays the number of failed WPA requests on this interface.

#### SNMP ID:

1.3.64.22

Telnet path: Status > WLAN > Encryption

## Ports

This table provides an overview of the accepted or rejected connection requests for each logical interface.

#### SNMP ID:

1.46.3

## Telnet path:

Status > IEEE802.1x

# Port

Displays the name of the interface.

#### SNMP ID:

1.46.3.1

## Telnet path:

Status > IEEE802.1x > Ports

# Num-accept

Displays the number of successful WPA requests on this interface.

#### SNMP ID:

1.46.3.2

# Telnet path:

Status > IEEE802.1x > Ports

## Num-reject

Displays the number of failed WPA requests on this interface.

## SNMP ID:

1.46.3.3

Telnet path: Status > IEEE802.1x > Ports

#### Num-ReauthMax-reached

SNMP ID:

1.46.3.4

#### Telnet path:

Status > IEEE802.1x > Ports

# 9.8 Adaptive transmission power

As of LCOS version 9.20, the failure of any APs on the network can be automatically compensated for by increasing the transmission power of the other APs.

# 9.8.1 Adaptive transmission power

Dynamic transmission power adaptation is an essential feature for WLAN environments with professional backup scenarios. If an AP fails, the remaining access points automatically increase their transmission power to ensure full WLAN coverage at all times.

To do this, specify how many APs operate within a broadcast domain. So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs becomes equal to the expected number of devices. The other APs return their transmission power to the default value.

# Setting up Adaptive Transmission Power with LANconfig

To configure this in LANconfig, go to **Wireless LAN** > **General**. In the **Extended settings** section, click the button Expert WLAN settings and, if your AP has multiple WLAN interfaces, select the appropriate one. Go to the **Backup transmission power reduction** tab and enter the number of expected APs and the power reduction.

Expert WLAN settings - WLAN interface									
Beaconing Roaming Backup transmission power reduction									
Expected APs:	0	]							
Backup Tx. power red.	0	dB							
		OK Cancel							

## **Expected APs**

Specify how many APs operate within a broadcast domain.

#### Backup TX power red.

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

The default transmission power reduction is configured under **Wireless LAN** > **General** by clicking the button **Physical WLAN settings** (selecting the WLAN interface, if necessary) and accessing the **Radio** tab.

# 9.8.2 Additions to the Setup menu

# **Redundancy settings**

In this directory, you configure the dynamic adjustment of transmission power in the event of the failure of an AP a cluster of several APs.

## SNMP ID:

2.23.20.24

Telnet path:

Setup > Interfaces > WLAN

#### lfc

The interface that this entry refers to.

#### SNMP ID:

2.23.20.24.1

#### Telnet path:

Setup > Interfaces > WLAN > Redundancy-Settings

#### Other APs expected

Use this item to specify the number of other APs that are located in the AP cluster.

So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs is equal to the number of expected devices. The other APs return their transmission power to the default value.

#### SNMP ID:

2.23.20.24.2

#### Telnet path:

Setup > Interfaces > WLAN > Redundancy-Settings

## Possible values:

Max. 5 characters from [0-9]

## Backup transmission power reduction

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

#### SNMP ID:

2.23.20.24.3

## Telnet path:

Setup > Interfaces > WLAN > Redundancy-Settings

#### **Possible values:**

Max. 3 characters from [0-9]

# 9.9 Improved start-up conditions for WLAN RADIUS accounting

As of LCOS version 9.20, the RADIUS accounting start message is optionally generated only after the client has received a valid IP address. In this case the RADIUS accounting server always receives a valid framed IP address.

In LANconfig, go to the view **Wireless LAN** > **General** > **Logical WLAN settings**. On the tab "Network", enable the check box **RADIUS accounting activated**.

You can now set the accounting start condition with the drop-down menu. The following settings are available.

😑 Logical WLAN settings - WLAN network 1									
Network Transmission Alarms									
WLAN network enabled									
Network name (SSID):	LANCOM								
Suppress SSID broadcast:	No 👻								
MAC filter enabled									
Maximum count of clients:	0								
Minimal client signal strength:	0	%							
Client Bridge Support:	No 🔻	]							
TX bandwidth limit:	0	kbit/s							
RX bandwidth limit:	0	kbit/s							
Client TX bandwidth limit:	0	kbit/s							
Client RX bandwidth limit:	0	kbit/s							
RADIUS accounting activated									
RADIUS accounting server:		Select							
Accounting start condition:	Connected -	]							
Enable LBS tracking									
LBS tracking list:		]							
☑ Allow data traffic between stations of this SSID									
U-JAPSD / WMM powersave activated									
		OK Cancel							

## **Accounting-Start-Condition**

Normally, the WLAN stack sends a RADIUS "accounting start" message as soon as the WLAN client is connected. Often the WLAN client has no IP address at this time, most likely because one has not yet been issued by the DHCP server. Consequently the Framed-IP-Address attribute in the RADIUS accounting message may lack meaningful content.

#### Connected

Accounting starts when the WLAN client takes on the status "Connected". This is the default setting.

### Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6).

#### Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address.

### Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address.

APIPA addresses (169.254.1.0-169.254.254.255 and fe80:) are not recognized as valid IP addresses.

# 9.9.1 Additions to the Setup menu

# Accounting-Start-Condition

Use this entry to specify when the DHCP server reports the beginning of a billing period to a RADIUS accounting server.

#### SNMP ID:

2.23.20.1.27

## Telnet path:

Setup > Interfaces > WLAN > Network

# **Possible values:**

None

Accounting starts when the WLAN client takes on the status "Connected".

# Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6) from the DHCP server.

## Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address from the DHCP server.

# Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address from the DHCP server.

## Default:

None

# 9.10 Selecting a RADIUS server profile for 802.1X authentication

As of LCOS version 9.20, you have the option of specifying a RADIUS server profile when operating authentication as per the IEEE 802.1X standard.

WLAN encryption settings	- Edit Entry			? <mark>×</mark>
General Advanced				
Interface:	Wireless Network 1			
Encryption activated				
Method / Key 1 length:	802.11i (WPA)-PSK	•		
Key 1/passphrase:			Show	
	Generate password			
RADIUS server:		-	Select	
WPA version:	WPA2	-		
WPA1 session key type:	TKIP	-		
WPA2 session key type:	AES	-		
L				
		(	OK	Cancel

## **RADIUS** server

If you select an authentication method based on the IEEE 802.1X standard under **Method/Key 1 length**, you specify the profile of a RADIUS server here.

# 9.10.1 Additions to the Setup menu

# **RADIUS** profile

If you are operating an authentication method based on the IEEE 802.1X standard, you specify the profile of a RADIUS server here.

## SNMP ID:

2.23.20.3.21

## Telnet path:

Setup > Interfaces > WLAN > Encryption

# Possible values:

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

## Default:

empty

# 9.11 Configurable data rates per WLAN module

As of LCOS version 9.20, it is possible to configure the data rates separately for each WLAN module. The following LANCOM devices support this option:

- L-151
- L-3xx
- L-4xx
- L-822
- LN-830
- L-13xx
- IAP-xxx
- OAP-xxx
- All E-series devices

The data rate currently being used is displayed in the status tree for the WLAN client and in LANmonitor.

# 9.11.1 Configurable data rates per WLAN module

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates "announced" by the AP to the client for its communication with the AP (RX).

This rate adaptation specifies a minimum and a maximum data rate, and it also allows you to disable certain data rates between these limits.

() The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

# Configuring the data rates with LANconfig

To configure the data rates with LANconfig, switch to the view **Wireless LAN** > **General**, and in the section **Extended settings** open the dialog **WLAN transmission rates**. LANconfig lists the settings for all of the available interfaces. To change the setting for an interface, select its entry and click on **Edit**.

G WLAN transmission rates - Edit Entry			? 🗙
802.11abg         802.11abg           802.11n         1 Mbit:           HT-1         1 Mbit:           HT-2         2 Mbit:           HT-3         5.5 Mbit:           802.11ac         11 Mbit:           Butter         8w/           Mbit:         8w/           Butter         8w/	Tx required  Tx required Tx allowed	12 Mbit: 18 Mbit: 24 Mbit: 36 Mbit: 48 Mbit: 54 Mbit:	Rx/Tx allowed       Rx/Tx allowed       Rx/Tx allowed       Rx/Tx allowed       Rx/Tx allowed       Rx/Tx allowed
			OK Cancel

On the left you select the standard that you want to configure.

#### Addendum

## 9 WLAN

🔄 WLAN transmission rates - Edit Entry	,			? 💌
802.11abg 802.11n HT-1 HT-2 HT-3 802.11ac	- 802.11n - HT-1 - 6.5 Mbit: 19.5 Mbit: 39 Mbit: 58.5 Mbit:	Rx/Tx allowed     ▼       Rx/Tx allowed     ▼       Rx/Tx allowed     ▼       Rx/Tx allowed     ▼	13 Mbit: 26 Mbit: 52 Mbit: 65 Mbit:	Rx/Tx allowed <ul> <li>Rx/Tx allowed</li> <li>Rx/Tx allowed</li> <li>Rx/Tx allowed</li> <li>Rx/Tx allowed</li> <li>Tx allowed</li> </ul>
WLAN transmission rates - Edit Entry	,			OK Cancel
802.11abg 802.11n HT-1 HT-2 HT-3 802.11ac	802.11ac - VHT- MCS RX: 802.11ac - VHT- MCS RX: 802.11ac - VHT-	1 None 2 None 3	MCS TX:	None   None
	MCS RX:	None	MCS TX:	None

The configuration can be modified for each of the standards separately

- 802.11abg
- 802.11n
  - □ HT-1
  - □ HT-2
  - □ HT-3
- 802.11ac
  - □ VHT-1
  - VHT-2
  - VHT-3

Depending on the standard, the following settings are available for each transmission rate and each SSID or P2P link:

## **Rx/Tx required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

## **Rx/Tx allowed**

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### **Rx allowed**

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Deactivated

The AP does not announce this rate and does not use it to communicate with the client.

#### MCS-9/8/7

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

#### None

With 802.11ac modules, the respective stream option is disabled for the corresponding data direction.

# 9.11.2 Additions to the Setup menu

# **Rate selection**

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates "announced" by the AP to the client for its communication with the AP (RX).

This rate adaptation specifies a minimum and a maximum data rate, and it also allows certain data rates between these limits to be disabled. This can save airtime under certain circumstances.



The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

In this directory you configure these data rates.

## SNMP ID:

2.23.20.25

## Telnet path:

Setup > Interfaces > WLAN

#### 1M

Here you configure how the AP is to handle this data rate for this interface.

## SNMP ID:

2.23.20.25.1

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx-required

#### 2M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.2

### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

## **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx-required

## lfc

This entry shows which interface is being configured.

#### SNMP ID:

2.23.20.25.3

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## 5.5M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.4

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## Possible values:

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

## Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# 11M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.6

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

## Default:

Rx/Tx

# 6M

Here you configure how the AP is to handle this data rate for this interface.

### SNMP ID:

2.23.20.25.8

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### 9M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.9

### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

## **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

## Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

## 12M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.10

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## Possible values:

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# 18M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.11

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

## Default:

Rx/Tx

## 24M

Here you configure how the AP is to handle this data rate for this interface.

## SNMP ID:

2.23.20.25.12

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# 36M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.13

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

## 48M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.14

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

## 54M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.15

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

## Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-1-6.5M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.28

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

## **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

## Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

## Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-1-13M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.29

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

## Default:

Rx/Tx

# HT-1-19.5M

Here you configure how the AP is to handle this data rate for this interface.

### SNMP ID:

2.23.20.25.30

## **Telnet path:**

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-1-26M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.31

### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

## **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

## Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-1-39M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.32

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

### Possible values:

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

## HT-1-52M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.33

## Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

## No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

## Default:

Rx/Tx

#### HT-1-58.5M

Here you configure how the AP is to handle this data rate for this interface.

## SNMP ID:

2.23.20.25.34

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

## **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.
#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# HT-1-65M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.35

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# 9 WLAN

# HT-2-13M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.36

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

# Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-2-26M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.37

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# **Possible values:**

# No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

# Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-2-39M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.38

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

9 WLAN

#### Default:

Rx/Tx

# HT-2-52M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.39

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# HT-2-78M

Here you configure how the AP is to handle this data rate for this interface.

# SNMP ID:

2.23.20.25.40

# Telnet path:

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-2-104M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.41

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# 9 WLAN

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-2-117M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.142

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-2-130M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.43

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# HT-3-19.5M

Here you configure how the AP is to handle this data rate for this interface.

# SNMP ID:

2.23.20.25.44

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

## Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

## **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# HT-3-39M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.45

#### Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

#### **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-3-58.5M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.46

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-3-78M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.47

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

# Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-3-117M

Here you configure how the AP is to handle this data rate for this interface.

#### **SNMP ID:**

2.23.20.25.48

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-3-156M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.49

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

#### Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

# HT-3-175.5M

Here you configure how the AP is to handle this data rate for this interface.

# SNMP ID:

2.23.20.25.50

# Telnet path:

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

#### **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

#### Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

# Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

#### Default:

Rx/Tx

#### HT-3-195M

Here you configure how the AP is to handle this data rate for this interface.

#### SNMP ID:

2.23.20.25.51

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

#### **Possible values:**

#### No

The AP does not announce this rate and does not use it to communicate with the client.

# **Rx/Tx-required**

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

# Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

# **Rx-required**

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

# Default:

Rx/Tx

# VHT-1-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

#### SNMP ID:

2.23.20.25.105

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

**Possible values:** 

None MCS7 MCS8 MCS9

Default:

MCS9

# VHT-1-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

# SNMP ID:

2.23.20.25.106

# Telnet path:

# 9 WLAN

#### **Possible values:**

None
MCS7
MCS8
MCS9

# Default:

MCS9

# VHT-2-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

# SNMP ID:

2.23.20.25.115

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

None MCS7 MCS8 MCS9

#### Default:

MCS9

# VHT-2-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

# SNMP ID:

2.23.20.25.116

# Telnet path:

**Possible values:** 

None MCS7 MCS8 MCS9

Default:

MCS9

# VHT-3-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

# SNMP ID:

2.23.20.25.125

# Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

# Possible values:

None MCS7 MCS8 MCS9

#### Default:

MCS9

# VHT-3-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

# SNMP ID:

2.23.20.25.126

# Telnet path:

Addendum

#### 9 WLAN

Possible values: None MCS7 MCS8 MCS9 Default: MCS9

# 9.12 Maximum length of the AP device name in the WLC config increased to 64 characters

As of LCOS version 9.20, AP device names in the access point table can be specified using up to 64 characters.

# 9.12.1 Additions to the Setup menu

Name

Name of the AP in managed mode.

SNMP ID:

2.37.1.4.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > Accesspoints

**Possible values:** 

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

Default:

empty

# 9.13 LANconfig: Modified WLAN encryption dialog

In LCOS version 9.20 the dialog for configuring the WLAN encryption settings has changed. The WLAN encryption settings in LANconfig are located under **Wireless LAN** > **Encryption**.

# **10.1 WIDS integration in WLCs**

As of LCOS version 9.20, WLCs manage WIDS profiles for configuring Wireless Intrusion Detection settings on their managed APs.

# 10.1.1 Managing the Wireless Intrusion Detection System with WLC profiles

The Wireless Intrusion Detection System (WIDS) in LCOS devices monitors the different WLANs by using a wide range of specified thresholds. If a potential attack is detected, the system reports it immediately via e-mail, SYSLOG, or SNMP traps.

Attacks are detected by monitoring for known or similar patterns.

With the aid of a WLC, you can conveniently manage the WIDS settings for all of your APs even in large network

Please note that detection based on pattern recognition (heuristics) can lead to false alarms ("false positives").

environments. In this case you use WIDS profiles on the WLC, and these are assigned to the APs.

The factory settings include a profile named "DEFAULT" which contains preassigned values that are typical for specific attack scenarios.

# Using LANconfig to manage WIDS profiles

Switch to the view WLAN controller > Profiles and open the dialog Advanced profiles.

Advanced Profiles	? <b>×</b>				
The following profiles, which are assigned in the WLAN profiles, control the LEDs of the device.					
Device LED profiles					
With the automatical wireless distribution system (AutoWDS) it is possible to automatically expand a WLAN network on the basis of radio links (point-to-point).					
AutoWDS					
The following profiles control which Location Based Services server (LBS server) is contacted by the access points (AP). LBS - Server					
Here you define wireless ePaper profiles, that are to be used in the WLAN profiles table above, which specify the wireless ePaper information to be used by the access points.					
Wireless ePaper profi	les				
With the Wireless Intrusion Detection System (Wireless IDS) you can identify specific attacks on your wireless LAN infrastructure.					
Wireless IDS profiles					
ОК	Cancel				

Open the dialog **Wireless IDS profiles**. A profile named "DEFAULT" is already available and contains preassigned values that are typical for specific attack scenarios. Click **Edit** to modify this profile. Click **Add** to create a new WIDS profile.

The General tab is used to configure the general profile settings:

🔄 Wireless IDS profiles - Edit Entry		? 🔀						
General Signatures Signatures								
Profile name:	DEFAULT	]						
Entry active								
With the Wireless Intrusion Detection System (Wireless IDS) you can identify specific attacks on your wireless LAN infrastructure.								
☑ Wireless-IDS active	Promiscuous r	node						
👿 Messaging via SYSLOG	🥅 Messaging via	a SNMP traps						
🥅 Messaging via E-Mail								
E-Mail recipient:		]						
E-Mail aggregate interval:	10	seconds						
Set the limits and time intervals of the two pages. These values control wh	several alarm functions of the v len the Wireless-IDS alerts are g	Wretess-IDS on the following enerated.						
		OK Cancel						

#### **Profile name**

Enter a unique profile name.

#### **Entry active**

Enables or disables this profile.

#### Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

#### Promiscuous mode

With the ("promiscuous mode") enabled, the AP additionally receives packets that were addressed to other network participants. Among other things, this affects data packets that are not broadcasts and that have a target MAC address different from the address of the AP.

This fact ensures that some of the attack types mentioned below can be detected. However, this mode affects the performance of the device. For this reason, frame aggregation is automatically disabled when the promiscuous mode is enabled.

# Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

#### Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

# Messaging via e-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

# **E-mail recipient**

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

#### E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

The two **Signature** tabs are used to configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

🔄 Wireless IDS profiles - Edit Entry		? 💌	🔄 Wireless IDS profiles - Edit Entry	/	? 💌
General Signatures Signatures			General Signatures Signatures		
EAPOL start:	250	Packets	Out-of-window:	200	Packets
per interval of:	10	seconds	per interval of:	5	seconds
Broadcast probe:	1.500	Packets	Block Ack after DelBA:	100	Packets
per interval of:	10	seconds	per interval of:	5	seconds
Authentication request:	250	Packets	Null data flood:	500	Packets
per interval of:	10	seconds	per interval of:	5	seconds
Deauthentication:	250	Packets	Null data PS buffer overfl.:	200	Packets
per interval of:	10	seconds	per interval of:	5	seconds
Broadcast deauthenticat.:	2	Packets	Multi stream data:	100	Packets
per interval of:	1	seconds	per interval of:	5	seconds
Association request:	250	Packets			
per interval of:	10	seconds	Premature EAPOL success:	2	Packets
Reassociation request:	250	Packets	per interval of:	1	seconds
per interval of:	10	seconds	Premature EAPOL failure:	2	Packets
Disassociation request:	250	Packets	per interval of:	1	seconds
per interval of:	10	seconds			
Broadcast disassociate:	2	Packets	PS poll TIM interval:	100	Packets
per interval of:	1	seconds	per interval of:	5	seconds
			Listen interval difference:	5	
		OK Cancel			OK Cancel

The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

- EAPOL-Start
- Broadcast probe
- Authentication request
- Deauthentication request (\*)
- Broadcast deauthentication
- Association request
- Reassociation request
- Disassociation request (\*)
- Broadcast disassociate
- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (\*)
- Premature EAPOL failure (\*)
- PS poll TIM interval

Listen interval difference

There are typical default values set for the different attack scenarios.

(\*): Only if the promiscuous mode is active.

# **Viewing WIDS statistics with LANmonitor**

# 10.1.2 Additions to the Setup menu

# Name

This directory is used to configure the Wireless IDS profiles for the managed APs.

# SNMP ID:

2.37.1.248

# Telnet path:

Setup > WLAN-Management

# Name

Contains the unique name of this WIDS profile.

# SNMP ID:

2.37.1.248.1

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# Possible values:

Max. 31 characters from

# Operating

Specify whether this profile is enabled or disabled. Inactive profiles are not transmitted by the WLC to an AP.

#### SNMP ID:

2.37.1.248.2

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

**Possible values:** 

Yes No

# Default:

Yes

# EAPOLStartCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.3

#### Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# EAPOLStartCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.37.1.248.4

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### Possible values:

Max. 4 characters from [0-9]

# Default:

10

## ProbeBroadCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.5

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# Possible values:

Max. 4 characters from [0-9]

# Default:

1500

# ProbeBroadCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.37.1.248.6

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### **Possible values:**

Max. 4 characters from [0-9]

# Default:

10

# DeauthenticateBroadCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

# SNMP ID:

2.37.1.248.7

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# **Possible values:**

Max. 4 characters from [0-9]

# Default:

#### DeauthenticateBroadCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.37.1.248.8

#### Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### **Possible values:**

Max. 4 characters from [0-9]

#### Default:

1

# DeauthenticateCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.9

#### Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### Possible values:

Max. 4 characters from [0-9]

# Default:

250

#### DeauthenticateCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.37.1.248.10

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# **Possible values:**

Max. 4 characters from [0-9]

#### Default:

# AssociateReqCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.11

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# **Possible values:**

Max. 4 characters from [0-9]

# Default:

250

# AssociateReqCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.37.1.248.12

#### Telnet path:

Setup > WLAN-Management > Wireless-IDS

# Possible values:

Max. 4 characters from [0-9]

# Default:

10

# ReAssociateReqCounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.13

# Telnet path:

Setup > WLAN-Management > Wireless-IDS

# **Possible values:**

Max. 4 characters from [0-9]

#### Default:

# ReAssociateReqCounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.37.1.248.14

#### Telnet path:

Setup > WLAN-Management > Wireless-IDS

#### **Possible values:**

Max. 4 characters from [0-9]

#### Default:

10

# AuthenticateCounterLimit

Use this entry to specify the maximum number of login attempts before WIDS reports an attack.

#### SNMP ID:

2.37.1.248.15

#### Telnet path:

#### Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Possible values:

Max. 10 characters from [0-9]

#### Default:

250

#### AuthenticateCounterInterval

Set the interval in seconds, within which the threshold set for the number of login attempts must be exceeded in order for WIDS to notify of an attack.

#### SNMP ID:

2.37.1.248.16

#### Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

#### Default:

# DisAssociateCounterLimit

Set the threshold number of disassociate data packets, beyond which the WIDS will notify of an attack.

#### SNMP ID:

2.37.1.248.17

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

250

# DisAssociateCounterInterval

Set the interval in seconds, within which the threshold set for the number of disassociate data packets must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.37.1.248.18

#### Telnet path:

#### Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Possible values:

Max. 10 characters from [0-9]

#### Default:

10

# **IDS-Operational**

Activates or deactivates the Wireless Intrusion Detection System (WIDS).

#### SNMP ID:

2.37.1.248.19

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Possible values:

No

The Wireless Intrusion Detection System is deactivated.

Yes

The Wireless Intrusion Detection System is activated.

# Default:

Yes

# Syslog-Operational

Activates or deactivates the messaging via SYSLOG.

# SNMP ID:

2.37.1.248.20

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

No

WIDS messaging via SYSLOG is disabled.

# Yes

WIDS messaging via SYSLOG is enabled.

# Default:

Yes

# **SNMPTraps-Operational**

Activates or deactivates the WIDS messaging via SNMP traps.

# SNMP ID:

2.37.1.248.21

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

# No

Sending and receiving SNMP traps is disabled.

# Yes

Sending and receiving SNMP traps is enabled.

#### Default:

No

# E-mail

Activates or deactivates the messaging via e-mail.

An SMTP account has to be configured in order to use messaging via e-mail.

# SNMP ID:

2.37.1.248.22

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Possible values:

#### No

WIDS messaging via e-mail is disabled.

Yes

WIDS messaging via e-mail is enabled.

# Default:

No

# **E-Mail-Receiver**

The e-mail address of the recipient when messaging via e-mail is activated. The field must contain a valid e-mail address.

#### SNMP ID:

2.37.1.248.23

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

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

## Default:

empty

# E-Mail-Aggregate-Interval

This setting sets the delay in seconds before a new e-mail is sent in case the WIDS is triggered again. This prevents flooding by e-mail in case of extensive attacks.

#### SNMP ID:

2.37.1.248.24

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

10

# BlockAck-Out-Of-Window-Counter

With this entry, you specify the number of out-of-window events after which WIDS reports an attack.

#### SNMP ID:

2.37.1.248.26

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

200

# BlockAck-Out-Of-Window-Counter-Time

Specify a period of time in seconds for counting the out-of-window events.

#### SNMP ID:

2.37.1.248.27

#### Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

#### BlockAck-Frames-Rx-After-D-E-L-B-A-Counter

With this entry, you specify the number of Frames-Rx-After-D-E-L-B-A events after which WIDS reports an attack.

#### SNMP ID:

2.37.1.248.28

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

100

# BlockAck-Frames-Rx-After-D-E-L-B-A-Counter-Time

Specify a period of time in seconds for counting the Frames-Rx-After-D-E-L-B-A events.

#### SNMP ID:

2.37.1.248.29

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

#### Default:

5

# Null-Data-DoS-Counter

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

# SNMP ID:

2.37.1.248.31

#### **Telnet path:**

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Null-Data-DoS-Counter-Time

Specify a period of time in seconds for counting the Null-Data-DoS events.

#### SNMP ID:

2.37.1.248.32

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

5

# Null-Data-P-S-Buffer-Overflow-Counter

With this entry, you specify the number of Null-Data-P-S-Buffer-Overflow events after which WIDS reports an attack.

# SNMP ID:

2.37.1.248.34

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

200

#### Null-Data-P-S-Buffer-Overflow-Counter-Time

Specify a period of time in seconds for counting the Null-Data-P-S-Buffer-Overflow events.

# SNMP ID:

2.37.1.248.35

## Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

#### P-S-Poll-T-I-M-Interval-Diff

Set the reception interval within which the threshold set for the number of P-S-Poll-T-I-M-Interval data packets must be exceeded in order for WIDS to notify of an attack.

# SNMP ID:

2.37.1.248.37

#### Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# Possible values:

Max. 10 characters from [0-9]

# Default:

5

# P-S-Poll-T-I-M-Interval-Diff-Counter

This entry sets the threshold for P-S-Poll-T-I-M-Interval packets per interval.

# SNMP ID:

2.37.1.248.38

#### Telnet path:

#### Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

100

# PS-Poll-T-I-M-Interval-Diff-Counter-Time

This entry specifies the time interval in seconds for counting the PS-Poll-TIM interval packets.

#### SNMP ID:

2.37.1.248.39

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

#### S-M-P-S-Mul-Stream-Frame-Counter

With this entry, you specify the number of S-M-P-S-Mul-Stream-Frame events after which WIDS reports an attack.

#### SNMP ID:

2.37.1.248.41

# Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

100

# S-M-P-S-Mul-Stream-Frame-Counter-Time

Specify a period of time in seconds for counting the S-M-P-S-Mul-Stream-Frame events.

#### SNMP ID:

2.37.1.248.42

#### Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

5

# DisAssociateBroadCounterLimit

This entry specifies the threshold for broadcast disassociate packets per interval, after which WIDS issues an alarm.

#### SNMP ID:

2.37.1.248.45

#### Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

# DisAssociateBroadCounterInterval

This entry specifies the time interval in seconds for counting the broadcast disassociate packets.

#### SNMP ID:

2.37.1.248.46

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

1

# EAPOLSuccessCounterLimit

Contains the threshold for EAPOL success packets per interval.

# SNMP ID:

2.37.1.248.47

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

#### Default:

2

# EAPOLSuccessCounterInterval

This entry contains the time interval in seconds for counting the EAPOL success packets.

#### SNMP ID:

2.37.1.248.48

#### Telnet path:

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

# Default:

#### EAPOLFailureCounterLimit

Contains the threshold for EAPOL failure packets per interval.

# SNMP ID:

2.37.1.248.49

# Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

# **Possible values:**

Max. 10 characters from [0-9]

# Default:

2

# EAPOLFailureCounterInterval

This entry contains the time interval in seconds for counting the EAPOL failure packets.

#### SNMP ID:

2.37.1.248.50

#### Telnet path:

# Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

Max. 10 characters from [0-9]

#### Default:

1

# Promiscuous-Mode

This entry is used to enable or disable the promiscuous mode.

# SNMP ID:

2.37.1.248.51

#### **Telnet path:**

Setup > WLAN-Management > AP-Configuration > Wireless-IDS

#### **Possible values:**

#### No

The promiscuous mode is disabled.

# Yes

The promiscuous mode is enabled.

Default:

No

# 10.1.3 Additions to the Status menu

# Alarms

This entry contains the status values for the WIDS alarms.

 $(\mathbf{i})$ 

A change in this triggers an SNMP trap "88". If the connection to an AP listed here is lost, LCOS deletes all entries for this AP from this list.

# SNMP ID:

1.73.248.2

Telnet path:

Status > WLAN-Management > Wireless-IDS

# MAC address

This entry contains the MAC address of the AP that triggered the WIDS alarm.

# SNMP ID:

1.73.248.2.1

# Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

#### lfc

This entry indicates the interface where the WIDS alarm was triggered.

SNMP ID:

1.73.248.2.2

# Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

# Signature

This entry contains the signature of the WIDS alarm.

# SNMP ID:

1.73.248.2.3
### Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

### Name

This entry contains the name of the AP.

### SNMP ID:

1.73.248.2.4

### Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

## Counter

This entry contains the number of WIDS alarms.

### SNMP ID:

1.73.248.2.5

### Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

## Alarm-Status

This entry contains the status of the WIDS alarm.

### SNMP ID:

1.73.248.2.6

### Telnet path:

Status > WLAN-Management > Wireless-IDS > Alarms

## **IDS-Operational**

This entry indicates whether WIDS is enabled on this interface.

### SNMP ID:

1.73.9.2.37

### Telnet path:

Status > WLAN-Management > AP-Status > Active-Radios

# 10.2 Automatically switch off IAPP if a CAPWAP tunnel exists

As of LCOS version 9.20, a WLC automatically disables the IAPP on managed APs as soon as a CAPWAP administration tunnel is established between APs and WLC.

# 10.3 Multiple configurable AutoWDS profiles

As of LCOS version 9.20 WLCs are able to manage multiple AutoWDS profiles.

## 10.3.1 Additions to the Setup menu

## **AutoWDS** profiles

This table contains the parameters for the AutoWDS profiles which you assign to the individual APs by means of the WLAN profile in order to implement meshed networks. AutoWDS profiles collect the settings and limits that form the P2P topology and the AutoWDS base networks.

In simple network environments, the use of the preset AutoWDS profile "DEFAULT" is sufficient. If you use several different AutoWDS profiles, the following conditions should be observed:

- APs with different AutoWDS profiles cannot be connected to one other, neither automatically nor manually.
- The maximum number of AutoWDS profiles corresponds to the maximum possible number of WLAN profiles on the WLC.
- The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.
- If two different AutoWDS profiles are used, then the rollout SSIDs must also be different. Similarly, the linking of an AutoWDS profile to a WLAN profile must be unique and unequivocal. If this is not the case, the WLC reports a profile error.
- Each AutoWDS profile uses its own SSID. This reduces the number of SSIDs that are available for the profiles. If an SSID is used multiple times, the WLC reports a profile error.
- There is only one WLC-TUNNEL-AUTOWDS interface on the WLC. The individual rollout SSIDs therefore use the same interface on the WLC as the endpoint. By default, communication between the WLAN clients is disabled during the integration.
- When express integration is enabled, the rollout SSID for unconfigured WLAN clients is initially unimportant. This means that during an express integration, an AP is able to retrieve its configuration from the WLC via an AP with a different AutoWDS profile; however, in this case it only receives its AutoWDS profile and the manually configured topology entries and/or P2P links. The automatic generation of a P2P configuration does not take place if the AutoWDS profiles of the two APs do not match. If only one AutoWDS profile is transferred in this case, the AP falls back to scan mode after the usual time: however, it has by then been assigned its AutoWDS rollout SSID and it then integrates with the corresponding AutoWDS APs (according to its profile).

## SNMP ID:

2.37.1.15

### Telnet path:

Setup > WLAN-Management > AP-Configuration

#### Name

Name of the AutoWDS profile which you reference from other tables.

(i) The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.

### SNMP ID:

2.37.1.15.1

### Telnet path:

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

#### **Possible values:**

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

#### Default:

empty

### Commonprofile

Enter the name of the WLAN profile which the AutoWDS base network is assigned to. All APs operating with this WLAN profile simultaneously deploy the corresponding AutoWDS base network.

Different AutoWDS profiles may not refer to the same WLAN profile.

### SNMP ID:

2.37.1.15.2

### Telnet path:

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

### **Possible values:**

```
Name from Setup > WLAN-Management > AP-Configuration > Commonprofiles.
```

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

### Default:

empty

### SSID

Enter the name of the logical WLAN network (SSID) that a managed AP uses to deploy the AutoWDS base network. In client mode, unassociated APs use the SSID entered here to receive a configuration from the WLC.

**()** 

This SSID is reserved exclusively for this AutoWDS profile. The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within your WLAN infrastructure.

10 WLAN management

### SNMP ID:

2.37.1.15.3

## Telnet path:

## Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles

## Possible values:

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

### Default:

AutoWDS-Rollout

## AutoWDS-Topology

Name of the AutoWDS profile for which this manual P2P configuration applies.

### SNMP ID:

2.37.1.16.1

## Telnet path:

Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology

### **Possible values:**

```
Name from Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles
Max. 15 characters from [A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.
```

### Default:

empty

# 11.1 Shorter units for absolute expiry

As of LCOS version 9.20, Public Spot vouchers can be set with shorter units of time (days, hours, minutes). This is especially useful for scenarios with a high customer frequency in combination with short linger times.

Shorter expiry times for Public Spots are configured in LANconfig under Public Spot > Wizard.

User template for e-mail, SMS and Login after consent			
Expiry type:	Relative & absolute 🔹 🔻		
Relative expiry:	3.600	seconds	
Absolute expiry:	365	]	
Unit for absolute expiry:	days 🗸		
Multiple login			
Max. concurrent logins:	1	×	
Time budget:	0	minutes	
Volume budget:	0	Megabyte	
Comment:		]	

### Unit for absolute expiry

To configure shorter expiry times, use the drop-down menu to select the unit for absolute expiry. Adjust the value for the absolute expiry if necessary.

## 11.2 Circuit ID as a Public Spot URL-redirect variable

As of LCOS version 9.20, the redirect variable "%d" enables you to display different welcome pages on authenticated clients, depending on their location.

### %**d**

Enter the URL parameter '%d' as the circuit ID, for example

http://ipaddress/?circuit=%d&nas=%i. The Public Spot module replaces this variable with the circuit ID that is detected in the client's DHCP request.

This requires "DHCP snooping" to be configured on the AP in such a way that the AP can query the circuit ID in the Public Spot station table of the WLC.

In this way it is possible for the Public Spot welcome page displayed on the clients to be customized by location.

# 11.3 Creating Public Spot users on a remote Public Spot gateway

As of LCOS version 9.20, the web API enables you to create Public Spot users on a remote Public Spot gateway.

## 11.3.1 Creating Public Spot users on a remote Public Spot gateway

With Smart Ticket operating, each user is given a Public Spot account on the RADIUS server of the local Public Spot gateway.

However, where multiple Public Spot gateways are in use but the user accounts should be managed by the RADIUS server of just one gateway, Smart Ticket causes the Public Spot account to be created on this central RADIUS server. To implement this, the remote Public Spot gateway needs to be specified in the LCOS menu tree under **Setup** > **Public Spot module** > **Authentication modules**.

If no remote Public Spot gateway is defined, the Public Spot user accounts are created on the local Public Spot gateway.

## 11.3.2 Additions to the Setup menu

## **Radius-Server**

Use this menu to specify the settings used when Public Spot user accounts are created on the RADIUS server of the remote Public Spot gateway.

### SNMP ID:

2.24.41.5

### Telnet path:

Setup > Public-Spot-Module > Authentication-Modules

### Provider

Use this entry to specify the RADIUS server profile, which is located in the Public Spot provider table and references the RADIUS server of the remote Public Spot gateway.

### SNMP ID:

2.24.41.5.1

### Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > Radius-Server

### Possible values:

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

### Default:

empty

### Name

Use this entry to specify which administrator account is used for creating user accounts on the remote Public Spot gateway.

### SNMP ID:

2.24.41.5.2

### Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > Radius-Server

### **Possible values:**

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

### Default:

empty

### Password

Use this entry to enter the password for the administrator account specified above.

### SNMP ID:

2.24.41.5.3

### Telnet path:

### Setup > Public-Spot-Module > Authentication-Modules > Radius-Server

### Possible values:

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

### Default:

empty

## 11.4 PMS template: Accept GTC

Depending on the configuration, authentication at a Public Spot optionally depends upon the acceptance of the general terms and conditions of use (GTC). In some combinations of login options (e.g. via stored reservation data or SMS authentication) the confirmation of the GTC was not clearly structured until now.

As of LCOS version 9.20, the appearance of the login page when using a combination of login methods has been redesigned.

## 11.5 Hiding fields in the setup wizard "Manage Public Spot Account"

As of LCOS version 9.20 you have the option of permanently hiding table columns in the wizard "Manage Public Spot Account".

## 11.5.1 Hiding fields in WEBconfig

In the setup wizard "Manage Public Spot Account", the **Show/hide column** button enables you to display or conceal columns of the table. These changes are only temporary. Hidden columns are shown again after a page refresh or in a new session.

If you want to permanently hide specific fields, use the LCOS menu tree and navigate to the view **Setup** > **Public Spot module** > **Manage user wizard**. All of the fields are displayed by default. If you hide certain fields, for example to conceal the time budget, they will stay hidden in the wizard itself and also in the drop-down menu behind the button **Show/hide column** after reloading the page.

In order to delete authenticated Public Spot users, the columns "Calling station ID mask" and "Called station ID mask" need to be visible in the wizard. Unauthenticated users can be deleted even if these two columns are hidden.

Please note that hidden fields are not printed out when you press the **Print** button. On the other hand, exporting a CSV file includes all of the data. The **Save as CSV** button can optionally be hidden. To do this, use the LCOS menu tree to navigate to the view **Setup** > **Public Spot module** > **Add User Wizard** > **Hide CSV export**. Select "Yes" and save your entry.

## Additions to the Setup menu

## Show expiry type

This entry gives you the option to hide the "Expiry type" column in the Setup Wizard.

## SNMP ID:

2.24.44.12

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

Yes

The Setup Wizard shows the "Expiry type" column.

No

The Setup Wizard hides the "Expiry type" column.

### Default:

Yes

### Show abs. expiry

This entry gives you the option to hide the "Absolute expiry" column in the Setup Wizard.

## SNMP ID:

2.24.44.13

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

Yes

The Setup Wizard shows the "Absolute expiry" column.

No

The Setup Wizard hides the "Absolute expiry" column.

### Default:

Yes

## Show rel. expiry

This entry gives you the option to hide the "Relative expiry" column in the Setup Wizard.

### SNMP ID:

2.24.44.14

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

#### Yes

The Setup Wizard shows the "Relative expiry" column.

## No

The Setup Wizard hides the "Relative expiry" column.

### Default:

Yes

### Show time budget

This entry gives you the option to hide the "Time budget" column in the Setup Wizard.

### SNMP ID:

2.24.44.15

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

#### **Possible values:**

### Yes

The Setup Wizard shows the "Time budget" column.

### Addendum

11 Public Spot

No

The Setup Wizard hides the "Time budget" column.

### Default:

Yes

### Show volume budget

This entry gives you the option to hide the "Volume budget MByte" column in the Setup Wizard.

### SNMP ID:

2.24.44.16

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### Possible values:

Yes

The Setup Wizard shows the "Volume budget MByte" column.

### No

The Setup Wizard hides the "Volume budget MByte" column.

### Default:

Yes

### Show case sensitive

This entry gives you the option to hide the "Case sensitive" column in the Setup Wizard.

### SNMP ID:

2.24.44.17

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

### Yes

The Setup Wizard shows the "Case sensitive" column.

## No

The Setup Wizard hides the "Case sensitive" column.

### Default:

Yes

## Show active

This entry gives you the option to hide the "Show active" column in the Setup Wizard.

### SNMP ID:

2.24.44.18

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

## **Possible values:**

### Yes

The Setup Wizard shows the "Show active" column.

No

The Setup Wizard hides the "Show active" column.

## Default:

Yes

## Show TX limit

This entry gives you the option to hide the "TX limit" (max. transmission bandwidth) column in the Setup Wizard.

### SNMP ID:

2.24.44.19

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

## Yes

The Setup Wizard shows the "TX limit" column.

### No

The Setup Wizard hides the "TX limit" column.

### Default:

Yes

### Show RX limit

This entry gives you the option to hide the "RX limit" (max. receiving bandwidth) column in the Setup Wizard.

### SNMP ID:

2.24.44.20

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

Yes

The Setup Wizard shows the "RX limit" column.

#### No

The Setup Wizard hides the "RX limit" column.

### Default:

Yes

## Show calling station

This entry gives you the option to hide the "Show calling station" column in the Setup Wizard.

### SNMP ID:

2.24.44.21

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

## Possible values:

## Yes

The Setup Wizard shows the "Show calling station" column.

### No

The Setup Wizard hides the "Show calling station" column.

### Default:

Yes

### Show called station

This entry gives you the option to hide the "Show called station" column in the Setup Wizard.

### SNMP ID:

2.24.44.22

### Telnet path:

### Setup > Public-Spot-Module > Manage-User-Wizard

### **Possible values:**

## Yes

The Setup Wizard shows the "Show called station" column.

#### No

The Setup Wizard hides the "Show called station" column.

## Default:

Yes

## Show online time

This entry gives you the option to hide the "Online time" column in the Setup Wizard.

## SNMP ID:

2.24.44.23

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

## Possible values:

## Yes

The Setup Wizard shows the "Online time" column.

### No

The Setup Wizard hides the "Online time" column.

### Default:

Yes

### Show traffic

This entry gives you the option to hide the "Traffic (Rx / Tx Kbyte)" column in the Setup Wizard.

### SNMP ID:

2.24.44.24

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### Addendum

11 Public Spot

### **Possible values:**

Yes

The Setup Wizard shows the "Traffic (Rx / Tx Kbyte)" column.

No

The Setup Wizard hides the "Traffic (Rx / Tx Kbyte)" column.

### Default:

Yes

## Show status column

This entry gives you the option to hide the "Status" column in the Setup Wizard.

### SNMP ID:

2.24.44.25

## Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

## Possible values:

### Yes

The Setup Wizard shows the "Status" column.

## No

The Setup Wizard hides the "Status" column.

### Default:

Yes

## Show MAC address

This entry gives you the option to hide the "MAC address" column in the Setup Wizard.

### SNMP ID:

2.24.44.26

## Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

#### **Possible values:**

### Yes

The Setup Wizard shows the "MAC address" column.

No

The Setup Wizard hides the "MAC address" column.

### Default:

Yes

### Show IP address

This entry gives you the option to hide the "IP address" column in the Setup Wizard.

#### SNMP ID:

2.24.44.27

### Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

### Possible values:

Yes

The Setup Wizard shows the "IP address" column.

No

The Setup Wizard hides the "IP address" column.

### Default:

Yes

## 11.6 Redirect for HTTPS connections switchable

To minimize the load on Public Spot gateways, LCOS version 9.20 introduced the option for HTTPS connections from unauthenticated clients to be redirected.

## 11.6.1 Redirect for HTTPS connections

If an unauthenticated client attempts to access an HTTPS website via an interface operated by the Public Spot, the connection request is redirected to the Public Spot gateway itself, which then presents its login page to the user (as is also the case with HTTP). Usually, the user's browser displays a certificate warning, because the name or IP of the requested website is different from the name or IP address of the Public Spot. To prevent this and the increased load on the Public Spot from the HTTPS/TLS connections, this setting allows you to prevent HTTPS connections from being established for unauthenticated clients.



Once the client is authenticated, redirection is stopped and the client can establish any HTTP or HTTPS connection.

Modern clients carry out a "captive portal detection" via HTTP. The client attempts to access a certain URL via HTTP to check for the presence of a login page (from the Public Spot or other solutions). This mechanism is not affected by turning off the HTTPS redirect, since detection is usually via HTTP.

However, if unauthenticated WLAN clients should not perform connect requests over HTTP, this ineffective HTTPS redirect would place unnecessary load on the Public Spot gateway. For this reason it is possible to disable this HTTPS redirect. In this case, the user's browser displays a blank page.

In LANconfig, you configure the HTTPS redirect under **Public Spot** > **Server** > **Operational settings**.

Operational settings		? 💌
Operational settings		
Select the local area netw authentication should be	vork interfaces for which ( enabled.	user
	Interfaces	
Table of used VLAN IDs		
	Network table	]
WEBconfig access by authentication pages	public spot interfaces lim	ited to
Idle timeout:	0	seconds
Device hostname:		
The Public Spot can mon page to the user in case of	itor a peer and present a of a loss of connectivity.	temporary error
Remote site:	-	Select
Accept TLS connection	ons from unauthenticated	clients
	OK	Cancel

To enable the HTTPS redirect, activate the option **Accept TLS connections from unauthenticated clients**. This option is disabled by default.

## 11.6.2 Additions to the Setup menu

## **Redirect TLS connections**

Use this option to determine whether the Public Spot redirects HTTPS connections for unauthenticated clients. With this option disabled, unauthenticated clients are unable to establish HTTPS connections.

### SNMP ID:

2.24.51

### Telnet path:

Setup > Public-Spot-Module

## Possible values:

### No

The Public Spot does not perform HTTPS redirects for unauthenticated WLAN clients.

## Yes

The Public Spot performs HTTPS redirects for unauthenticated WLAN clients.

### Default:

No

# 11.7 Printout of bandwidth profile on the voucher

As of LCOS version 9.20, the voucher printout optionally shows the user-specific bandwidth profile. It is entered into the voucher template with this new template identifier:

## BANDWIDTHPROFNAME

Valid for:<pbelem>

This identifier contains the bandwidth profile that the user is associated with.

(1) This identifier is available from LCOS version 9.18 RU1 . Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1 .

## RXBANDWIDTH

Valid for:<pbelem>

This identifier contains the maximum reception bandwidth of the bandwidth profile.



This identifier is available from LCOS version 9.18 RU1 . Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1 .

## TXBANDWIDTH

Valid for:<pbelem>

This identifier contains the maximum transmission bandwidth of the bandwidth profile.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

## 11.8 Template preview

As of LCOS version 9.20 you have the option to preview the uploaded Public Spot templates.

# 11.8.1 Template preview in WEBconfig

You can view the changes to the Public Spot templates in WEBconfig by switching to the view **Extras** > **Public Spot template preview**.

Choose the template to show.		
• 🕪 <u>Welcome page</u>		
• 🕪 Login page		
• 🕪 Error page		
• 🕪 <u>Start page</u>		
• 🕪 <u>Status page</u>		
<ul> <li>Mage</li> </ul>		
• 🕪 <u>Help page</u>		
<ul> <li>Mo-proxy page</li> </ul>		
<ul> <li>Voucher page</li> </ul>		
<ul> <li>Mathematical Structure</li> <li>Mathematical Stru</li></ul>		
<ul> <li>Megistration page (e-mail)</li> </ul>		
• < <u>Login page (e-mail)</u>		
<ul> <li>Magnetic Registration page (SMS)</li> </ul>		
• 🕪 Login page (SMS)		
<ul> <li>Maintaine Page</li> </ul>		

Select a template to display from the list.

The selected template is displayed in the same browser window. Use the "Back" function of your browser to return to WEBconfig.

Some templates contain JavaScript code. This code is executed when the template is invoked. For example, the "Voucher page" template contains code that starts a printout when the page is displayed.

This page contains test data. However, no user is created at this point. This allows you to test the template and print it out.

Drucken	e895df7066a 🔍 🗙
Drucker Name: Canon MP970 series Printer   Status: Bereit Typ: Canon MP970 series Printer Standort: CNB.NP_000085E765C6 Kommentar:   Ausgabe in Datei	Test - WLAN Voucher Zugangsdaten / Access Data
Druckbereich     Exemplare       @ Ales     Anzahl Exemplare:       © Seten von:     bis:       Markierung     123         OK     Abbrechen	<b>(</b> Hotspot
SSID(Netzwerkname/Network name): Benutzername / Username: Passwort / Password: Gültig bis / Valid until: Dauer / Duration: Preview. No user is created.	Test SSID Testuser Testpassword 01.01.2099 00:000 1 Hour(s)

 $\bigcirc$ 

If a template does not exist or cannot be found, an error message is displayed by WEBconfig.

## **11.9 Logging DNS requests and responses to external SYSLOG servers**

As of LCOS version 9.20, it is possible to log the DNS requests and responses for the domains that are invoked by clients.

## 11.9.1 Logging DNS requests and responses to external SYSLOG servers

The DNS server in LANCOM devices resolves the DNS queries from clients. SYSLOG provides an overview of the clients, the names they requested, and the responses they received.

It is not possible to use the router/AP's own internal SYSLOG. For this reason it is necessary to employ an external SYSLOG server.

DNS logging is configured in LANconfig under **IPv4** > **DNS** in the section **SYSLOG**.

SYSLOG		
DNS replies to clients can be logged to an external SYSLOG server.		
Log DNS resolutions to an external SYSLOG server		
Server address:		
	Advanced	

### Log the DNS resolutions on an external SYSLOG server

Select this option to enable the DNS logging.

This option is independent of the setting in the SYSLOG module. Even if the SYSLOG module is disabled (setting under Log & Trace > General in the section SYSLOG), DNS logging is carried out nevertheless.

The corresponding SYSLOG message is structured as follows:

PACKET\_INFO: DNS for <IP address>, TID {Hostname}: Resource-Record

#### Server address

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

The settings behind the button Advanced influence the content of SYSLOG messages.

Advanced			? <b>- X</b>
Source:	Router	•	
Priority:	Notice	•	
Source address (optional):	INTRANET	•	Select
	OK		Cancel

### Source

Contains the log source as displayed in the SYSLOG messages.

### Priority

Contains the log level as displayed in the SYSLOG messages.

### Source address (optional)

Contains the source address that is shown in the SYSLOG messages.

## 11.9.2 Additions to the Setup menu

## Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

### SNMP ID:

2.17.20

Telnet path:

Setup > DNS

### Log DNS resolutions

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under Setup > SYSLOG > Operating. If you enable this option to log DNS requests, the DNS server in the device sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (ANSWER record or ADDITIONAL record) generates a SYSLOG message with the following structure PACKET\_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record.

The parameters have the following meanings:

- The TID (transaction ID) contains a 4-character hexadecimal code.
- The {host name} is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The resource record consists of three parts: The request, the type or class, and the IP resolution (for example www.mydomain.com STD A resolved to 193.99.144.32)

### SNMP ID:

2.17.20.1

### Telnet path:

Setup > DNS > Syslog

### Possible values:

No

Disables the logging of DNS requests and responses.

### Yes

Enables the logging of DNS requests and responses.

### Default:

No

### Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.

Tł

The use of the IP addresses 127.0.0.1 and :: 1 to force the use of an external server is not permitted.

### SNMP ID:

2.17.20.2

## Telnet path:

Setup > DNS > Syslog

## Possible values:

Max. 64 characters from [A-Z][a-z][0-9].-:%

## Log source

Contains the log source as displayed in the SYSLOG messages.

### SNMP ID:

2.17.20.3

## Telnet path:

Setup > DNS > Syslog

Possible values:

System Login System time Console login Connections Accounting Administration Router

### Default:

Router

## Log level

Contains the priority that is shown in the SYSLOG messages.

### SNMP ID:

2.17.20.4

### Telnet path:

Setup > DNS > Syslog

### **Possible values:**

Emergency Alert Critical Error Warning Notice Info Debug

#### Default:

Notice

### Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

(f) If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

### SNMP ID:

2.17.20.5

### Telnet path:

Setup > DNS > Syslog

### **Possible values:**

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

### **Special values:**

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

### Facility

The mapping of sources to specific facilities.

### SNMP ID:

2.22.3.2

Telnet path:

```
Setup > SYSLOG > Facility-Mapper
```

**Possible values:** 

KERN USER MAIL DAEMON AUTH SYSLOG LPR NEWS UUCP CRON AUTHPRIV SYSTEM0 SYSTEM1 SYSTEM2 SYSTEM3 SYSTEM4 LOCAL0 LOCAL1 LOCAL2 LOCAL3 LOCAL4 LOCAL5 LOCAL6 LOCAL7

## **IP** address

Contains the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a DNS name.

## SNMP ID:

2.22.2.7

### Telnet path:

Setup > SYSLOG > SYSLOG table

### **Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-:%

# 11.10 Protection against brute force attacks

Starting with version 9.20, LCOS provides protection against brute-force attacks on the Public Spot.

## 11.10.1 Protection against brute force attacks

Brute force attacks are the most common type of attack on networks. This method of attack tries out a variety of potential passwords in the shortest possible time, until the right one is found. One form of protection against brute-force attacks is to react to one or more successive failed attempts by delaying the time until the entry is allowed to be attempted again.

Configure the protection against brute-force attacks in LANconfig under **Public Spot** > **Server** in the section **Brute force protection**.

Brute force protection		
Lock after:	10	failed attempts
Lock duration:	60	minutes

### Lock after

Specify how many unsuccessful attempts are permitted before the entry lock takes effect.

### Lock duration

Specify for how long the entry lock is to apply.

You can use the console to display the current status of the brute-force protection with the command show pbbruteprotector:

### show pbbruteprotector

Shows all of the MAC addresses that are associated with the Public Spot.

### show pbbruteprotector [MAC address[ MAC address [ ...]]]

Specifying one or more space-separated MAC addresses shows the status of all of the respective MAC addresses.

MAC addresses are specified in the format 11:22:33:44:55:66, 11-22-33-44-55-66 or 112233445566.

## 11.10.2 Additions to the Setup menu

## **Brute force protection**

This menu contains the settings for the brute-force protection used by the Public Spot.

### SNMP ID:

2.24.49

## Telnet path:

Setup > Public-Spot-Module

## Max. login tries

Specify how many unsuccessful attempts are permitted before the login block takes effect.

### SNMP ID:

2.24.49.1

### Telnet path:

Setup > Public-Spot-Module > Brute-Force-Protection

### **Possible values:**

Max. 3 characters from [0-9]

## Default:

10

## **Blocking time in minutes**

Specify how long the login block of the brute-force protection applies.

### SNMP ID:

2.24.49.2

### Telnet path:

Setup > Public-Spot-Module > Brute-Force-Protection

## **Possible values:**

Max. 5 characters from [0-9]

### Default:

60

### Unblocking check in seconds

Specify the interval after which the AP checks for the expiry of a login block for a MAC address.

### SNMP ID:

2.24.49.3

### Telnet path:

Setup > Public-Spot-Module > Brute-Force-Protection

### **Possible values:**

Max. 5 characters from [0-9]

### Default:

60

### Unblock

Use this action to remove the login block on a MAC address. Enter the parameters as one or more space-separated MAC addresses.

í

MAC addresses are specified in the format 11:22:33:44:55:66, 11-22-33-44-55-66 or 112233445566.

## SNMP ID:

2.24.49.4

## Telnet path:

Setup > Public-Spot-Module > Brute-Force-Protection

# 12 LANCOM Location Based Services (LBS)

## 12.1 Dynamic and persistent tracking lists for WLAN clients

As of LCOS version 9.20, LBS tracking lists can also be configured with LANconfig.

For WLCs, the LBS tracking list is configured under WLAN controller > Profiles > Logical WLAN networks.

Logical WLAN networks (SSIDs) - New Entry				? <b>×</b>
VLAN network	activated	WPA version:	WPA2 -	]
Name:		WPA1 session key type:	TKIP -	
Inheritance		WPA2 session key type:	AES -	
Inherit from entry:	▼ Select	WPA2 key management:	Standard 🗸	)
		Basis rate:	2 Mbit/s 👻	
	Innerited values	Client Bridge Support:	No	
Network name (SSID):		TX bandwidth limit:	0	kbit/s
Connect SSID to:	LAN at AP	RX bandwidth limit:	0	kbit/s
VLAN mode:	Untagged 👻	Maximum count of clients:	0	
VLAN ID:	2	Min. client signal strength:	0	%
Encryption:	802.11i (WPA)-PSK 👻	🔄 Enable LBS tracking		
Key 1/passphrase:	Show	LBS tracking list:		]
	Generate password	Use long preamble for 8	Ю2.11Ь	
RADIUS profile:	DEFAULT - Select	U-)APSD / WMM powe	ersave activated	<u>,</u>
Allowed frequency bands:	2.4/5 GHz 🔹	Encrypt mgmt. frames:	No	J
AP standalone time:	0 minutes	802.11n		
802.11u network profile:	- Select	Max. spatial streams:	Auto 🗸	]
OKC (Opportunistic Key Caching) activated     Allow short guard interval     Vert Allow short gua				
🔽 Allow data traffic betwee	en stations of this SSID			
			ОК	Cancel

### **Enable LBS tracking**

This option specifies whether the LBS server is permitted to track the client information.

(1) This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

### LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

12 LANCOM Location Based Services (LBS)

On the AP, the LBS tracking list is configured under **Wireless LAN** > **General** > **Logical WLAN settings** on the **Network** tab.

😑 Logical WLAN settings - WLAN network 1 🛛 💦 🔤				
Network Transmission Alarms				
WLAN network enabled				
Network name (SSID):	LANCOM			
Suppress SSID broadcast:	No			
MAC filter enabled				
Maximum count of clients:	0	]		
Minimal client signal strength:	0	%		
Client Bridge Support:	No 🔻	]		
TX bandwidth limit:	0	kbit/s		
RX bandwidth limit:	0	kbit/s		
Client TX bandwidth limit:	0	kbit/s		
Client RX bandwidth limit:	0	kbit/s		
RADIUS accounting activated				
RADIUS accounting server:	-	Select		
Accounting start condition:	Connected 👻	]		
Enable LBS tracking				
LBS tracking list:		]		
Allow data traffic between station	ns of this SSID			
U-JAPSD / WMM powersave ad Transmit only unicasts suppress	ctivated multicasts and broadcasts			
		OK Cancel		

### **Enable LBS tracking**

This option specifies whether the LBS server is permitted to track the client information.

This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

### LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

## 12.1.1 Using the LBS tracking lists of Public Spot users

APs and WLCs feature the option to add associated Public Spot users to lists, and to register these users at an LBS (location-based service) server.

You configure this function for APs and WLCs in LANconfig under **Public Spot** > **Users** in the **LBS tracking** section.

LBS tracking	
Enable LBS tracking	
LBS tracking list:	

### **Enable LBS tracking**

Here you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

## LBS tracking list

Name of the LBS tracking list sent by the AP or WLC to the LBS server.

## 12.1.2 Additions to the Setup menu

## LBS-Tracking

Here you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

### SNMP ID:

2.24.38

### Telnet path:

Setup > Public-Spot-Module

**Possible values:** 

No Yes

### Default:

No

## LBS tracking list

Name of the LBS tracking list.

#### SNMP ID:

2.24.39

### Telnet path:

Setup > Public-Spot-Module

### **Possible values:**

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

### Default:

empty

## LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

12 LANCOM Location Based Services (LBS)

### SNMP ID:

2.37.1.1.47

### Telnet path:

Setup > WLAN-Management > AP-Configuration

### Possible values:

Name from Setup > WLAN-Management > AP-Configuration > LBS-Tracking

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

### Default:

empty

## LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

### SNMP ID:

2.23.20.1.25

### Telnet path:

Setup > Interfaces > WLAN > Network

### **Possible values:**

No

LBS tracking is disabled.

### Yes

LBS tracking is enabled.

## LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

### SNMP ID:

2.23.20.1.26

### Telnet path:

Setup > Interfaces > WLAN > Network

### **Possible values:**

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

### Default:

empty

# 13 Voice over IP – VoIP

# 13.1 Signaling parallel calls in the ISDN

As of LCOS version 9.20, you have the option to signal a call in parallel on both ISDN buses.

## 13.1.1 Signaling parallel calls in the ISDN

LANCOM devices that support the All-IP option support parallel calls. If you use this feature, signaling occurs on both ISDN lines (ISDN 1 & ISDN 2). The call is accepted at the first telephone to pick up the call.

To enable parallel calls, navigate to Voice call Manager > Users > ISDN users.

ISDN users - New Entry		? 💌
V Entry active		
Internal call number:		
Display name:		
Comment:		
ISDN parameters		
MSN/DDI:		
ISDN/S0 bus:	ISDN 2 👻	
Parallel call:	Off 👻	
En-block detection:	Auto 🔻	
Authentication data for SI	P phone system	
This information is only es upstream SIP phone syste	sential if the user registers em (PBX).	to an
Domain/realm of PBX:	-	Select
Authentication name:		
Password:		Show
	Generate password 💌	
Device type:	Phone and/or Fax 🔹	
Suppress transmission o to the remote site (CLIR)	f own phone number ]	
	ОК	Cancel

In the **ISDN parameters** section and under **ISDN/S0 bus**, select the option "ISDN 1 & ISDN 2" and then set the item **Parallel call** to "On".

## 13.1.2 Additions to the Setup menu

## Parallel call

Enables or disables parallel calls.

### SNMP ID:

2.33.3.2.2.13

13 Voice over IP – VoIP

# Telnet path: Setup > Voice-Call-Manager > Users > ISDN-User > Users

Possible values:

No

Parallel call is disabled.

Yes

Parallel call is enabled.

### Default:

No

# 13.2 VoSIP support in the Voice Call Manager

As of version 9.20, LCOS supports Voice over Secure IP (VoSIP). This function enables you to encrypt the signaling and voice data. VoSIP can be operated on the following devices:

- LANCOM 1783 / 1784
- Any LANCOM with the All-IP option

🔄 SIP lines - New Entry		? 🔀
General Advanced		
V Entry active		
Mode:	Single account 🔹	
Provider name:		
Comment:		]
⊂ Provider data		
SIP domain/realm:	•	
Registrar (optional):		
Outbound proxy (opt.):		
Port:	5.060	
Switching at provider active		
Security		
Signaling encryption:	No (UDP) 🗸	]
Speech encryption:	Ignore 🗸	]
Allow SIP messages only from	registrar	
Login data		
🔽 (Re-)Registration		
SIP-ID/user:		
Display name (optional):		
Authentication name:		
Password:		Show
	Generate password 🔻	]
Call prefix:		1
Internal dest. number:		]
L		OK Cancel

## **Signaling encryption**

This setting determines the protocol used for signaling encryption (SIP/SIPS) for communications with the provider.

Signaling encryption	
UDP	All SIP packets are transmitted connectionless. Most providers support this setting.
ТСР	All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.
TLS	Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider.

### Speech encryption

This setting determines if and how the speech data (RTP/SRTP) is encrypted when communicating with the provider.

Speech encryption	
Reject	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are rejected. The speech channel is not encrypted.
Ignore	Encryption is not available for outgoing calls. Incoming calls with an encryption proposal are accepted. The speech channel is not encrypted.
Preferred	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are accepted. The speech channel is only encrypted if the remote peer also supports encryption.
Force	Encryption is offered for outgoing calls. Incoming calls without an encryption proposal are rejected. The speech channel is either encrypted or is not established.

If you require the encrypted transmission of speech data, the signaling must also use an encrypted channel. Please note that the use of SRTP is no guarantee of end-to-end encryption.

## 13.2.1 Additions to the Setup menu

## Transport

Use this entry to specify which protocol is used to encrypt the data streams.

### SNMP ID:

2.33.4.1.1.28

## Telnet path:

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

13 Voice over IP – VoIP

#### **Possible values:**

UDP TCP TLSv1 TLSv1.1 TLSv1.2

## Default:

UDP

## SRTP

Use this entry to specify how SRTP (secure real-time transport protocol) is handled.

### SNMP ID:

2.33.4.1.1.29

## Telnet path:

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

**Possible values:** 

Deny Ignore Preferred Forced

Default:

Ignore

# 13.3 SIP over TCP in the Voice Call Manager

As of LCOS version 9.20, SIP lines can use the SIP protocol over TCP. For each line, you decide whether TCP or UDP should be used.

The settings in LANconfig are located under **VoIP Call Manager** > **Lines** and the button **SIP lines**. You set the signaling encryption in the "Security" section.

🔄 SIP lines - New Entry		? 💌
General Advanced		
🔽 Entry active		
Mode:	Single account 🔹 👻	
Provider name:		
Comment:		
Provider data		
SIP domain/realm:	-	
Registrar (optional):		
Outbound proxy (opt.):		
Port:	5.060	
Switching at provider active		
Security		
Signaling encryption:	No (UDP) 🔻	
Speech encryption:	Ignore 🔻	
Allow SIP messages only from	registrar	
Login data		
📝 (Re-)Registration		
SIP-ID/user:		
Display name (optional):		
Authentication name:		
Password:	Concerts accounted by	Show
Call prefix:		
Internal dest. number:		
<u>.</u>		OK Cancel

## Signaling encryption

This setting determines the protocol used for signaling encryption (SIP/SIPS) for communications with the provider.

## Signaling encryption

UDP	All SIP packets are transmitted connectionless. Most providers support this setting.
ТСР	All SIP packets are transmitted connection-oriented. The device establishes a TCP connection to the provider and maintains it for as long as it stays registered. Specialized providers, such as the providers of SIP trunks, support or force this setting.
TLS	Transmission is the same as with TCP, but all of the SIP packets are encrypted all the way to the provider.

13 Voice over IP – VoIP

# **13.4 DTMF signaling on All-IP connections**

As of LCOS version 9.20, a selection of DTMF signaling options is available for the transmission of DTMF tones over All-IP connections.
Settings for the DTMF signaling can be performed via the SIP line configuration and the SIP user configuration.

🔄 SIP lines - New Entry		? 🗙
General Advanced		
VoIP router		
SIP proxy port:	0	
Routing tag:	0	
Line control		
Control method:	Auto	•
Control interval:	60	seconds
SIP privacy		
Trusted Area activated		_
Transmission method:	None	•
Codec filter		
DTMF signaling:	Telephone events - fallback t	o in-band 🔹
		OK Cancel

SIP users - New Entry	? 💌
V Entry active	
Internal call number:	
Comment:	
Login data	
Authentication name:	
Password:	Show
	Generate password 💌
Access from WAN:	denied 🔹
Device type:	Phone
The rest of the settin end device or client	ngs (e.g. domain) must be made on the SIP
Suppress transmission o to the remote site (CLIR)	f own phone number
DTMF signaling:	Telephone events - fallback to in-bar 💌
	OK Cancel

### **DTMF signaling**

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

### Only in-band (in audio)

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

### **Only SIP info**

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters Signal and Duration (as per RFC 2976). There is no parallel transmission of G.711 tones.

### Telephone events - fallback to in-band (default)

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to inband transfer as per G.711.

### Telephone events - fallback to SIP info

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to transfer as per SIP-Info message.

# 13.4.1 Additions to the Setup menu

# **DTMF-Method**

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

### SNMP ID:

2.33.3.1.1.20

### Telnet path:

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

### **Possible values:**

Inband

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

# SIP-INFO

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters Signal and Duration (as per RFC 2976). There is no parallel transmission of G.711 tones.

## **RTP-Event**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to inband transfer as per G.711.

### **RTP-Event/SIP-Info**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to transfer as per SIP-Info message.

# Default:

**RTP-Event** 

# **DTMF-Method**

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

### SNMP ID:

2.33.4.1.1.27

# Telnet path:

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

# **Possible values:**

### Inband

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

### SIP-INFO

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters Signal and Duration (as per RFC 2976). There is no parallel transmission of G.711 tones.

# **RTP-Event**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to inband transfer as per G.711.

## **RTP-Event/SIP-Info**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to transfer as per SIP-Info message.

# Default:

**RTP-Event** 

# **DTMF-Method**

Depending on the requirements, it may not be sufficient to transmit "inband" DTMF tones if a SIP receiver cannot recognize these. In this case, it is possible to configure an alternative method of DTMF transmission for All-IP connections.

### SNMP ID:

2.33.4.2.1.20

# Telnet path:

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

# Possible values:

### Inband

The tones are transmitted as DTMF tones (G.711) in the RTP (voice) stream.

### SIP-INFO

The DTMF tones are transmitted "out-of-band" as a SIP-info message with the parameters Signal and Duration (as per RFC 2976). There is no parallel transmission of G.711 tones.

### **RTP-Event**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to inband transfer as per G.711.

# **RTP-Event/SIP-Info**

The DTMF tones are transmitted as specially marked events within the RTP stream (as per RFC 4733). There is no parallel transmission of G.711 tones.

If the call-initialization SDP message does not include telephone-event signaling, negotiations fallback to transfer as per SIP-Info message.

### Default:

**RTP-Event** 

# 13.5 Configurable RTP port range in the Voice Call Manager

As of LCOS version 9.20, the Voice Call Manager gives you the option to configure the source port range of the RTP packets, which helps to ensure smooth operation behind a firewall.

# 13.5.1 Additions to the Setup menu

# **RTP-Port-Start**

Use this field to set the first available RTP port in the RTP port range.

### SNMP ID:

2.33.2.21

### Telnet path:

Setup > Voice-Call-Manager > General

# Possible values:

0 ... 65535

# Default:

0

# Special values:

0

Dynamic selection as long as RTP-Port-End is also set to "0".

# **RTP-Port-End**

Use this field to set the last available RTP port in the RTP port range.

# SNMP ID:

2.33.2.22

# Telnet path:

Setup > Voice-Call-Manager > General

# Possible values:

0 ... 65535

# Default:

0

# Special values:

0

Dynamic selection as long as RTP-Port-Start is also set to "0".

13 Voice over IP – VoIP

# 13.6 Allow SIP messages only from registrar

As of LCOS version 9.20, it is possible to prevent the processing of SIP messages from unknown VoIP servers.

SIP lines - New Entry		? 💌
General Advanced		
📝 Entry active		
Mode:	Single account 🔹	
Provider name:		
Comment:		
Provider data		
SIP domain/realm:		
Registrar (optional):		
Outbound proxy (opt.):		
Port:	5.060	
Switching at provider active		
Security		
Signaling encryption:	No (UDP) 🔹	
Speech encryption:	Ignore 🔹	
Allow SIP messages only from	registrar	
Login data		
🔽 (Re-)Registration		
SIP-ID/user:		
Display name (optional):		
Authentication name:		
Password:		Show
	Generate password 🛛 🔻	
Call prefix:		
Internal dest. number:		
		OK Cancel

# Allow SIP messages only from registrar

Enable this mode if the device should accept incoming SIP messages only from the registered IP address.

Please bear in mind that a high degree of compatibility is only assured if this feature is disabled. Incoming calls are not switched to internal subscribers if the VoIP provider signals calls that come from servers/IP addresses that do not match the registrar.

# 13.6.1 Additions to the Setup menu

# Strict-Mode

This option activates a security mechanism that stops the SIP user agent from processing SIP messages from unknown VoIP servers, which could otherwise lead to SIP calls being diverted or disconnected, for example.

### SNMP ID:

2.33.4.1.1.30

### Telnet path:

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

# Possible values:

No

The strict mode is disabled.

Yes

The strict mode is enabled.

# Default:

Yes

# Strict-Mode

This option activates a security mechanism that stops the SIP user agent from processing SIP messages from unknown VoIP servers, which could otherwise lead to SIP calls being diverted or disconnected, for example.

## SNMP ID:

2.33.4.2.1.21

### Telnet path:

Setup > Voice-Call-Manager > Lines > SIP-PBX > PBX

### **Possible values:**

No

The strict mode is disabled.

Yes

The strict mode is enabled.

### Default:

Yes

# **14 RADIUS**

# 14.1 User-definable attributes in the RADIUS client

As of LCOS version 9.20, LANconfig provides the option to independently configure all of the RADIUS attributes for the communications with RADIUS servers.

In LANconfig, you configure the attributes under **Communication** > **RADIUS** in the sections **Authentication via RADIUS for PPP and clip** and **Tunnel authentication via RADIUS for L2TP**.

Authentication via RADIUS for P	PP and CLIP	
RADIUS server: Deactivated		RADIUS
Address:		]
Server port:	1.812	]
Source address (optional):	-	Select
Attribute values:		]
Secret:		Show
	Generate password	]
PPP operation:	Deactivated -	]
PPP authentication protocols:		
PAP CHA	P 📝 MS-CHAP	MS-CHAPv2
	Clip settings	]

Tunnel authentication via RADIUS for L2TP				
RADIUS server: Deactivated	✓ Protocols:	RADIUS		
Address:				
Port:	1.812			
Source address (optional):	-	Select		
Attribute values:				
Secret:		Show		
	Generate password			
Password:		Show		
	Generate password			

# Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <a href="https://www.commons.org">https://www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <b style="text-align: commons.org">www.commons.org</a> <b style="text-align: center;">www.commons.org</a> <b style="text-align: center;">wwww.commons.org</a> <b style="text-align: center;">www.commons.org</a> <b style="text-align: center;">www.commons

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

### %n

Device name

%**e** 

Serial number of the device

88

Percent sign

### %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

# 14.2 Automatic clean-up of access information on the RADIUS server

As of LCOS version 9.20, the function "Auto-Cleanup-Accounting-Totals" is enabled by default.

# 14.2.1 Additions to the Setup menu

# Auto-Cleanup-Accounting-Totals

Closed accounting sessions are deleted if the function "RADIUS cleanup user table" has removed the related RADIUS account.

### SNMP ID:

2.25.10.18

### Telnet path:

Setup > RADIUS > Server

# Possible values:

No

Accounting information is not automatically deleted.

Yes

Accounting information is deleted automatically.

### Default:

Yes

14 RADIUS

# 14.3 Vendor-specific RADIUS attribute "LCS-Routing-Tag"

As of LCOS version 9.20, the RADIUS client supports the vendor-specific RADIUS attribute "LCS-Routing-Tag" for PPTP, L2TP, and PPPoE.

A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Office communications with LANCAPI
- Time server

# 15.1 DHCP snooping: New variable for LAN MAC address

As of LCOS version 9.20, a dedicated variable is available for the LAN MAC address. This MAC address applies system-wide and also appears in the SysInfo and in LANconfig.

%r: Inserts the interface-independent (i.e. valid throughout the system) MAC address of the device that received the DHCP request.

# 15.2 DHCP lease time per network

As of LCOS version 9.20 it is possible to give each DHCP network its own lease time.

Carry out the configuration in LANconfig under IPv4 > DHCPv4 and click on DHCP networks.

DHCP networks - New E	ntry				? <mark>-</mark> ×
Network name:		✓ Select	Addresses for DHCP cli	ients	
DHCP server enabled:	Auto	•	First address:	0.0.0.0	
📄 Evaluate broadcast bi	t		Last address:	0.0.0.0	
DHCP cluster			Netmask:	0.0.0.0	
Forwarding of DHCP qu	ieries		Broadcast:	0.0.0.0	
1. server address:	0.0.0.0		Default gateway:	0.0.0.0	
2. server address:	0.0.0.0		Name server addresses		
3. server address:	0.0.0.0		Primary DNS:	0.0.0.0	
4. server address:	0.0.0.0		Secondary DNS:	0.0.0.0	
Place server replies	in intermediate storage		Primary NBNS:	0.0.0.0	
Adapt server replies	to the local network		Secondary NBNS:	0.0.0.0	
Lease time					
Maximum lease time:	0	minutes			
Default lease time:	0	minutes			
				ОК	Cancel

### Lease time of address assignments

In addition to the global default lease time configured under **IPv4** > **DHCPv4**, it is possible to configure a lease time specifically for this DHCP network only.

# Maximum lease time

Here you specify the maximum lease time that a client may request.

### Default lease time

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

# 15.2.1 Additions to the Setup menu

# Max.-Lease

In addition to the global maximum lease time configured under **Setup** > **DHCP**, it is possible to configure a maximum lease time specifically for this DHCP network only.

Here you specify the maximum lease time that a client may request.

### SNMP ID:

2.10.20.20

### **Telnet path:**

Setup > DHCP > Network-List

### **Possible values:**

Max. 5 characters from [0-9]

### Default:

0

### Special values:

0

There is no limit on the lease time that the DHCP client may request.

# Def.-Lease

In addition to the global default lease time configured under **Setup** > **DHCP**, it is possible to configure a default lease time specifically for this DHCP network only.

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

### SNMP ID:

2.10.20.21

# Telnet path:

Setup > DHCP > Network-List

Possible values: Max. 5 characters from [0-9] Default: 0 Special values: 0

There is no limit on the lease time that can be assigned to the DHCP client.

# 15.3 DHCP lease RADIUS accounting

As of LCOS version 9.20, LCOS supports DHCP RADIUS accounting.

# 15.3.1 DHCP lease RADIUS accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a RADIUS accounting start to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a RADIUS accounting stop. In between these two events, the DHCP server regularly sends the RADIUS server a RADIUS accounting interim update in a configurable interval.

To enable or disable RADIUS accounting for the DHCP server, go to **IPv4** > **DHCPv4** and click on the option **Activate DHCP lease RADIUS accounting**.

The input box **Accounting interim interval** configures the interval for the RADIUS interim updates. You configure the RADIUS accounting server and the corresponding backup server by clicking on **DHCP lease RADIUS accounting**.

DHCP lease RADIUS accou	inting - New Entry	? <mark>-×</mark> -
Network name:	-	Select
Server IP address:	0.0.0.0	
Port:	1.813	
Secret:		Show
	Generate password 🖛	
Source address (opt.):	-	Select
Protocol:	RADIUS 👻	
Attribute values:		
Backup server IP address:	0.0.0.0	
Backup server port:	1.813	
Backup server secret:		C Show
	Generate password 🖛	
Source address (opt.):	-	Select
Protocol:	RADIUS -	
Backup server attr. values:		
	ОК	Cancel

#### Network name

Select here the name of the network for which RADIUS accounting messages are to be sent.

### Server IP address

Enter the IP address or the DNS name of the RADIUS server (IPv4 or IPv6).

### Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port "1813".

### Key

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

### Source address (optional)

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS 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.

#### Protocol

Use this entry to specify the protocol used by the DHCP server to communicate with the RADIUS accounting server.

### Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <a href="https://www.commons.org">https://www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <a href="https://www.commons.org">www.commons.org</a> <b style="text-align: commons.org">www.commons.org</a> <b style="text-align: commons.org"<br/>
<b style="text-align: commons.org">www.commons.org</a> <b style="text-align: commons.org"<br/>
<b style="text-align: commons.org">www.commons.org</a> <br/>
<b style="text-align: commons.org"<br/>
<b style="text-align: commons.org">www.commons.org</a> <br/>
<b style="text-align: commons.org"<br/>
<b style="text-align: commons.org">www.commons.org</a> <br/>
<b style="text-align: commons.org"<br/>
<br/>
<b

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

88

Percent sign

### %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

### **Backup server IP address**

Enter the IP address or the DNS name of the backup RADIUS server.

### **Backup server port**

Enter the TCP port used by the backup RADIUS server to receive accounting information. That is usually the port "1813".

### Backup server secret

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

### Source address (optional)

Here you optionally specify an alternative source address that the DHCP server transfers to the backup RADIUS server.

### Protocol

Use this entry to specify the protocol that the DHCP server uses for the RADIUS accounting server.

#### Backup server attr. values

Here you specify any additional attribute values for the RADIUS communication with the backup server.

# 15.3.2 Additions to the Setup menu

# **RADIUS** accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a RADIUS accounting start to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a RADIUS accounting stop. In between these two events, the DHCP server regularly sends the RADIUS server a RADIUS accounting interim update in a configurable interval.

This menu contains the settings for the DHCP lease RADIUS accounting.

#### SNMP ID:

2.10.23

**Telnet path:** 

Setup > DHCP

### Operating

Enables or disables the RADIUS accounting on this DHCP network.

### SNMP ID:

2.10.23.1

### Telnet path:

Setup > DHCP > RADIUS-Accounting

### **Possible values:**

No

RADIUS accounting is disabled for this network.

Yes

RADIUS accounting is enabled for this network.

### Default:

No

### **Interim Interval**

Here you specify the time interval in seconds after which the DHCP server sends a RADIUS interim update to the accounting server.

### SNMP ID:

2.10.23.2

### Telnet path:

Setup > DHCP > RADIUS-Accounting

# Possible values:

Max. 10 characters from [0-9]

# Network list

This table contains the IP networks for the RADIUS accounting.

## SNMP ID:

2.10.23.20

# Telnet path:

Setup > DHCP > RADIUS-Accounting

# Network name

Contains the name of the network.

# SNMP ID:

2.10.23.20.1

# Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

# Possible values:

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

### Default:

empty

### Server host name

Enter the host name of the RADIUS accounting server here.

### SNMP ID:

2.10.23.20.2

### Telnet path:

 ${\tt Setup} > {\tt DHCP} > > {\tt RADIUS}{\tt -Accounting} > {\tt Network}{\tt -List}$ 

# Possible values:

Max. 64 characters from [A-Z][a-z][0-9].-:%

# Default:

empty

# Accnt.-Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port "1813".

### SNMP ID:

2.10.23.20.3

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

### **Possible values:**

Max. 5 characters from [0-9]

# Default:

1813

# Secret

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

### SNMP ID:

2.10.23.20.4

#### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

# Possible values:

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

# Default:

empty

# Loopback address

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS 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:

2.10.23.20.5

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

### **Possible values:**

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

### Default:

empty

# Protocol

Use this entry to specify the protocol used to communicate with the RADIUS accounting server.

### SNMP ID:

2.10.23.20.6

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

**Possible values:** 

RADIUS RADSEC

### Default:

RADIUS

## Attribute-Values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form <Attribute\_1>=<Value\_1>;<Attribute\_2>=<Value\_2>.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- NAS-Port=1234 is not allowed, because the attribute is not unique (NAS-Port, NAS-Port-Id or NAS-Port-Type).
- NAS-Id=ABCD is allowed, because the attribute is unique (NAS-Identifier).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications Service-Type=Framed and Service-Type=2 are identical.

Specifying a value in quotation marks (" <Value>") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (\"), as does the backslash itself (\\).

The following variables are permitted as values:

### %n

Device name

# %**e**

Serial number of the device

# 88

Percent sign

# %{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: Called-Station-Id=%{NAS-Identifier} sets the attribute Called-Station-Id to the value with the attribute NAS-Identifier.

### SNMP ID:

2.10.23.20.7

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

### **Possible values:**

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

#### Default:

empty

### Backup server hostname

Enter the host name of the backup server here.

### SNMP ID:

2.10.23.20.12

### Addendum

15 Other services

### Telnet path:

### Setup > DHCP > > RADIUS-Accounting > Network-List

# Possible values:

Max. 64 characters from [A-Z][a-z][0-9].-:%

# Default:

empty

## Backup-Accnt.-Port

Here you enter the backup port used by the backup RADIUS accounting server.

## SNMP ID:

2.10.23.20.13

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

## **Possible values:**

Max. 5 characters from [0-9]

# Default:

0

### **Backup secret**

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

# SNMP ID:

2.10.23.20.14

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

# Possible values:

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

# Default:

empty

# Backup-Loopback-Address

Specify a loopback address for the backup RADIUS accounting server.

### SNMP ID:

2.10.23.20.15

# Telnet path:

### Setup > DHCP > > RADIUS-Accounting > Network-List

# **Possible values:**

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

### Default:

empty

# **Backup-Protocol**

Use this entry to specify the protocol used to communicate with the backup RADIUS accounting server.

### SNMP ID:

2.10.23.20.16

# Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

### **Possible values:**

RADIUS RADSEC

# Default:

RADIUS

# **Backup attribute values**

Here you specify the attribute values for the backup RADIUS accounting server.

# SNMP ID:

2.10.23.20.17

### Telnet path:

Setup > DHCP > > RADIUS-Accounting > Network-List

# Possible values:

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

## Default:

empty

# 15.4 SNMPv3 support

With version 9.20, LCOS now supports SNMPv3 to provide the following versions of SNMP:

- SNMPv1
- SNMPv2c
- SNMPv3

# 15.4.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) enables devices on a network to be monitored and configured from a central instance. Since the initial release of SNMPv1 in 1988, it has continued to evolve with the versions SNMPv2 and SNMPv3 to meet the needs of increasingly complex network infrastructures and the demands for user-friendliness, security and flexibility.

The protocol SNMP (simple network management protocol) meets the highest standards for convenient management and monitoring of a network. It allows for the early detection of problems and errors on a network and offers support in eliminating them. The simple network management protocol allows a central instance to monitor and configure the devices on a network from, and it regulates the communication between the monitored devices and the monitoring station. This means that parameters such as the status of the device, CPU utilization, the temperature of a device, its connection status, errors, and others can be monitored and analyzed with LANmonitor or LSM. The administrator benefits from active support with network management and is helped to detect problems at an early stage. The latest SNMPv3 version of the protocol, in contrast to the previous versions SNMPv1 and SNMPv2, now enables encrypted data communication between the network and its management system, which provides a crucial security factor. By offering different user accounts for authentication, the integrated user administration provides optimal control over access to the configurations. You have precise control over the rights to the different levels of access that administrators receive, and the network is optimally protected.

# **SNMP** components

The typical SNMP architecture consists of three components:

# **SNMP** manager

The SNMP manager sends SNMP requests to the SNMP agent and evaluates the SNMP responses from it. The LCMS tools LANconfig and LANmonitor are SNMP managers of this type. LANCOM devices comply with the standards SNMPv1, SNMPv2, and SNMPv3, so it is possible to use an alternative SNMP administration and management software.

# **SNMP** agent

The SNMP agent is a module that is active on the managed device. When it receives a request from the SNMP manager, it retrieves the requested status data from the MIB in the device and returns this information to the SNMP manager as an "SNMP response". Depending on the configuration, an SNMP agent that detects certain changes of state in the managed device can independently act to send an "SNMP trap" to the SNMP manager. It is also possible to send a notification to the device administrator by means of a SYSLOG message or an e-mail.

# Managed device

The status of this device is stored in its Management Information Base (MIB). When requested by the SNMP agent, the device reads out this information and returns it to the SNMP agent.

By default, SNMP requests and SNMP responses are exchanged between the SNMP manager and SNMP agent by the User Datagram Protocol (UDP) on port 161. SNMP traps are transmitted with the UDP via port 162 by default.

### **SNMP** versions

The differences between the various versions of SNMP can be summarized as follows:

### SNMPv1

Version 1 was launched in 1988 and has long been regarded as the de facto standard for network management. In SNMPv1, the SNMP manager authenticates at the SNMP agent by means of a community string, which must be identical on both components. The security of this is very limited, as the community strings are transmitted in cleartext. The increase in demands for secure network communication necessitated a revision of version 1.

### SNMPv2

After 1993, the main improvements in version 2 were to its user-friendliness. Numerous intermediate steps and the repeated rejection of concepts eventually led to the version SNMPv2c. This version allows large amounts of data to be requested via a GetBulkRequest command and also the communication between SNMP managers. However, the exchange of the community strings was still as cleartext as with version 1.

### SNMPv3

From 1999, version 3 finally met the by then much-needed security requirements. Among other things, the communication was encrypted and the communication partners first had to authenticate and authorize themselves. Also, the structure of SNMP became more modular so that improvements, for example in encryption technologies, can be incorporated into SNMPv3, without having to completely redesign the standard.

LCOS supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

# **SNMPv3** basics

The SNMP protocol structure has changed significantly with version 3. SNMPv3 is now divided into a number of modules with clearly defined interfaces that communicate with one another. The three main elements in SNMPv3 are "Message Processing and Dispatch (MPD)", "User-based Security Model (USM)" and "View-based Access Control Mechanism (VACM)".

### MPD

The MPD module is responsible for the processing and dispatch of inbound and outbound SNMP messages.

### USM

The USM module manages security features that ensure the authentication of the users and the encryption and integrity of the data. SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

### VACM

VACM ensures that the sender of an SNMP request is entitled to receive the requested information. The associated access permissions are found in the following settings and parameters:

### SNMPv3-Views

"SNMPv3-Views" collect together the content, status messages, and actions of the Management Information Base (MIB) that are permitted to receive or execute an SNMP request. These views can be single values, but also complete paths of the MIB. This content is specified by the OIDs of the MIB entries. In this way, a successfully authenticated sender of an SNMP request only has access to that data specified in the applicable SNMPv3 views.

### SNMPv3-Groups

"SNMPv3-Groups" collect users with the same permissions into a specific group.

### Security-Levels

"Security levels" relate to the exchange of SNMP messages. The following levels can be selected:

### NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

### Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

### Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

### Context

"Context" is used to distinguish the various SNMP entities.

# Setting up SNMP with LANconfig

In LANconfig you configure SNMP under **Management** > **Admin** in the section **SNMP** and by clicking on **SNMP** settings.

SNMP settings	? 💌		
Protocol versions			
SNMPv1	SNMPv2		
V SNMPv3			
SNMPv3 access settings for adm	ninistrators		
Decide whether administrators can access the device through SNMPv3 or not.			
Administrators have SNMPv3 device access rights	access according to their		
SNMP communities	Users		
	Groups		
Access rights	Views		
Traps			
Target addresses	Target parameters		
	OK Cancel		

### **Protocol versions**

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

### SNMPv3 access settings for administrators

Enable this option if registered administrators should also have access via SNMPv3.

### **SNMP** communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This configuration is relevant for the SNMP versions v1 and v2c only.

SNMP communities - New	v Entry	? 💌
📝 Entry active		
Name:		
Security name:	DEFAULT	
	ОК	Cancel

(i) The SNMP community public is set up by default, and this provides unrestricted SNMP read access.

# **Entry active**

Activates or deactivates this SNMP community.

### Name

Enter a descriptive name for this SNMP community.

### Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

### Users

Individual users can be granted access to the device in addition to the administrators registered on it. Here you configure the authentication and encryption settings for these users when operating SNMPv3.

Users - New Entry	? 💌
🔽 Entry active	
User name:	
Authentication:	HMAC-SHA 👻
Password for auth.	Show
	Generate password 💌
Privacy:	AES128 -
Password for priv.	Show
	Generate password 💌
	OK Cancel

### **Entry active**

Activates or deactivates this user.

### User name

Enter a descriptive name for this user.

# Authentication

Specify the method that the user is required to use to authenticate at the SNMP agent. The following options are available:

### None

Authentication of the user is not necessary.

# HMAC-MD5

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

# HMAC-SHA (default)

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

# Password for auth.

Enter the user password necessary for authentication here and repeat it in the box below.

## Encryption

Specify which encryption method is used for encrypted communication with the user. The following options are available:

### None

Communication is not encrypted.

# DES

Encryption is performed with DES (key length 56 bits).

# AES128 (default)

Encryption is performed with AES128 (key length 128 bits)

# AES192

Encryption is performed with AES192 (key length 192 bits)

# AES256

Encryption is performed with AES256 (key length 256 bits)

# Password for priv.

Enter the user password required by the encryption here and repeat it in the box below.

### Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.

Groups - New Entry		? 💌
📝 Entry active		
Group name:	•	Select
User/Security name:	•	Select
Security model:	SNMPv3 (USM) 🔷 🔻	]
	ОК	Cancel

### **Entry active**

Activates or deactivates this group.

### Group name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

### User/security name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

### Security model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly. Select one of the following entries accordingly:

# SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

### SNMPv2

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

### SNMPv3 (USM)

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

### NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

### AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

### AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.



### Access rights

This table brings together the different configurations for access rights, security models, and views.

Access rights - New Entry			? <mark>×</mark>
Country active		_	
Security model:	SNMPv3 user secur	•	
Minimal security level:	Authentication and p	•	
Readonly view:		•	Select
Write view:		•	Select
	ОК		Cancel

# **Entry active**

Activates or deactivates this entry.

# Group name

Here you select the name of a group that is to receive these assess rights.

### Security model

Activate the appropriate security model here.

### Minimal security level

Specify the minimum security level for access and data transfer.

### **Read-only view**

Set the view of the MIB entries for which this group is to receive read rights.

# Write view

Set the view of the MIB entries for which this group is to receive write rights.

# Views

Here you collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with the corresponding access rights.

Views - New Entry		? <mark>×</mark>
🔽 Entry active		
Name:		
Access to subtree:	added 💌	
OID subtree:		
	OK	Cancel

### **Entry active**

Activates or deactivates this view.

# Name

Give the view a descriptive name here.

### Access to subtree

Here you decide whether the OID subtrees specified in the following are "added" or "removed" from the view.

### **OID** subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.



The OIDs are taken from the device MIB, which you can download with WEBconfig under **Extras** > **Get Device SNMP MIB**.

### **Target addresses**

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.

Target addresses - New Er	itry 🧮	? 🗙
Name:		
Transport address:		
Target parameter name:	▼ Se	elect
	OK Ca	ancel

#### Name

Give the entry a descriptive name here.

# **Transport address**

Configure the address of the recipient here.

### Target parameter name

Here you select the desired entry from the list of recipient parameters.

# Target parameter name

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.

Target parameters - New E	ntry	? 🔀
Name:		
Message processing model:	SNMPv1 -	
Security name:	•	Select
Security model:	SNMPv1	
Security level:	No auth./No privacy. 💌	
	OK	Cancel

#### Name

Give the entry a descriptive name here.

### Message processing model

Here you specify the protocol for which the SNMP agent structures the message.

### Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

### Security model

Activate the appropriate security model here.

### Security level

Set the security level that applies for the recipient to receive the SNMP trap.

# No authentication/No privacy

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

# Authentication/No privacy

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

### Authentication and privacy

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

# 15.4.2 Configuring SNMP read-only access

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a "community". Authentication is optionally handled

- by the public community (unlimited SNMP read access),
- by a master password (limited SNMP read access), or
- a combination of user name and password, separated by a colon (limited SNMP read access)

. By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community public. Because this represents a potential security risk, especially with external access, LANconfig gives you the option define your own communities under **Management** > **Admin** and clicking **SNMP settings** and **SNMP communities**.

Entry active	Name	Secu	rity name				ОК
On public DEFi			AULT	- New Entry	2 2		Cancel
			☑ Entry active Name:				
🖓 QuickFine	fer		Security name:	DEFAULT		temove	

For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the public community in the list of the SNMP communities. 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. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community public has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

SNMP write access is reserved exclusively for administrators with the appropriate permissions.

For more information about SNMP, see the chapter *Simple Network Management Protocol (SNMP)* 

# 15.4.3 Additions to the Setup menu

# Communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This table is used to configure the SNMP communities.

The SNMP community public is set up by default, and this provides unrestricted SNMP read access.

### SNMP ID:

2.9.27

Telnet path: Setup > SNMP

# Name

Enter a descriptive name for this SNMP community.

### SNMP ID:

2.9.27.1

### Telnet path:

Setup > SNMP > Communities

### **Possible values:**

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

### Default:

empty

### Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

### SNMP ID:

2.9.27.3

Telnet path: Setup > SNMP > Communities

### Addendum

15 Other services

### Possible values:

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

### Default:

empty

# Status

This entry is used to enable or disable this SNMP community.

### SNMP ID:

2.9.27.8

# Telnet path:

Setup > SNMP > Communities

# Possible values:

Active

The community is enabled.

# Inactive

The community is disabled.

# Default:

Active

# Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.

### SNMP ID:

2.9.28

### Telnet path:

Setup > SNMP

## Security-Model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

You select a security model here as is appropriate.

#### SNMP ID:

2.9.28.1

### Telnet path:

Setup > SNMP > Groups

# Possible values:

### SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

### SNMPv2

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

### SNMPv3(USM)

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

#### NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

### AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

### AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

### Default:

SNMPv3(USM)

### Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

### SNMP ID:

2.9.28.2

### Telnet path:

Setup > SNMP > Groups

### **Possible values:**

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

### Default:

empty

# Group-Name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

### SNMP ID:

2.9.28.3

# Telnet path:

Setup > SNMP > Groups

# **Possible values:**

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

### Default:

empty

# Status

Activates or deactivates this group configuration.

### SNMP ID:

2.9.28.5

Telnet path: Setup > SNMP > Groups

**Possible values:** 

Active Down

# Default:

Active

# Access

This table brings together the different configurations for access rights, security models, and views.

# SNMP ID:

2.9.29

Telnet path:

Setup > SNMP

## Group-Name

Here you select the name of a group that is to receive these assess rights.

### SNMP ID:

2.9.29.1

# Telnet path:

Setup > SNMP > Access

## **Possible values:**

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

### Default:

empty

# Security model

Activate the appropriate security model here.

### SNMP ID:

2.9.29.3

Telnet path: Setup > SNMP > Access

# **Possible values:**

Any

Any model is accepted.

# SNMPv1

SNMPv1 is used.

# SNMPv2

SNMPv2c is used.

# SNMPv3(USM)

SNMPv3 is used.

### Default:

Any

### Addendum

15 Other services

### **Read-View-Name**

Set the view of the MIB entries for which this group is to receive read rights.

# SNMP ID:

2.9.29.5

### Telnet path:

Setup > SNMP > Access

# Possible values:

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

## Default:

empty

# Write-View-Name

Set the view of the MIB entries for which this group is to receive write rights.

### SNMP ID:

2.9.29.6

### Telnet path:

Setup > SNMP > SNMPv3-Accesses

## **Possible values:**

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

### Default:

empty

# Notify-View-Name

Set the view of the MIB entries for which this group is to receive notify rights.

# SNMP ID:

2.9.29.7

## **Telnet path:**

Setup > SNMP > Access

### Possible values:

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

### Default:

empty
### Status

Activates or deactivates this entry.

#### SNMP ID:

2.9.29.9

#### Telnet path:

Setup > SNMP > Access

#### **Possible values:**

Active Down

#### Default:

Active

#### **Min-Security-Level**

Specify the minimum security level for access and data transfer.

#### SNMP ID:

2.9.29.10

#### Telnet path:

Setup > SNMP > Access

#### **Possible values:**

#### **NoAuth-NoPriv**

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

#### Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

### Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

#### Default:

Auth-Priv

### Views

This table is used to collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with their corresponding access rights.

SNMP ID:

2.9.30

Telnet path: Setup > SNMP

### View-Name

Give the view a descriptive name here.

#### SNMP ID:

2.9.30.1

### Telnet path:

Setup > SNMP > Views

#### **Possible values:**

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

### Default:

empty

### **OID-Subtree**

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.

The OIDs are taken from the device MIB, which you can download with WEBconfig under Extras > Get Device SNMP MIB.

### SNMP ID:

2.9.30.2

### Telnet path:

Setup > SNMP > Views

#### **Possible values:**

Max. 128 characters from [A-Z][a-z][0-9]@{|}~!\$%&'()+-,/:;<=>?[\]^\_.`

#### Default:

empty

### Туре

Here you decide whether the OID subtrees specified in the following are "Included" or "Excluded" from the view.

#### SNMP ID:

2.9.30.4

#### Telnet path:

Setup > SNMP > Views

#### **Possible values:**

Included

This setting outputs MIB values.

### Excluded

This setting blocks the output of MIB values.

### Default:

Included

### Status

Activates or deactivates this view.

### SNMP ID:

2.9.30.6

#### Telnet path:

Setup > SNMP > Views

### **Possible values:**

Active Down

#### Default:

Active

### SNMPv3-Users

This menu contains the user configuration.

### SNMP ID:

2.9.32

15 Other services

Telnet path:

Setup > SNMP

#### User name

Specify the SNMPv3 user name here.

#### SNMP ID:

2.9.32.2

### Telnet path:

Setup > SNMP > SNMPv3-Users

### **Possible values:**

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

### Default:

empty

### Authentication-Protocol

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

### SNMP ID:

2.9.32.5

Telnet path: Setup > SNMP > Users

### **Possible values:**

#### None

Authentication of the user is not necessary.

# HMAC-MD5

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

### HMAC-SHA

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

### Default:

HMAC-SHA

#### Authentication-Password

Enter the user password necessary for authentication here and repeat it in the box below.

#### SNMP ID:

2.9.32.6

### Telnet path:

Setup > SNMP > Users

### **Possible values:**

```
Max. 40 characters from [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
```

#### Default:

empty

### **Privacy-Protocol**

Specify which encryption method is used for encrypted communication with the user.

#### SNMP ID:

2.9.32.8

### Telnet path:

Setup > SNMP > SNMPv3-Users

#### Possible values:

### None

Communication is not encrypted.

### DES

Encryption is performed with DES (key length 56 bits).

### AES128

Encryption is performed with AES128 (key length 128 bits).

### AES192

Encryption is performed with AES192 (key length 192 bits).

### AES256

Encryption is performed with AES256 (key length 256 bits)

#### Default:

AES128

### **Privacy-Password**

Enter the user password required by the encryption here and repeat it in the box below.

#### SNMP ID:

2.9.32.9

15 Other services

### Telnet path:

Setup > SNMP > Users

### Possible values:

Max. 40 characters from  $[A-Z][a-z][0-9]#@{|}~!$  %&'() \*+-, /:; <=>?[\]^\_. `

### Default:

empty

### Status

Activates or deactivates this user.

### SNMP ID:

2.9.32.13

### Telnet path:

Setup > SNMP > Users

### Possible values:

Active Down

### Default:

Active

### **SNMPv3-Notifiers**

This menu contains the table with the SNMPv3 notifications.

### SNMP ID:

2.9.33

### Telnet path:

Setup > SNMP

### Notify-Name

Enter a name for this notifier here.

### SNMP ID:

2.9.33.1

#### Telnet path:

Setup > SNMP > SNMPv3-Notifiers

### **Possible values:**

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

### Default:

empty

### Notify-Tag

Enter the notifier tag here.

### SNMP ID:

2.9.33.2

#### Telnet path:

Setup > SNMP > SNMPv3-Notifiers

### Possible values:

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

#### Default:

empty

### Notify-Type

Contains the notification types.

### SNMP ID:

2.9.33.3

### Telnet path:

Setup > SNMP > SNMPv3-Notifiers

**Possible values:** 

**NOTIFICATION-TRAP** 

### Default:

NOTIFICATION-TRAP

### **Target-Address**

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.

#### SNMP ID:

2.9.34

### Telnet path:

 $\mathbf{Setup} > \mathbf{SNMP}$ 

### Target-Address-Name

Specify the target address name here.

#### SNMP ID:

2.9.34.1

### Telnet path:

Setup > SNMP > Target-Address

### Possible values:

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

### Default:

empty

### Target-Transport-Address

Contains the IP address which the SNMP traps are sent to.

### SNMP ID:

2.9.34.3

### Telnet path:

Setup > SNMP > Target-Address

### **Possible values:**

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

#### Default:

empty

### Target-Tag-List

Contains a tag list for defining target addresses for specific tasks.

### SNMP ID:

2.9.34.6

#### Telnet path:

Setup > SNMP > Target-Address

### **Possible values:**

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

### Default:

empty

### **Parameters-Name**

Here you select the desired entry from the list of recipient parameters.

### SNMP ID:

2.9.34.7

### Telnet path:

Setup > SNMP > Target-Address

### Possible values:

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

#### Default:

empty

### **Target-Params**

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.

### SNMP ID:

2.9.35

Telnet path: Setup > SNMP

### Name

Give the entry a descriptive name here.

### SNMP ID:

2.9.35.1

### Telnet path:

Setup > SNMP > Target-Params

15 Other services

### **Possible values:**

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

### Default:

empty

### Message-Processing-Model

Here you specify the protocol for which the SNMP agent structures the message.

### SNMP ID:

2.9.35.2

### Telnet path:

Setup > SNMP > Target-Params

Possible values:

SNMPv1 SNMPv2c SNMPv3

### Default:

SNMPv3

### Security model

Use this entry to specify the security model.

### SNMP ID:

2.9.35.3

### Telnet path:

Setup > SNMP > Target-Params

#### **Possible values:**

SNMPv1 SNMPv2 SNMPv3(USM)

### Default:

SNMPv3(USM)

#### Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

#### SNMP ID:

2.9.35.4

#### Telnet path:

Setup > SNMP > Target-Params

#### **Possible values:**

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

#### Default:

empty

#### Security-Level

Set the security level that applies for the recipient to receive the SNMP trap.

#### SNMP ID:

2.9.35.5

#### Telnet path:

Setup > SNMP > Target-Params

#### **Possible values:**

#### **NoAuth-NoPriv**

The SNMP message is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

### Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

#### Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

#### Default:

NoAuth-NoPriv

### Notification-Server-Enable

This entry specifies whether the server notification is enabled or disabled.

#### SNMP ID:

2.9.36

### Telnet path:

 $\mathbf{Setup} > \mathbf{SNMP}$ 

### Possible values:

No

Server notification is disabled.

#### Yes

Server notification is enabled.

### Default:

No

### **Admitted-Protocols**

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

### SNMP ID:

2.9.37

Telnet path:

Setup > SNMP

Possible values:

SNMPv1 SNMPv2 SNMPv3

Default:

SNMPv1

SNMPv2

SNMPv3

### SNMPv3-Allow-Admins

Enable this option if registered administrators should also have access via SNMPv3.

#### SNMP ID:

2.9.38

Telnet path: Setup > SNMP Possible values: No Yes Default: Yes

### SNMPv3-Admin-Authentication

Sets the authorization method for administrators.



SNMP ID:

2.9.39

Telnet path:

Setup > SNMP

**Possible values:** 

AUTH-HMAC-SHA

#### Default:

AUTH-HMAC-SHA

### SNMPv3-Admin-Privacy

Specifies the encryption settings for administrators.

(i) This value cannot be modified.

SNMP ID:

2.9.40

Telnet path: Setup > SNMP

15 Other services

Possible values:

AES256

Default:

AES256

### Operating

This entry enables or disables SNMP traps. Clear the checkbox to disable SNMP traps.

SNMP ID:			
2.9.41			
Telnet path: Setup > SNMP			
Possible values:			
No Yes			
Default:			
Yes			

# 15.5 Logging DNS queries with SYSLOG

As of LCOS version 9.20, the DNS server on the device sends DNS responses to the clients and also as SYSLOG messages to a SYSLOG server.

With the move to LCOS version 9.20, LCOS converts existing table entries into the new form. In case you downdate to an earlier LCOS version, any changes you make with LCOS version 9.20 will be lost (e.g. entries for IP addresses). As long as the device configuration remains unchanged since you updated to LCOS version 9.20, it is possible to downdate to an earlier LCOS version without losing data.

## 15.5.1 Logging DNS queries with SYSLOG

In order to document the requests from the clients to the DNS server in the device, this option allows the server to additionally send its responses to clients as SYSLOG messages to a SYSLOG server on a continual basis.

Please be aware that recording DNS requests must be performed in accordance with the applicable data privacy regulations in your country.

In LANconfig, you configure the documentation of DNS requests under IPv4 > DNS in the section SYSLOG.

SYSLOG		
DNS replies to clients can be logged to an external SYSLOG server.		
🔽 Log DNS resolutions to an exte	rnal SYSLOG server	
Server address:		
	Advanced	

### Log the DNS resolutions on an external SYSLOG server

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under Log & Trace > General > SYSLOG. Thus, if you enable this option to log DNS requests, the DNS server sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (ANSWER record or ADDITIONAL record) generates a SYSLOG message with the following structure PACKET\_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record.

The parameters have the following meanings:

- The TID (transaction ID) contains a 4-character hexadecimal code.
- The {host name} is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The resource record consists of three parts: The request, the type or class, and the IP resolution (for example www.mydomain.com STD A resolved to 193.99.144.32)

#### Server address

Enter the address of the SYSLOG server. You can enter an IPv4/IPv6 address or a DNS name.

The use of the IP addresses 127.0.0.1 and :: 1 to force the use of an external server is not permitted.

To configure the SYSLOG message, click on Advanced.

Advanced		? 🗙
Source:	Router	
Priority:	Notice •	
Source address (optional):	INTRANET -	Select
	OK	Cancel

#### Source

Here you select which source is entered in the SYSLOG messages.

#### Priority

Here you select the source that is entered in the SYSLOG messages.

### Source address (optional)

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

(1) If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

For more information on SYSLOG and the available settings, see the section *The SYSLOG module*.

### 15.5.2 Additions to the Setup menu

### Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

#### SNMP ID:

2.17.20

Telnet path:

Setup > DNS

#### Log DNS resolutions

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under Setup > SYSLOG > Operating. If you enable this option to log DNS requests, the DNS server in the device sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (ANSWER record or ADDITIONAL record) generates a SYSLOG message with the following structure PACKET\_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record.

The parameters have the following meanings:

- The TID (transaction ID) contains a 4-character hexadecimal code.
- The {host name} is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The resource record consists of three parts: The request, the type or class, and the IP resolution (for example www.mydomain.com STD A resolved to 193.99.144.32)

#### SNMP ID:

2.17.20.1

#### **Telnet path:**

Setup > DNS > Syslog

### **Possible values:**

No

Disables the logging of DNS requests and responses.

Yes

Enables the logging of DNS requests and responses.

Default:

No

### Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.

(i) The use of the IP addresses 127.0.0.1 and ::1 to force the use of an external server is not permitted.

#### SNMP ID:

2.17.20.2

#### Telnet path:

Setup > DNS > Syslog

### **Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-:%

### Log source

Contains the log source as displayed in the SYSLOG messages.

#### SNMP ID:

2.17.20.3

#### Telnet path:

Setup > DNS > Syslog

#### **Possible values:**

System Login System time Console login Connections Accounting Administration Router

#### Default:

Router

### Log level

Contains the priority that is shown in the SYSLOG messages.

#### SNMP ID:

2.17.20.4

Telnet path: Setup > DNS > Syslog

Possible values:

Emergency Alert Critical Error Warning Notice Info Debug

#### Default:

Notice

#### Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.



If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

#### SNMP ID:

2.17.20.5

**Telnet path:** 

```
Setup > DNS > Syslog
```

#### **Possible values:**

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

**Special values:** 

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

### Source

Here you select which source is entered in the SYSLOG messages.

### SNMP ID:

2.22.2.3

Telnet path:

Setup > SYSLOG > SYSLOG table

**Possible values:** 

None System Login System time Console login Connections Accounting Administration Router

### Default:

None

### Level

Here you select the source that is entered in the SYSLOG messages. Multiple entries can be selected.

### SNMP ID:

2.22.2.4

#### Telnet path:

Setup > SYSLOG > SYSLOG table

### Possible values:

None Alert Error Warning Info Debug

### Default:

None

### **IP** address

Contains the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a DNS name.

### SNMP ID:

2.22.2.7

### Telnet path:

Setup > SYSLOG > SYSLOG table

### **Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-:%

### Facility

The mapping of sources to specific facilities.

### SNMP ID:

2.22.3.2

# Telnet path:

Setup > SYSLOG > Facility-Mapper

15 Other services

Possible values:

KERN USER MAIL DAEMON AUTH SYSLOG LPR NEWS UUCP CRON AUTHPRIV **SYSTEM0** SYSTEM1 SYSTEM2 SYSTEM3 SYSTEM4 LOCAL0 LOCAL1 LOCAL2 LOCAL3 LOCAL4 LOCAL5 LOCAL6 LOCAL7