

■ connecting your business



Addendum

LCOS 9.00 RC2

Contents

1 Addendum to LCOS version 9.00.....	7
2 LCMS.....	8
2.1 Enhancements to LANconfig.....	8
2.1.1 Automatic authentication for read-only access to LANmonitor.....	8
2.1.2 Display of administrator user name.....	8
2.1.3 Authenticating against a proxy server.....	9
2.2 Enhancements to LANmonitor.....	10
2.2.1 Internal IPv6 support.....	10
2.2.2 Displaying static WAN IPs in the Status tree.....	10
3 Configuration.....	16
3.1 Output additional ports in SYSINFO at the console	16
3.2 Specifying a custom SNMP port.....	16
3.2.1 Additions to the Setup menu.....	16
3.3 Password protection for WLAN keys.....	17
3.4 Sorted display of a menu on the console.....	17
3.5 Customize the management ports for device access.....	17
3.5.1 Additions to the Setup menu.....	18
3.6 Comment box for access stations.....	18
3.6.1 Additions to the Setup menu.....	19
3.7 Elliptic curve cryptography (ECC).....	19
3.7.1 Additions to the Setup menu.....	20
3.8 Changing the SIM card PIN.....	33
3.8.1 Additions to the Status menu.....	33
3.8.2 Additions to the Setup menu.....	34
4 IPv6.....	35
4.1 Dual-Stack Lite (DS-Lite).....	35
4.1.1 Additions to the Status menu.....	36
4.1.2 Additions to the Setup menu.....	40
4.2 IPv6 support for RAS services.....	41
4.2.1 RAS interfaces.....	41
4.2.2 Prefix pools.....	43
4.2.3 Additions to the Setup menu.....	43
4.3 RADIUS attribute extensions for IPv6 RAS services.....	50
4.4 Loopback addresses for IPv6.....	51
4.4.1 Loopback addresses.....	51
4.4.2 Additions to the Setup menu.....	51
4.5 Lightweight DHCPv6 relay agent (LDRA).....	53
4.5.1 Additions to the Setup menu.....	55
4.6 Router advertisement snooping.....	58
4.6.1 Additions to the Setup menu.....	59

5 RADIUS.....	62
5.1 Separate RADIUS accounting server for each SSID	62
5.1.1 Additions to the Setup menu.....	62
5.2 Accessing the RADIUS server via IPv6.....	66
5.2.1 Additions to the Setup menu.....	67
5.3 New attribute in the RADIUS server, shell privilege level.....	68
5.3.1 Using RADIUS to login to the LCOS management GUI.....	68
5.3.2 Additions to the Setup menu.....	70
5.4 RADIUS client: Alternative input of hostnames instead of IP addresses.....	72
5.4.1 Additions to the Setup menu.....	72
5.5 EAP-SIM module in the RADIUS server.....	76
5.5.1 Additions to the Setup menu.....	76
6 Public Spot.....	82
6.1 Number format for Smart Ticket.....	82
6.2 Viewing Public Spot clients.....	82
6.3 Displaying advertising to Public Spot users.....	82
6.3.1 Additions to the Setup menu.....	83
6.3.2 Extensions to the RADIUS attributes.....	87
6.4 Additional attributes for the XML interface.....	87
6.5 Dynamic change of a user session via the XML interface.....	88
7 WLAN.....	90
7.1 Support of 802.11ac WLAN interfaces.....	90
7.1.1 Additions to the Status menu.....	90
7.2 Specifying client-bridge mode and bandwidth limit for each SSID.....	103
7.2.1 Additions to the Setup menu.....	104
7.3 Separation of P2P and WLAN/SSID configuration.....	107
7.3.1 Configuration of P2P connections.....	107
7.3.2 Additions to the Setup menu.....	108
7.4 Flexible WLAN capture format.....	125
7.4.1 Additions to the Setup menu.....	125
7.5 Band steering with delayed scan at 2.4 GHz.....	126
7.5.1 Additions to the Setup menu.....	126
7.6 Advanced wireless LAN traces.....	127
7.6.1 Additions to the Setup menu.....	128
7.7 Fast roaming as per IEEE 802.11r.....	129
7.7.1 Fast roaming.....	129
7.7.2 Configuration.....	130
7.7.3 Additions to the Status menu.....	131
7.7.4 Additions to the Setup menu.....	132
7.8 WPA2 with AES as factory setting.....	133
7.9 WLAN protected management frames (PMF).....	134
7.9.1 Additions to the Status menu.....	136
7.9.2 Additions to the Setup menu.....	141
7.10 Redundant connections using PRP.....	143

7.10.1 Basic function.....	143
7.10.2 Advantages of WLAN PRP.....	144
7.10.3 Implementation of PRP in the access points.....	144
7.10.4 Dual roaming.....	144
7.10.5 Diagnostic options.....	145
7.10.6 Tutorial: Setting up a PRP connection over a point-to-point network (P2P).....	146
7.10.7 Tutorial: Roaming with a dual-radio client and PRP.....	148
7.10.8 Additions to the Setup menu.....	150
8 WLAN management.....	159
8.1 AutoWDS – wireless integration of APs via P2P connections.....	159
8.1.1 Notes on operating AutoWDS.....	161
8.1.2 How it works.....	163
8.1.3 Setup by means of preconfigured integration.....	169
8.1.4 Accelerating preconfigured integration by pairing.....	171
8.1.5 Express integration.....	171
8.1.6 Switching from express to preconfigured integration.....	172
8.1.7 Manual topology management.....	172
8.1.8 Redundant paths by means of RSTP.....	175
8.1.9 Additions to the Status menu.....	176
8.1.10 Additions to the Setup menu.....	205
8.2 IP-dependent auto configuration and tagging of APs.....	222
8.2.1 Setting up assignment groups for IP-dependent auto configuration.....	223
8.2.2 Setting up tag groups for the detailed selection of APs.....	224
8.2.3 Additions to the Status menu.....	224
8.2.4 Additions to the Setup menu.....	231
8.2.5 Enhancements to command-line commands	235
8.3 Automatic selection of the 2.4-/5-GHz mode.....	237
8.3.1 Additions to the Status menu.....	238
8.3.2 Additions to the Setup menu.....	239
8.4 WLC cluster.....	241
8.4.1 WLC tunnel for internal communication.....	241
8.4.2 Setting up a CA hierarchy.....	246
8.4.3 Enabling/disabling CAPWAP in the WLC.....	252
8.4.4 Finding the ideal WLC.....	253
8.4.5 Determining the ideal AP distribution.....	254
8.4.6 Manually initiate ideal AP distribution.....	254
8.5 One-click backup of the SCEP-CA.....	254
8.6 Automatic restart of managed APs after firmware update.....	255
8.6.1 Load firmware in managed AP.....	255
8.7 Automatic search for alternative WLCs.....	255
8.8 U-APSD configurable by WLC.....	255
8.8.1 Additions to the Status menu.....	255
8.8.2 Additions to the Setup menu.....	256
8.9 Group-related radio field optimization.....	257

8.10 Adding new APs with the WEBconfig Setup Wizard.....	258
8.10.1 Additions to the Status menu.....	258
8.11 Maximum bandwidth can be adjusted for each WLAN module.....	259
8.11.1 Additions to the Status menu.....	261
8.11.2 Additions to the Setup menu.....	263
8.12 Client-steering by the WLC.....	265
8.12.1 Configuration.....	266
8.12.2 Additions to the Status menu.....	268
8.12.3 Additions to the Setup menu.....	270
8.13 Automatic frequency-band selection.....	275
8.13.1 Additions to the Setup menu.....	276
9 VPN.....	278
9.1 VPN remote access wizard in WEBconfig:.....	278
9.2 L2TPv2 (Layer-2 Tunneling Protocol version 2).....	278
9.2.1 Configuring the L2TP tunnel.....	279
9.2.2 Authentication via RADIUS.....	281
9.2.3 Operation as an L2TP access concentrator (LAC).....	282
9.2.4 Operation as the L2TP network server (LNS) for RAS clients.....	284
9.2.5 Operation as an L2TP network server (LNS) with authentication via RADIUS.....	285
9.2.6 Additions to the Status menu.....	287
9.2.7 Additions to the Setup menu.....	295
9.3 Support of the DH groups 15 and 16.....	322
9.3.1 Additions to the Setup menu.....	322
10 Routing and WAN connections.....	327
10.1 Revised flow control.....	327
10.1.1 Additions to the Status menu.....	327
10.1.2 Additions to the Setup menu.....	328
10.2 AC name configurable for PPPoE server.....	329
10.2.1 Additions to the Setup menu.....	329
10.3 Dual-SIM support for mobile devices.....	330
10.3.1 Configuring WWAN access.....	330
10.3.2 Switching between mobile profiles or SIM cards.....	334
10.3.3 Additions to the Status menu.....	334
10.3.4 Additions to the Setup menu.....	334
10.4 Combined UMTS-GPRS operation for LTE devices.....	335
10.4.1 Additions to the Setup menu.....	335
11 Other services.....	336
11.1 Deactivating device LEDs – boot-persistent.....	336
11.1.1 Additions to the Setup menu.....	337
11.2 Comment box for CRON jobs.....	338
11.2.1 Configuring the scheduler.....	338
11.2.2 Additions to the Setup menu.....	339
11.3 LANCAPI disabled by default.....	339
11.3.1 Additions to the Setup menu.....	340

11.4 DHCP snooping and DHCP option 82.....340

 11.4.1 Additions to the Setup menu.....342

11.5 Enabling LLDP with LANconfig.....345

11.6 Wildcard certificates in the LANCOM Content Filter.....346

 11.6.1 Additions to the Setup menu.....346

1 Addendum to LCOS version 9.00

This document describes the changes and enhancements in LCOS version 9.00 since the previous version.

2 LCMS

2.1 Enhancements to LANconfig

2.1.1 Automatic authentication for read-only access to LANmonitor

As of 9.00, LANconfig offers a new user-friendly feature: With a device configuration opened in LANconfig, LANmonitor can be started without you having to enter access credentials again.

Login information

Enter the access credentials for the external programs in this field. Click **New** to select one or more application(s) and enter the corresponding access credentials. Depending on your selection, the dialog window requests different access credentials. If you invoke the program from LANconfig, you have the option of authenticating yourself with the username and password of your administrator login.

In the case of LANmonitor, you have the option to specify an individual SNMP community for read-only access. By default, when LANconfig opens a device configuration it checks whether and to what extent you have stored access credentials for external programs. If you do not have access credentials or if these credentials have been configured in the form of an SNMP community only, then invoking LANmonitor prompts LANconfig to take the SNMP community from the loaded device configuration. If you edit a configuration in LANconfig and you have set an SNMP community here, LANconfig automatically saves the SNMP community for the corresponding device. This convenient behavior reduces the scope of authentication for LANmonitor, so no separate configuration of the read-only access is required.

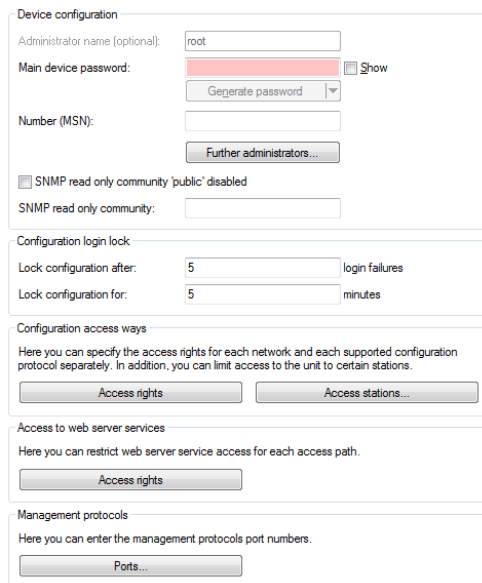


LANconfig evaluates the setup parameter *2.9.15 Read-Only-Community* for the convenient behavior described above. Any additional read-only SNMP communities configured in the device are ignored.

For more information about the SNMP access through single or multiple SNMP communities, see the Reference Manual.

2.1.2 Display of administrator user name

In order to show which username is linked to the main password, as of version 9.00 LANconfig shows **root** as the administrator user name in the device configurations and in the Wizards.



Device configuration

Administrator name (optional):

Main device password: ☐ Show

Number (MSN):

☐ SNMP read only community 'public' disabled

SNMP read only community:

Configuration login lock

Lock configuration after: login failures

Lock configuration for: minutes

Configuration access ways

Here you can specify the access rights for each network and each supported configuration protocol separately. In addition, you can limit access to the unit to certain stations.

Access to web server services

Here you can restrict web server service access for each access path.

Management protocols

Here you can enter the management protocols port numbers.

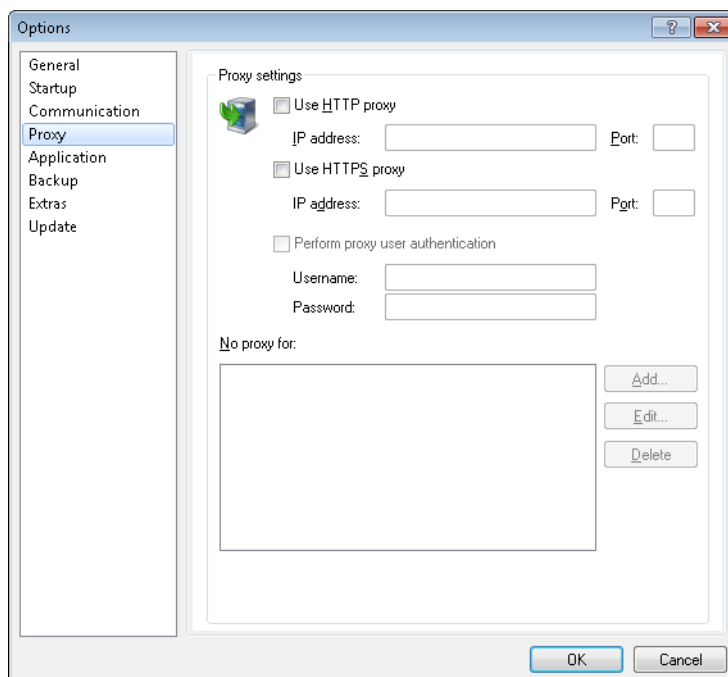
2.1.3 Authenticating against a proxy server

As of version 9.00 it is possible for LANconfig to authenticate against an external proxy.

Proxy

If you wish to use a proxy server for access to your device, you can configure this here. Activate the required protocol and enter the address and port for accessing the proxy server.

Depending on the protocol, it may be possible to specify a list of networks or individual hosts for which the proxy settings do not apply.



Options

General
Startup
Communication
Proxy
Application
Backup
Extras
Update

Proxy settings

☐ Use HTTP proxy
IP address: Port:

☐ Use HTTPS proxy
IP address: Port:

☐ Perform proxy user authentication
Username:
Password:

No proxy for:

Use HTTP proxy

Enables the use of an HTTP proxy.

- **Address:** Enter the IP address of the the HTTP proxy server.
- **Port:** Enter the port used by the HTTP proxy server.

Use HTTPS proxy

Enables the use of an HTTPS proxy.

- **Address:** Enter the IP address of the the HTTPS proxy server.
- **Port:** Enter the port used by the HTTPS proxy server.

Perform proxy user authentication

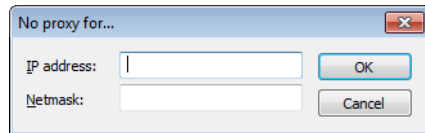
If the proxy server requires authentication, enter the user name and password here.



This option is available only if the proxy setting is enabled.

No proxy for

Enter the IP addresses and the corresponding netmask to which the proxy settings do not apply.



This option is available only if the proxy setting is enabled.

2.2 Enhancements to LANmonitor

2.2.1 Internal IPv6 support

As of version 9.00, LANmonitor can handle IPv6 addresses internally and can thus communicate with devices via IPv6.

2.2.2 Displaying static WAN IPs in the Status tree

As of version 9.00, LANmonitor can optionally display a static WAN IP in the Status tree.

Additions to the Status menu**IPv4**

This table contains the list of static IPv4 stations on the WAN.

SNMP ID:

1.4.13.1

Telnet path:

Status > WAN > IP-Addresses

Remote site

Name of the remote device.

SNMP ID:

1.4.13.1.1

Telnet path:

Status > WAN > IP-Addresses > IPv4

Type

Type of the assigned IPv4 address

SNMP ID:

1.4.13.1.2

Telnet path:

Status > WAN > IP-Addresses > IPv4

Possible values:

static
DHCP
PPP
Autoconfig

IP address

Assigned IPv4 address.

SNMP ID:

1.4.13.1.3

Telnet path:

Status > WAN > IP-Addresses > IPv4

IP netmask

Assigned IPv4 netmask.

SNMP ID:

1.4.13.1.4

Telnet path:

Status > WAN > IP-Addresses > IPv4

Gateway

Assigned gateway.

SNMP ID:

1.4.13.1.5

Telnet path:

Status > WAN > IP-Addresses > IPv4

DNS default

Primary assigned DNS server.

SNMP ID:

1.4.13.1.6

Telnet path:

Status > WAN > IP-Addresses > IPv4

DNS backup

Alternative assigned DNS server.

SNMP ID:

1.4.13.1.7

Telnet path:

Status > WAN > IP-Addresses > IPv4

NBNS default

Primary assigned NBNS server.

SNMP ID:

1.4.13.1.8

Telnet path:

Status > WAN > IP-Addresses > IPv4

NBNS backup

Alternative assigned NBNS server.

SNMP ID:

1.4.13.1.9

Telnet path:**Status > WAN > IP-Addresses > IPv4****Domain**

The assigned domain.

SNMP ID:

1.4.13.1.10

Telnet path:**Status > WAN > IP-Addresses > IPv4****IPv6**

This table contains the list of static IPv6 stations on the WAN.

SNMP ID:

1.4.13.2

Telnet path:**Status > WAN > Addresses****Remote site**

Name of the remote device.

SNMP ID:

1.4.13.2.1

Telnet path:**Status > WAN > IP-Addresses > IPv6****Type**

Type of the assigned IPv6 address

SNMP ID:

1.4.13.2.2

Telnet path:

Status > WAN > IP-Addresses > IPv6

Possible values:

**Unknown
static
DHCP
Autoconfig
tunnel**

IP address

Assigned IPv6 address.

SNMP ID:

1.4.13.2.3

Telnet path:

Status > WAN > IP-Addresses > IPv6

Prefix length

Assigned prefix length.

SNMP ID:

1.4.13.2.4

Telnet path:

Status > WAN > IP-Addresses > IPv6

Gateway

Assigned gateway.

SNMP ID:

1.4.13.2.5

Telnet path:

Status > WAN > IP-Addresses > IPv6

DNS default

Primary assigned DNS server.

SNMP ID:

1.4.13.2.6

Telnet path:**Status > WAN > IP-Addresses > IPv6****DNS backup**

Alternative assigned DNS server.

SNMP ID:

1.4.13.2.7

Telnet path:**Status > WAN > IP-Addresses > IPv6****Domain**

The assigned domain.

SNMP ID:

1.4.13.2.10

Telnet path:**Status > WAN > IP-Addresses > IPv6**

3 Configuration

3.1 Output additional ports in SYSINFO at the console

As of version 9.00, the `sysinfo` command also outputs the numbers of the following ports:

- HTTP
- HTTPS
- TELNET
- TELNET-SSL
- SSH
- SNMP
- TFTP

3.2 Specifying a custom SNMP port

As of LCOS 9.00 you have the option of changing the default port for the SNMP service from port 161.

Enter the respective port in LANmonitor, for example, when adding a new device. You also have the option of configuring new devices by entering IP addresses and the SNMP port when executing the program. To do this, start the LANmonitor with the syntax `lanmon /add: [<IPv6-Address>]:<Port>`, for example, `lanmon /add:[fe80::2a0:57ff:fe1b:3302]:161`.

3.2.1 Additions to the Setup menu

Port

Enter the port of the computer where an SNMP manager is installed.

SNMP ID:

2.9.2.5

Telnet path:

Setup > SNMP > IP-Traps

Possible values:

Max. 5 characters from 0123456789

0 ... 65535

Default:

empty

Port

Using this parameter, you specify the port which external programs (such as LANmonitor) use to access the SNMP service.

SNMP ID:

2.9.21

Telnet path:

Setup > SNMP

Possible values:

0 ... 65535

Default:

161

3.3 Password protection for WLAN keys

As of LCOS 9.00 the system no longer displays WPA and WEP group keys in plain text on the console, but masked (*****). As a result, it is no longer possible to read these keys via SNMP, for example.

3.4 Sorted display of a menu on the console

As of LCOS 9.00 you have the option of sorting the output of the menu items by using the argument `-s`.

Command	Description
<code>dir list ls llong [-a] [-r] [-s]</code> <code>[<Path>] [<Filter>]</code>	<p>Displays the current directory content. Possible arguments are:</p> <ul style="list-style-type: none"> ■ <code>-a</code>: In addition to the content of the query, this also lists the SNMP IDs. The output begins with the SNMP ID of the device followed by the SNMP ID of the current menu. The SNMP IDs of the subordinate items can be read from the individual entries. ■ <code>-r</code>: Also lists all subdirectories as well as the tables they contain. ■ <code>-s</code>: Sorts the displayed menu items in ascending alphabetical order.

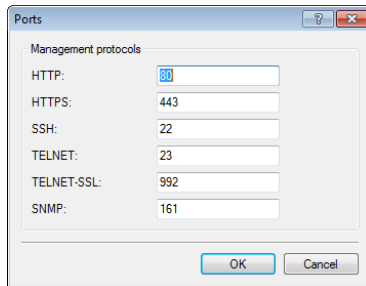
Alternatively, you have the option of setting the default to sorted output using the corresponding setup parameter **Setup > Config > Sort-menu**.

3.5 Customize the management ports for device access

LANconfig features the option to change the port numbers for the management protocols.

1. Start LANconfig and open the configuration dialog for the device.
2. Switch to the dialog **Management > Admin** and click **Ports**.

3. Enter the port numbers for the required management protocols.



The 'Ports' dialog box contains a section titled 'Management protocols' with the following fields:

Protocol	Port
HTTP:	80
HTTPS:	443
SSH:	22
TELNET:	23
TELNET-SSL:	992
SNMP:	161

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

4. Close all open dialog windows by clicking on **OK**.

LANconfig writes the configuration back to the device.

3.5.1 Additions to the Setup menu

Sort-menu

Using this parameter, you specify whether the device displays menu items in ascending alphabetical order on the console by default. The setting corresponds to the option switch `-s` when listing menu or table contents.

SNMP ID:

2.11.73

Telnet path:

Setup > Config

Possible values:

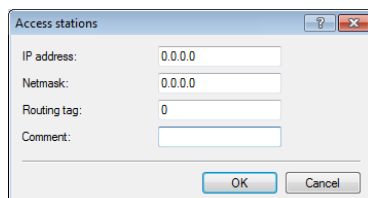
No
Yes

Default:

No

3.6 Comment box for access stations

As of LCOS9.00 you can add comments to the filter entries in the table of access stations.



The 'Access stations' dialog box contains the following fields:

Field	Value
IP address:	0.0.0.0
Netmask:	0.0.0.0
Routing tag:	0
Comment:	

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

3.6.1 Additions to the Setup menu

Comment

This parameter allows you to enter a comment on the entry.

SNMP ID:

2.7.6.4

Telnet path:

Setup > TCP-IP > Access-list

Possible values:

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

Default:

empty

3.7 Elliptic curve cryptography (ECC)

As of LCOS9.00 you can generate ECDSA keys on a device in addition to the RSA and DSA keys.

SSH key generation with LCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the console:

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

-?, -h

Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa)

This parameter specifies what type of key is generated. SSH supports the following types of keys:

- RSA keys are most widely used and have a length between 512 and 16384 bits. If possible you should work with keys of 1024 to 2048 bits in length.
- DSA keys follow the Digital Signature Standard (DSS) set down by the National Institute of Standards and Technology (NIST) and are typically used in environments which are required to comply with the Federal Information Processing Standard (FIPS). DSA and DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.
- ECDSA keys are a variant of DSA keys, whereby the device uses elliptic curves for key generation (elliptic curve cryptography, ECC). ECC is an alternative to the conventional signature and key exchange techniques such as RSA and Diffie-Hellman. The main advantage of elliptic curves is that their mathematical properties offer the same key strength as RSA or Diffie-Hellman but with a significantly shorter key length. This provides for better hardware performance. ECC and its integration in SSL and TLS are described in RFCs 5656 and 4492.

If no type is specified, the command generates an RSA key by default.

-b <bits>

This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.

-f <OutputFile>

These parameters specify the mounting point of the generated key file in the device file system. The choice of mounting point depends on what type key you are generating. The choices available to you are:

- **ssh_rsakey** for RSA keys
- **ssh_dsakey** for DSA keys
- **ssh_ecdsakey** for ECDSA keys

-q

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

3.7.1 Additions to the Setup menu

SSL

The parameters for HTTPS connections are specified here.

SNMP ID:

2.21.40

Telnet path:

Setup > HTTP

Port

Port for the HTTPS server connection

SNMP ID:

2.21.40.10

Telnet path:

Setup > HTTP > SSL

Possible values:

0 ... 65535

Default:

443

Use-User-Provided-Certificate

Here you select whether you want to use a user-provided certificate.

SNMP ID:

2.21.40.11

Telnet path:**Setup > HTTP > SSL****Possible values:****Yes****No****Default:****Yes****Versions**

This bitmask specifies which versions of the protocol are allowed.

SNMP ID:**2.21.40.3****Telnet path:****Setup > HTTP > SSL****Possible values:****SSLv3****TLSv1****TLSv1.1****TLSv1.2****Default:****SSLv3****TLSv1****Key-exchange algorithms**

This bitmask specifies which key-exchange methods are available.

SNMP ID:**2.21.40.4****Telnet path:****Setup > HTTP > SSL**

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.21.40.5

Telnet path:

Setup > HTTP > SSL

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

SNMP ID:

2.21.40.6

Telnet path:

Setup > HTTP > SSL

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

Key-exchange algorithms

The MAC key exchange algorithms are used to negotiate the key algorithm. Select one or more of the available algorithms.

SNMP ID:

2.11.28.3

Telnet path:

Setup > Config > SSH

Possible values:

diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2
curve25519-sha256

Default:

diffie-hellman-group1-sha1

diffie-hellman-group14-sha1

diffie-hellman-group-exchange-sha1

diffie-hellman-group-exchange-sha256

Hostkey algorithms

The host key algorithms are used to authenticate hosts. Select one or more of the available algorithms.

SNMP ID:

2.11.28.4

Telnet path:

Setup > Config > SSH

Possible values:

ssh-rsa
ssh-dss
ecdsa-sha2
ssh-ed25519

Default:

ssh-rsa
ssh-dss

Elliptic curves

This is where you select the (NIST) curves used by the device for the elliptic curve cryptography (ECC).



All of the NIST curves given here are suitable for the ECDH key agreement, whereas host keys are based on the curves `nistp256` and `nistp384`.

SNMP ID:

2.11.28.9

Telnet path:

Setup > Config > SSH

Possible values:

nistp256
nistp384
nistp521

Default:

nistp256

nistp384

nistp521

Telnet-SSL

The parameters for Telnet-SSL connections are specified here.

SNMP ID:

2.11.29

Telnet path:

Setup > Config

PORT

This port is used for encrypted configuration connections via telnet.

SNMP ID:

2.11.29.10

Telnet path:

Setup > Config > Telnet-SSL

Possible values:

0 ... 65535

Default:

992

Versions

This bitmask specifies which versions of the protocol are allowed.

SNMP ID:

2.11.29.2

Telnet path:**Setup > Config > Telnet-SSL****Possible values:****SSLv3**
TLSv1
TLSv1.1
TLSv1.2**Default:****SSLv3**

TLSv1**Key-exchange algorithms**

This bitmask specifies which key-exchange methods are available.

SNMP ID:**2.11.29.3****Telnet path:****Setup > Config > Telnet-SSL****Possible values:****RSA**
DHE
ECDHE**Default:****RSA**

DHE

ECDHE**Crypto-Algorithms**

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:**2.11.29.4****Telnet path:****Setup > Config > Telnet-SSL**

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

SNMP ID:

2.11.29.5

Telnet path:

Setup > Config > Telnet-SSL

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

SHA2-384

EAP-TLS

The parameters for EAP-TLS connections are specified here.

SNMP ID:

2.25.10.10.19

Telnet path:

Setup > RADIUS > Server > EAP

Check username

TLS authenticates the client via certificate only. If this option is activated, the RADIUS server additionally checks if the username in the certificate is contained in the RADIUS user table.

SNMP ID:

2.25.10.10.19.10

Telnet path:

Setup > RADIUS > Server > EAP > EAP-TLS

Possible values:

Yes

No

Default:

No

Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

SNMP ID:

2.25.10.10.19.3

Telnet path:

Setup > RADIUS > Server > EAP > EAP-TLS

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.25.10.10.19.4

Telnet path:

Setup > RADIUS > Server > EAP > EAP-TLS

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

SNMP ID:

2.25.10.10.19.5

Telnet path:

Setup > RADIUS > Server > EAP > EAP-TLS

Possible values:

**MD5
SHA1
SHA2-256
SHA2-384**

Default:

MD5

SHA1

SHA2-256

SHA2-384

RADSEC

The parameters for RADSEC connections are specified here.

SNMP ID:

2.25.20

Telnet path:

Setup > RADIUS

Versions

This bitmask specifies which versions of the protocol are allowed.

SNMP ID:

2.25.20.1

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default:

SSLv3

TLSv1

Key-exchange algorithms

This bitmask specifies which key-exchange methods are available.

SNMP ID:

2.25.20.2

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

RSA
DHE
ECDHE

Default:

RSA

DHE

ECDHE

Crypto-Algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.25.20.3

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash algorithms

This bit mask specifies which hash algorithms are allowed and implies what HMAC algorithms used to protect of the integrity of the messages.

SNMP ID:

2.25.20.4

Telnet path:

Setup > RADIUS > RADSEC

Possible values:

MD5
SHA1
SHA2-256
SHA2-384

Default:

MD5

SHA1

SHA2-256

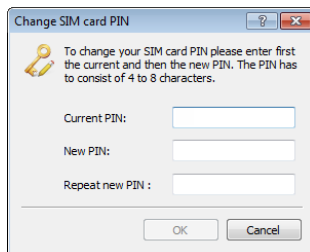
SHA2-384

3.8 Changing the SIM card PIN

For devices with a cellular modem, LANconfig gives you the option to change the PIN of the SIM card. You make the change simply by entering the old PIN and then the new PIN. In the interests of security, LANconfig requires an additional confirmation of the new PIN. Alternatively you can make the change from the command line by executing the action **PIN-change**.

The following steps describe the procedure in LANconfig.

1. In the LANconfig device overview, select the device requiring the PIN change.
2. From the menu bar, choose **Device > Change SIM card PIN**. A new dialog box opens.



3. Enter the old PIN and then your new PIN. Confirm the new PIN by entering it again.
4. Click **OK** to accept the change.

3.8.1 Additions to the Status menu

PIN change

Use this action to change the PIN of the SIM card. The syntax when entering the arguments is:

```
<oldPIN> <newPIN> <newPIN>
```



The action can be performed only after the modem has been successfully initialized. This is particularly important when scripts are being used to implement a configuration.

SNMP ID:

1.49.42

Telnet path:

Status > Modem-Cellular-Network

Possible arguments:

<oldPIN>

Old PIN

<newPIN>

New PIN

<newPIN>

Confirmation of the new PIN

3.8.2 Additions to the Setup menu

PIN change

This action changes the PIN of the SIM card in your device. Syntax:

```
do pin-change <old_PIN><new_PIN> <new_PIN>
```

SNMP ID:

2.23.41.12

Telnet path:

Setup > Interfaces > Mobile

Possible values:

4 characters from [0-9]

4 IPv6

4.1 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, abbreviated DS-Lite, is used so that Internet providers can supply their customers with access to IPv4 servers over an IPv6 connection. That is necessary, for example, if an Internet provider is forced to supply its customer with an IPv6 address due to the limited availability of IPv4 addresses. In contrast to the other three IPv6 tunnel methods "6in4", "6rd" and "6to4", DS-Lite is also used to transmit IPv4 packets on an IPv6 connection (IPv4 via IPv6 tunnel).

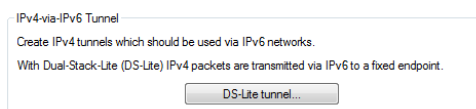
For this, the router packages the IPv4 packets in an IPv4-in-IPv6 tunnel and transmits them unmasked to the provider, who then performs a NAT with one of their own remaining IPv4 addresses.

To define a DS-Lite tunnel, all the router needs is the IPv6 address of the tunnel endpoint and the routing tag with which it can reach this address.

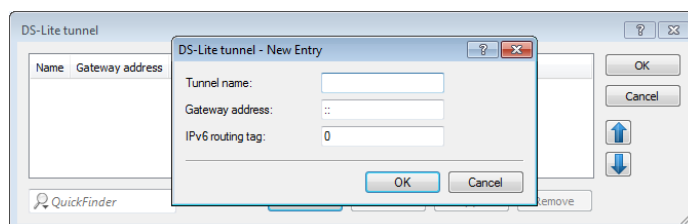
By default, the router uses the IPv4 address of the corresponding internal network, e.g., from "INTRANET". If you would like to define a different IP address instead (e.g., 192.0.0.2), it must be entered in the IP parameter list along with the remote site name of the DS-Lite tunnel.

Entering an IPv4 DNS server is not recommended for a DS-Lite tunnel, since its entries would unnecessarily fill the NAT table of the Internet provider.

You set up a DS-Lite tunnel in LANconfig via **IPv4 > Tunnel** by clicking on **DS-Lite tunnel**.



Then click on the **Add** button and enter the designation of the tunnel, the IPv6 address of the gateway, and the routing tag.



Name of the tunnel

This entry determines the name of the IPv4-over-IPv6 tunnel.

Gateway address

This entry defines the address of the DS-Lite gateway, the so-called Address Family Transition Router (AFTR).

The following values are possible:

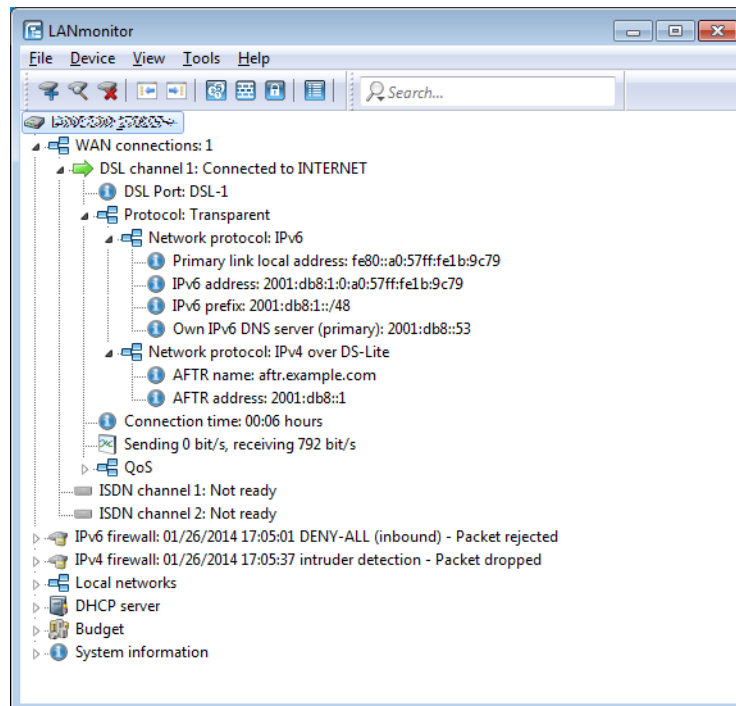
- One IPv6 address (e.g. 2001:db8::1)
- An FQDN (Fully Qualified Domain Name) that can be resolved by DNS, e.g., aftr.example.com
- The IPv6 unspecified address "::" determines that the device should retrieve the address of the AFTRs via DHCPv6 (factory setting).
- An empty field behaves the same as the entry "::".

IPv6 routing tag

The routing tag uniquely specifies the route to the DS-Lite gateway.

- i** With DS-Lite, since the NAT is performed by the provider, the function of many applications depends on the settings of the NAT provider (e.g., SIP, H.323, IRC or IPSec). PPTP does not work via DS-Lite at all. If the provider does not operate port forwarding, the IPv4 server services do not function.

The status table and the number of current DS-Lite connections can be shown using LANmonitor:



4.1.1 Additions to the Status menu

DS-Lite

The statistics of the DS-Lite tunnel are located in this directory.

SNMP ID:

1.81

Telnet path:

State

Rx-Packets

This entry shows the number of data packets received by all DS-Lite interfaces.

SNMP ID:

1.81.1

Telnet path:**Status > DS-Lite****Tx-Packets**

This entry shows the number of data packets sent by all DS-Lite interfaces.

SNMP ID:

1.81.2

Telnet path:**Status > DS-Lite****Queue error**

This entry shows the number data packets sent by all DS-Lite interfaces.

SNMP ID:

1.81.3

Telnet path:**Status > DS-Lite****Connections**

This table shows an overview of the active DS-Lite connections.

Once the device has established a DS-Lite connection, it appears in this table. After a connection terminates without errors, the entry in the table is deleted automatically. If there is an error, the entry remains until the connection is reestablished or you manually delete it.

Every status change of a DS-Lite connection sends an SNMP trap (ID 83) with the content of the corresponding line in the status table

SNMP ID:

1.81.4

Telnet path:**Status > DS-Lite****Remote site**

This entry shows the name of the DS-Lite tunnel.

SNMP ID:

1.81.4.1

Telnet path:**Status > DS-Lite > Connections****State**

This entry shows the state of the DS-Lite tunnel.

SNMP ID:

1.81.4.2

Telnet path:**Status > DS-Lite > Connections****Last error**

This entry shows the last error on the connection.

SNMP ID:

1.81.4.3

Telnet path:**Status > DS-Lite > Connections****IPv4 address**

This entry shows the IPv4 address of the device when it sends data packets.

SNMP ID:

1.81.4.4

Telnet path:**Status > DS-Lite > Connections****phys. conn.**

This entry shows the name of the IPv6 interface running the DS-Lite connection.

SNMP ID:

1.81.4.5

Telnet path:**Status > DS-Lite > Connections****AFTR-Name**

This entry shows the DNS name of the tunnel endpoint (Address Family Transition Router, AFTR).

SNMP ID:

1.81.4.6

Telnet path:**Status > DS-Lite > Connections****AFTR-IPv6-Address**

This entry shows the IPv6 address of the DS-Lite tunnel endpoint.

SNMP ID:

1.81.4.7

Telnet path:**Status > DS-Lite > Connections****Conn. time:**

This entry shows how long the connection already exists. The query via SNMP provides the connection age in seconds; TELNET provides the system time when the connection was established.

SNMP ID:

1.81.4.8

Telnet path:**Status > DS-Lite > Connections****Tunnel**

This entry shows the number of active DS-Lite connections.

SNMP ID:

1.81.5

Telnet path:**Status > DS-Lite**

Tunnel

This action deletes all values of the DS-Lite statistics.

SNMP ID:

1.81.6

Telnet path:

Status > DS-Lite

4.1.2 Additions to the Setup menu

DS-Lite-Tunnel

Dual-Stack Lite, abbreviated DS-Lite, is used so that Internet providers can supply their customers with access to IPv4 servers over an IPv6 connection. That is necessary, for example, if an Internet provider is forced to supply its customer with an IPv6 address due to the limited availability of IPv4 addresses. In contrast to the other three IPv6 tunnel methods "6in4", "6rd" and "6to4", DS-Lite is also used to transmit IPv4 packets on an IPv6 connection (IPv4 via IPv6 tunnel).

For this, the router packages the IPv4 packets in an IPv4-in-IPv6 tunnel and transmits them unmasked to the provider, who then performs NAT with one of their own remaining IPv4 addresses.

To define a DS-Lite tunnel, the router only needs the IPv6 address of the tunnel endpoint and the routing tag with which it can reach this address.

SNMP ID:

2.2.40

Telnet path:

Setup > WAN

Name

Enter the name for the tunnel.

SNMP ID:

2.2.40.1

Telnet path:

Setup > WAN > DS-Lite-Tunnel

Possible values:

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

Default:

empty

Gateway address

This entry defines the address of the DS-Lite gateway, the so-called Address Family Transition Router (AFTR). Enter a valid value from the following selection:

- An IPv6 address, e. g., 2001:db8::1
- An FQDN (fully qualified domain name) which can be resolved by DNS, e. g., aftr.example.com
- The IPv6 unspecified address "::" means that the device should obtain the address of the AFTR via DHCPv6 (factory setting).
- An empty field behaves the same as the entry "::".

SNMP ID:

2.2.40.2

Telnet path:

Setup > WAN > DS-Lite-Tunnel

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Default:

empty

Rtg tag

Enter the routing tag where the router reaches the gateway.

SNMP ID:

2.2.40.3

Telnet path:

Setup > WAN > DS-Lite-Tunnel

Possible values:

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

Default:

empty

4.2 IPv6 support for RAS services

As of LCOS 9.00, RAS remote stations are able login via IPv6. The configuration is done in LANconfig under **IPv6 > General** and the setup of prefix pools under **IPv6 > Router advertisement**.

4.2.1 RAS interfaces

There are basically two ways to manage the configuration of RAS remote stations:

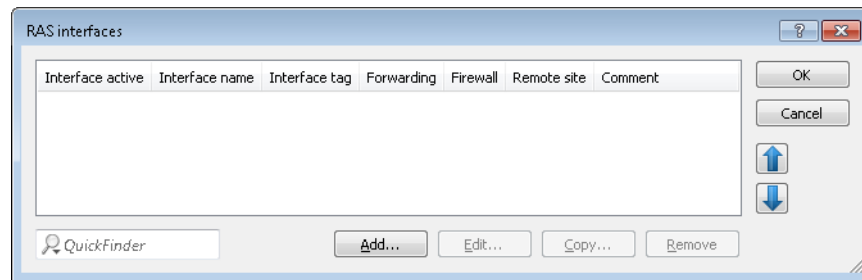
The user data or the configurations are locally stored on the device.

The advantage of this alternative is that a RADIUS server is not necessary, which reduces the management and cost of the network infrastructure.

The user data or the configurations are stored on an external RADIUS server.

The advantage of this alternative is the centralized user management for extensive distributed network scenarios.

For RAS access via IPv6, you must also set up the corresponding **RAS interface**.



Entries in the **RAS interfaces** table have the following meaning:

- **Interface active:** Enable or disable this interface here.
- **Interface name:** Here you define the name of the RAS interface that the IPv6 remote sites use for access.
- **Interface tag:** The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- **Forwarding:** Enables or disables the forwarding of data packets to other interfaces.
- **Firewall:** If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, navigate to **Firewall/QoS > General** and check the option **IPv6 firewall/QoS enabled**.

If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

- **Remote site:** Specify the remote site or a list of remote sites for RAS dial-in users.

The following values are possible:

- A single remote station from the tables under **Setup > WAN > PPTP-Peers**, **Setup > WAN > L2TP-Peers** or **Setup > PPPoE-Server > Name-list**.
- The wildcard "*" makes the interface valid for all PPTP, PPPoE and L2TP peers.
- The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL".

Using the wildcards you can create several peers for IPv6 RAS services based on so-called template interfaces. These template interfaces can be used as normal interfaces for IPv6 services such as DHCPv6 server or router advertisements. For example, using these, a group of RAS interfaces can be provided from an IPv6 prefix pool.

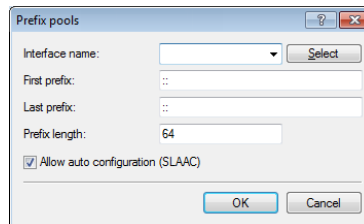
- **Comment:** Enter a descriptive comment for this entry.

Information on RADIUS attributes for IPv6 RAS services can be found under [RADIUS attribute extensions for IPv6 RAS services](#) on page 50.

i If RAS clients are to be delegated to an IPv6 DNS server or are to receive their prefixes by prefix delegation, you must create a corresponding entry in the table **DHCPv6 networks** under **IPv6 > DHCPv6**.

i If you wish to authenticate a user by PPP list, you navigate to **Communication > Protocols > PPP list** and enable the option **Activate IPv6 routing** for that user.

4.2.2 Prefix pools



This table contains the pools of prefixes which RAS users receive when they connect remotely via IPv6. The following settings are possible:

Interface name

Specifies the name of the RAS interface that is valid for this prefix pool.

First prefix

Specifies the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., "2001:db8::". Each user is assigned precisely one /64 prefix from the pool.

Last prefix

Specifies the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. '2001:db9:FFFF::'. Each user is assigned precisely one /64 prefix from the pool.

Prefix length

Specifies the length of the prefix that the remote user is assigned by the router advertisement here. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

SLAAC

Specifies whether the prefix can be used for a stateless address auto-configuration (SLAAC).

4.2.3 Additions to the Setup menu

RAS-Interface

In this directory, you specify the settings for RAS access via IPv6.

SNMP ID:

2.70.14

Telnet path:

Setup > IPv6

Interface name

Here you define the name of the RAS interface that the IPv6 remote sites use for access.

SNMP ID:

2.70.14.1

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:**Max. 16 characters from `[A-Z][0-9]{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`**Default:***empty***Rtg tag**

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will contain this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

SNMP ID:

2.70.14.2

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:**Max. 5 characters from `0123456789`**Default:**

0

Interface status

Enable or disable this interface here.

SNMP ID:

2.70.14.3

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:****Active**
Idle**Default:**

Active

Forwarding

Enables or disables the forwarding of data packets to other interfaces.

SNMP ID:

2.70.14.4

Telnet path:

Setup > IPv6 > RAS-Interface

Possible values:

Yes

No

Default:

Yes

Firewall

If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, change the setting under **IPv6 > Firewall > Enabled** to **yes**.

If you disable the global firewall, the firewall for an individual interface is also disabled. This applies even if you have enabled this option.

SNMP ID:

2.70.14.5

Telnet path:

Setup > IPv6 > RAS-Interface

Possible values:

Yes

No

Default:

Yes

DaD attempts

Before the device can use an IPv6 address on an interface, it uses 'Duplicate Address Detection (DAD)' to check to see whether the IPv6 address already exists on the local network. In this way, the device avoids address conflicts in the network.

This option is the number of attempts with which the device searches for duplicate IPv6 addresses in the network.

SNMP ID:

2.70.14.6

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:**

1 characters from 0123456789

Default:

0

Remote site

Set a remote station or a list of remote stations for RAS dial-in users.

The following values are possible:

- An individual remote site from the tables under **Setup > WAN > PPTP-Peers** or **Setup > PPPoE-Server > Name-List**.
- The "*" wildcard makes this interface valid for all PPTP and PPPoE peers.
- The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL", selects interfaces with names that match.

By using wildcards you can implement template interfaces, which apply to peers which are named accordingly. In this manner, the name of the IPv6 RAS interface can be used many places in the IPv6 configuration.

SNMP ID:

2.70.14.7

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:**

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

Default:*empty***Comment**

Enter a descriptive comment for this entry.

SNMP ID:

2.70.14.8

Telnet path:**Setup > IPv6 > RAS-Interface****Possible values:**

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

Default:*empty***Prefix pools**

In this directory you can define pools of prefixes for remote users and/or the corresponding RAS interfaces (PPTP, PPPoE). Define the prefixes for Ethernet interfaces under **Setup > IPv6 > Router > Router-Advertisements > Prefix-Options** or in LANconfig under **IPv6 > Router advertisement > Prefix list**.

SNMP ID:

2.70.2.6

Telnet path:**Setup > IPv6 > Router-Advertisement****Interface name**

Specify the name of the RAS interface applicable for this prefix pool.

SNMP ID:

2.70.2.6.1

Telnet path:**Setup > IPv6 > Router-Advertisement > Prefix-Pools****Possible values:**

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

Default:*empty***Start-Prefix-Pool**

Here you specify the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., "2001:db8::". Each user is assigned precisely one /64 prefix from the pool.

SNMP ID:

2.70.2.6.2

Telnet path:**Setup > IPv6 > Router-Advertisement > Prefix-Pools****Possible values:**

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

Default:*empty***End-Prefix-Pool**

Here you specify the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. '2001:db9:FFFF::'. Each user is assigned precisely one /64 prefix from the pool.

SNMP ID:

2.70.2.6.3

Telnet path:**Setup > IPv6 > Router-Advertisement > Prefix-Pools****Possible values:**Max. 43 characters from `[A-F][a-f][0-9]:./`**Default:**

::

Prefix length

Here you specify the length of the prefix assigned to the remote user by the router advertisement. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

SNMP ID:

2.70.2.6.4

Telnet path:**Setup > IPv6 > Router-Advertisement > Prefix-Pools****Possible values:**Max. 3 characters from `0123456789`**Default:**

64

Adv.-OnLink

Indicates whether the prefix is "on link".

SNMP ID:

2.70.2.6.5

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Pools

Possible values:

Yes

No

Default:

Yes

Adv.-Autonomous

Specifies whether the client can use the prefix for a stateless address auto-configuration (SLAAC).

SNMP ID:

2.70.2.6.6

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Pools

Possible values:

Yes

No

Default:

Yes

Adv.-Pref.-Lifetime

Specifies the time in milliseconds for which an IPv6 address is "Preferred". The client also uses this lifetime for its generated IPv6 address. If the lifetime of the prefix has expired, the client no longer uses the corresponding IPv6 address. Is the "preferred lifetime" of an address expires, it will be marked as "deprecated". This address is then used only by already active connections until those connections end. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.6.7

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Pools

Possible values:

Max. 10 characters from 0123456789

Default:

604800

Adv.-Valid-Lifetime

Defines the time in seconds, after which the validity of an IPv6 address expires. Expired addresses are no longer available for new connections.

SNMP ID:

2.70.2.6.8

Telnet path:

Setup > IPv6 > Router-Advertisement > Prefix-Pools

Possible values:

Max. 10 characters from 0123456789

Default:

2592000

4.3 RADIUS attribute extensions for IPv6 RAS services

The RADIUS client can request RADIUS attributes, such as the "Framed-IP-Address", from an external RADIUS server and provide these, for example, to a PPPoE server in order to authenticate them at PPPoE, PPTP or L2TP servers. LANCOM devices accept the following attributes in access-accept messages:

96

Framed-Interface-ID

This attribute conveys the IPv6 interface identifier that should be configured for the user in the IPv6CP.

97

Framed-IPv6-Prefix

Prefix, which is sent to the user via router advertisements.

99

Framed-IPv6-Route

This attribute conveys the route to be used for this user. The device supplements the IPv6 routing table with this route and the next hop to this user.

100

Framed-IPv6-Pool

This indicates the IPv6 pool from which a prefix is to be taken for the user. The IPv6 pool is referenced by its name and must be present under **IPv6 > Router advertisement > Prefix pools**.

123

Delegated-IPv6-Prefix

Prefix, which is sent to the user via DHCPv6 prefix delegation.

The newly available RADIUS attributes are implemented according to RFCs 3162 and 4818. An example for a PPP user test with IPv6 in the FreeRADIUS is as follows:

```
test Cleartext-Password := "1234"
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IPv6-Prefix = "fec0:1:2400:1::/64",
```

```
Delegated-IPv6-Prefix = "fec0:1:2400:1100::/56",
Framed-IP-Address = 172.16.3.33,
```

The user "test" in a dual-stack PPP session receives the IPv4 address 172.16.3.33, the prefix fec0:1:2400:1::/64 via router advertisement, and the prefix fec0:1:2400:1100::/56 via DHCPv6 prefix delegation.

4.4 Loopback addresses for IPv6

As of LCOS 9.00, you can use IPv6 loopback addresses as the sender address for ping commands at the command line.

Parameters	Meaning
-6	Sets an IPv6 loopback interface as the sender address.
<Loopback-Interface>	

4.4.1 Loopback addresses

IPv6 loopback addresses can be specified in the **Loopback addresses** table. The device sees each of these addresses as its own address, which is also available if a physical interface is disabled, for example.

Entries in the **Loopback addresses** table have the following meaning:

- **Name:** Enter a unique name for this loopback address.
- **IPv6 address:** Enter a valid IPv6 address here.
- **Routing tag:** Here you specify the routing tag of the network that the loopback address belongs to. Only packets with this routing tag will reach this address.
- **Comment:** You have the option to enter a comment here.

4.4.2 Additions to the Setup menu

Loopback

You can set IPv6 loopback addresses here. The device sees each of these addresses as its own address, which is also available if a physical interface is disabled, for example.

SNMP ID:

2.70.4.3

Telnet path:

Setup > IPv6 > Network

Name

Enter a unique name for this loopback address.

SNMP ID:

2.70.4.3.1

Telnet path:**Setup > IPv6 > Network > Loopback****Possible values:**Max. 16 characters from `[A-Z][0-9]@{ | }~!$%&'()+-,/:;=>?[\]^_.`**Default:***empty***IPv6-Loopback-Addr.**

Enter a valid IPv6 address here.

SNMP ID:

2.70.4.3.2

Telnet path:**Setup > IPv6 > Network > Loopback****Possible values:**Max. 39 characters from `0123456789ABCDEFabcdef:./`**Default:***empty***Rtg tag**

Here you specify the routing tag of the network that the loopback address belongs to. Only packets with this routing tag will reach this address.

SNMP ID:

2.70.4.3.3

Telnet path:**Setup > IPv6 > Network > Loopback****Possible values:**Max. 5 characters from `0123456789`**Default:**

0

Comment

You have the option to enter a comment here.

SNMP ID:

2.70.4.3.4

Telnet path:

Setup > IPv6 > Network > Loopback

Possible values:

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

Default:

empty

4.5 Lightweight DHCPv6 relay agent (LDRA)

Unlike a DHCPv6 relay agent, which has the full IPv6 features (such as ICMPv6) and can route data packets on the network (layer 3), a lightweight DHCPv6 relay agent as per RFC 6221 enables only the creation and forwarding of relay-agent information between DHCPv6 clients and DHCPv6 servers (layer 2).

In contrast to DHCPv4 snooping, the LDRA does not simply append the DHCPv6 packets with information about the relay agent: Instead, it packs the message from the client into a separate option, prepends its own relay-agent header and then forwards this DHCPv6 packet with its supplementary information to the DHCPv6 server (relay forward message).

The DHCPv6 server evaluates this data packet and sends a similarly packaged response to the relay agent. This then extracts the message and sends it to the requesting client (relay-reply message).

In LANconfig you can set up DHCPv6 snooping for each interface under **Interfaces > Snooping** and a click on **DHCPv6 snooping**.

IGMP snooping

IGMP snooping module activated: Auto

Unregistered data packets: Flood to router ports only

Port table

Static members...

Simulated queriers...

Advertise interval: 20 seconds

Query interval: 125 seconds

Query-Response interval: 10 seconds

Robustness: 2

Router advertisement snooping

In this table you can configure for each port the protocol filter for router advertisement messages.

RA-Snooping

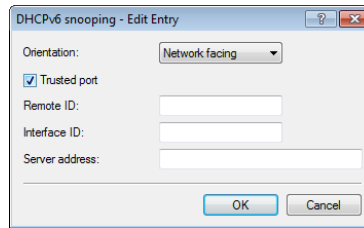
DHCP snooping

DHCP snooping allows for the interception of DHCP packets, which can be modified and/or filtered based on their contents and the interface they are received on.

DHCP snooping

DHCPv6 snooping

After selecting the appropriate interface, you can set the following:



Orientation

This is where you enable or disable DHCPv6 snooping. The following options are possible:

- **Network facing:** The LDRA uses this interface to communicate with a DHCPv6 server.
- **Client facing:** The LDRA uses this interface to communicate with DHCPv6 clients connected to the network.

The default setting **Network facing** disables the LDRA.

Trusted port

With this option enabled, the LDRA forwards DHCP requests from clients and also DHCP responses from DHCP servers. If this interface is classified as not trusted, the LDRA discards DHCPv6 requests to this interface. Similarly, the LDRA does not forward DHCPv6 responses with the wrong interface ID to the client.

Remote ID

According to RFC 4649, the remote ID uniquely identifies the client making a DHCPv6 request.

Interface ID

The interface ID uniquely identifies the interface used by a client to make a DHCPv6 request.

Server address

You can set the IPv6 address of a DHCPv6 server here.



Leave this field blank if you want to receive responses from all DHCPv6 servers on the network. Otherwise the LDRA reacts only to DHCPv6 responses from the server you have specified. In this case, the LDRA discards responses from other DHCPv6 servers.

You can use the following variables for **Remote ID** and **Interface ID**:

- **%:** Inserts a percent sign.
- **%c:** Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%i:** Inserts the name of the interface where the relay agent received the DHCP request.
- **%n:** Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- **%v:** Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p:** Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s:** Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- **%e:** Inserts the serial number of the relay agent, to be found for example under **Management > General**.

4.5.1 Additions to the Setup menu

DHCPv6-Snooping

This is where you can configure the lightweight DHCPv6 relay agent.

SNMP ID:

2.20.41

Telnet path:

Setup > LAN-Bridge

Port

Indicates the physical or logical interface to which this DHCPv6-snooping configuration applies.

SNMP ID:

2.20.41.1

Telnet path:

Setup > LAN-Bridge > DHCPv6-Snooping

Possible values:**LAN-x**

All physical LAN interfaces

WLAN-x

All physical WLAN interfaces

WLAN-x-x

All logical WLAN interfaces

P2P-x-x

All logical P2P interfaces

WLC-TUNNEL-x

All virtual WLC tunnels

Orientation

Enable or disable DHCPv6 snooping here.

SNMP ID:

2.20.41.2

Telnet path:

Setup > LAN-Bridge > DHCPv6-Snooping

Possible values:**Network-facing**

Disables DHCPv6 snooping for this interface. The LDRA does not forward any DHCPv6 requests to a DHCPv6 server.

Client-facing

Enables DHCPv6 snooping for this interface.

Default:

Network-facing

Type

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets.

SNMP ID:

2.20.41.3

Telnet path:

Setup > LAN-Bridge > DHCPv6-Snooping

Possible values:**Trusted**

The LDRA forwards DHCP requests from clients and also DHCP responses from DHCP servers.

Untrusted

If this interface is classified as untrusted, the LDRA discards DHCPv6-server requests to this interface. This prevents unauthorized clients from acting as "rogue DHCPv6 servers". Similarly, the LDRA does not forward DHCPv6 responses with the wrong interface ID to the client.



Interfaces that are facing clients should be set as untrusted.

Default:

Trusted

Remote ID

The remote ID according to RFC 4649 uniquely identifies the client that is making a DHCPv6 request.



This option is analogous to the DHCP option "remote ID" of the relay agent in the case of IPv4.

You can use the following variables:

- %: Inserts a percent sign.
- %c: Inserts the MAC address of the interface at which the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %i: Inserts the name of the interface on which the relay agent received the DHCP request.

- **%n**: Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For others clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

2.20.41.4

Telnet path:**Setup > LAN-Bridge > DHCPv6-Snooping****Possible values:**

Max. 30 characters [A-Z][a-z][0-9]#@[| } ~ ! \$ % & ' () * + - , / : ; < = > ? [\] ^ _ .

Default:*empty***Interface-ID**

The interface ID uniquely identifies the interface used by the client to make a DHCPv6 request.

You can use the following variables:

- **%**: Inserts a percent sign.
- **%c**: Adds the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%i**: Inserts the name of the interface on which the relay agent received the DHCP request.
- **%n**: Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For others clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

2.20.41.5

Telnet path:**Setup > LAN-Bridge > DHCPv6-Snooping**

Possible values:

Max. 30 characters `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]^_.`

Default:

empty

Server address

Here you can specify the IPv6 address of a DHCPv6 server.



Leave this field blank if you want to receive responses from all of the DHCPv6 servers on the network. Otherwise the LDRA reacts only to DHCPv6 responses from the server you have specified. In this case, the LDRA discards responses from other DHCPv6 servers.

SNMP ID:

2.20.41.6

Telnet path:

Setup > LAN-Bridge > DHCPv6-Snooping

Possible values:

Max. 39 characters `0123456789ABCDEFabcdef:.`

Default:

empty

4.6 Router advertisement snooping

In an IPv6 network, router advertisements are sent by routers, either periodically or upon request, to present themselves as a gateway for networked clients. As with DHCPv4, attackers can use this mechanism to deliver a fake network configuration to the requesting clients.

With RA snooping, the device mediates router advertisements from routers only, and not from clients. By specifying the address of a router, the router advertisements can be restricted to one specific router as the broadcaster.

In LANconfig you can set up RA snooping for each interface under **Interfaces > Snooping** and a click on **RA snooping**.

After selecting the appropriate interface, you can set the following:

Port type

Specify the preferred interface type here. The following options are possible:

- **Router:** The device mediates all of the RAs arriving at this interface (default).
- **Client:** The device discards all of the RAs arriving at this interface.

Router-Address

If you have selected the interface type **Router**, enter an optional router address here. If you specify a router address, the device will only mediate RAs from that router.

With the interface type **Client** selected, the device ignores this input field.

4.6.1 Additions to the Setup menu

RA-Snooping

You can configure the RA snooping here.

SNMP ID:

2.20.42

Telnet path:

Setup > LAN-Bridge

Port

Indicates the physical or logical interface to which this RA-snooping configuration applies.

SNMP ID:

2.20.42.1

Telnet path:

Setup > LAN-Bridge > RA-Snooping

Possible values:**LAN-x**

All physical LAN interfaces

WLAN-x

All physical WLAN interfaces

WLAN-x-x

All logical WLAN interfaces

P2P-x-x

All logical P2P interfaces

WLC-TUNNEL-x

All virtual WLC tunnels

Orientation

Specify the preferred interface type here.

SNMP ID:

2.20.42.3

Telnet path:

Setup > LAN-Bridge > RA-Snooping

Possible values:**Router**

The device mediates all of the RAs arriving at this interface.

Client

The device discards all of the RAs arriving at this interface.

Default:

Router

Router-Address

If you have selected the interface type **Router**, enter an optional router address here. If you specify a router address, the device will only mediate RAs from that router. With the interface type **Client** selected, the device ignores this input field.

SNMP ID:

2.20.42.4

Telnet path:

Setup > LAN-Bridge > RA-Snooping

Possible values:

Max. 39 characters 0123456789ABCDEFabcdef : .

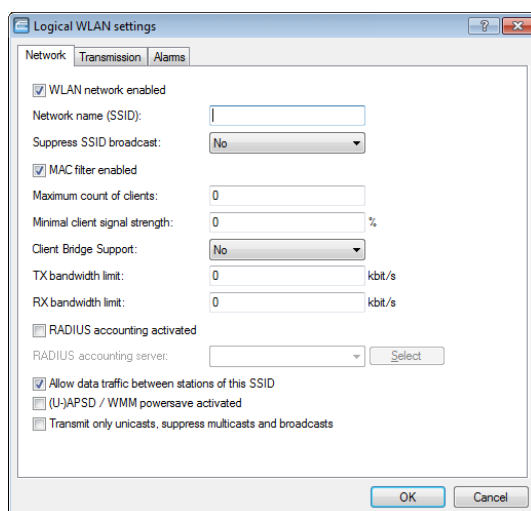
Default:

empty

5 RADIUS

5.1 Separate RADIUS accounting server for each SSID

As of LCOS 9.00 you can assign a separate RADIUS accounting server to each logical WLAN interface.



The following settings are made in LANconfig in **Wireless LAN > General > Logical WLAN settings > Network**.

- **RADIUS accounting activated**

Enable this option to switch on RADIUS accounting for this SSID.

- **RADIUS accounting server**

Enter a RADIUS accounting server for the respective SSID. The servers that can be selected here are specified in the table under **Wireless-LAN > Stations > RADIUS-Accounting-Server**.

5.1.1 Additions to the Setup menu

Servers

This table provides the option to specify alternative RADIUS accounting servers for logical WLAN interfaces. This means that you can use special accounting servers for selected WLAN interfaces instead of the globally specified server.

SNMP ID:

2.12.45.17

Telnet path:

Setup > WLAN > RADIUS-Accounting

Name

Name of the RADIUS server performing the accounting for WLAN clients. The name entered here is used to reference that server from other tables.

SNMP ID:

2.12.45.17.1

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

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

Default:

empty

Port

Port for communication with the RADIUS server during accounting

SNMP ID:

2.12.45.17.3

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

0 ... 65535

Default:

0

Key

Enter the key (shared secret) for access to the accounting server here. Ensure that this key is consistent with that specified in the accounting server.

SNMP ID:

2.12.45.17.4

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

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

Default:*empty***Loopback-Addr.**

You have the option to enter a different address here (name or IP) to which the RADIUS accounting server sends its reply message. To do this, select:

- Name of the IP network (ARF network), whose address should be used
- INT for the address of the first Intranet
- DMZ for the address of the first DMZ



If an interface with the name "DMZ" already exists, the device will select that address instead.

- LB0...LB15 for one of the 16 loopback addresses or its name
 - Any IPv4 Address
-



If the sender address that is entered here is a loopback address, remote stations that work with masking will also use it **unmasked** !

By default, the server returns its replies to the IP address of your device without you entering it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

SNMP ID:

2.12.45.17.5

Telnet path:**Setup > WLAN > RADIUS-Accounting > Servers****Possible values:**

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

Default:*empty***Protocol**

Using this item you specify the protocol that the accounting server uses.

SNMP ID:

2.12.45.17.6

Telnet path:**Setup > WLAN > RADIUS-Accounting > Servers**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

Backup

Enter the name of the RADIUS backup server used for the accounting of WLAN clients if the actual accounting server is not available. This allows you to specify a backup chaining of multiple backup servers.

SNMP ID:

2.12.45.17.7

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

Name from **Setup > WLAN > RADIUS-Accounting > Server**

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

Default:

empty

Host name

Here you enter the IPv4 or IPv6 address or hostname of the RADIUS server used by RADIUS clients to perform accounting for WLAN clients.



The RADIUS client automatically detects which address type is involved.



The general values for repetitions and timeouts must also be specified in the RADIUS section.

SNMP ID:

2.12.45.17.8

Telnet path:

Setup > WLAN > RADIUS-Accounting > Servers

Possible values:

IPv4/IPv6 address or hostname, max. 64 characters from `[A-Z][a-z][0-9].-: %`

Default:

empty

Accounting server

Using this parameter, you define a RADIUS accounting server for the corresponding logical WLAN interface.

SNMP ID:

2.23.20.1.22

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:

Name from **Setup > WLAN > RADIUS-Accounting > Server**

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

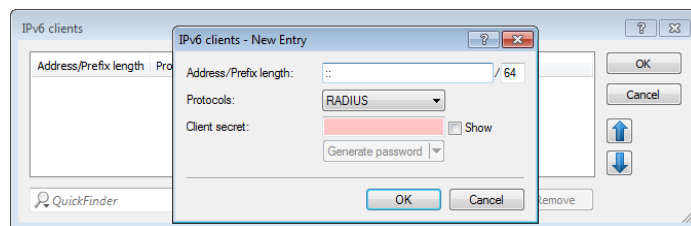
Default:

empty

5.2 Accessing the RADIUS server via IPv6

As of LCOS 9.00, the RADIUS server is also accessible for IPv6 clients. You can configure these clients in LANconfig under **RADIUS server > General** by clicking on **IPv6 clients**.

IPv6 clients



The following values are entered for each client:

Address/prefix length

IP address (or address range) of the clients for which the password entered in this dialog applies.



To use an address, the prefix length must be 128 bits. The entry "fd00::/64", for example, permits access to the entire network, the entry "fd00::1/128" only permits exactly one client.

Protocols

Protocol for communication between the internal server and the clients.

Client secret

Password required by the clients for access to the internal server.



In order for IPv6 clients to access the RADIUS server, a corresponding inbound rule must be entered in the IPv6 firewall, if necessary.

5.2.1 Additions to the Setup menu

IPv6 clients

Specify the RADIUS login data of IPv6 clients here.

SNMP ID:

2.25.10.16

Telnet path:

Setup > RADIUS > Server

Address-Prefix-Length

This value specifies the IPv6 network and the prefix length, e.g., "fd00::/64". The entry "fd00::/64", for example, permits access to the entire network, the entry "fd00::1/128" only permits exactly one client.

SNMP ID:

2.25.10.16.1

Telnet path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:

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

Default:

empty

Address-Prefix-Length

This value specifies the password required by the clients for access to the internal server.

SNMP ID:

2.25.10.16.2

Telnet path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:

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

Default:

empty

Protocols

This selection specifies the protocol for communication between the internal server and the clients.

SNMP ID:

2.25.10.16.4

Telnet path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:

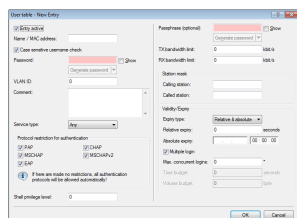
RADIUS
RADSEC
All

Default:

RADIUS

5.3 New attribute in the RADIUS server, shell privilege level

As of LCOS version 9.00, the RADIUS server supports a vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept. This attribute can be specified under **RADIUS Server > General > User table**.



5.3.1 Using RADIUS to login to the LCOS management GUI

Currently users can login to the management interface of a device by means of RADIUS, TACACS+, or the internal user management. With RADIUS, this is possible for the following protocols:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

! RADIUS authentication via SNMP is not currently supported.

! A RADIUS authentication via LL2M (LANCOM Layer-2 Management Protocol) is not supported, because LL2M requires plain text access to the password that is stored in the device.

The RADIUS server handles user management in terms of authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin access accounts in large network installations with multiple routers.

Logging in via a RADIUS server follows this procedure:

1. At login, the device sends the user's credentials to the RADIUS server on the network. The server data are stored in the device.
2. The server checks the credentials for validity.
3. If the data is invalid, the server sends a corresponding message to the device, which aborts the login process with an error message.
4. If the credentials are valid, the server returns the access rights and privileges to the device and the user then has access to the approved features and directories.
5. If the user's sessions are subject to budgeting by the RADIUS server (accounting), the device stores the session data including the start time, end time, user name, authentication mode and, if available, the port used.

In LANconfig you can set the authentication method under **Management > Authentication**.

Device Login Authentication

Select the method for authenticating users while accessing the device.

Authentication via: Internal administrator table

RADIUS authentication

Specify the attribute to be used by the RADIUS server for transmitting access rights.

Access rights via: Provider specific attribute

Specify if accounting data shall be transmitted via RADIUS.

Accounting: No

Configure the RADIUS servers in the following table.

RADIUS server...

Device login authentication

In the section **Device login authentication** you select the method for authenticating users when they access the device management GUI:

- **Internal administrator table:** The device handles over the overall user administration including the user login name, password, access rights, and privileges.
- **RADIUS:** User administration is handled by a RADIUS server on the network.
- **TACACS+:** User administration is handled by a TACACS+ server on the network.

RADIUS authentication

In the **RADIUS authentication** section you specify the necessary RADIUS server data and the additional administrative data.

Access rights via

The RADIUS server stores the user authorization. When a request arrives, the RADIUS server returns the access rights, privileges and the login data to the device, which then logs in the user with the appropriate rights.

Normally access rights are set in the RADIUS management privilege level (attribute 136), so that the device only needs to map the returned value to its internal access rights. However, it may be that the RADIUS server additionally needs to transfer privileges, or that attribute 136 is already used for other purposes and/or for vendor-specific authorization attributes. In this case, the device can evaluate a manufacturer-specific authorization.

- **Provider specific attribute:** The unit evaluates the vendor-specific attribute.
- **Management privilege level attribute:** The unit evaluates the management privilege level attribute from the RADIUS server.
- **Shell privilege attribute:** The unit evaluates the shell privilege attribute from the RADIUS server.

Accounting

Here you specify whether the device should record the user's session.

- **No:** The device does not record the session.
- **Yes:** The device records the session (start, end, username, authentication mode, port).

RADIUS server

You can adjust the RADIUS server settings in this table.

- **Profile name:** Enter a name for the RADIUS server.
- **Backup profile:** Specify the name of the alternative RADIUS server to which the device forwards requests when the first RADIUS server cannot be reached.



The backup server requires an additional entry in the Server table.

- **Server address:** Enter the IPv4 address of the RADIUS server here.
- **Port:** Specify here the port used by the RADIUS server to communicate with the device.
- **Shared secret:** Enter the password for accessing the RADIUS server and repeat it in the second input field.
- **Sender address:** This is where you can specify an optional sender address to be used by the device instead of the one that would normally be automatically selected for this target address.
- **Protocol:** Specify here the protocol used by the RADIUS server to communicate with the device.
- **Category:** Set the category for which the RADIUS server applies.

5.3.2 Additions to the Setup menu

Access rights transfer

The RADIUS server stores the user authorization. When a request is received, the RADIUS server returns the user's the access rights, privileges and login data to your device, which then logs in the user with the appropriate privileges.

Normally, access rights are set in the RADIUS management privilege level (attribute 136), so all the device needs to do is to map the transmitted value to its internal access rights (option **Mapped**). The attribute can have the following values, which are mapped by the device:

Attribute	Access rights
1	User, read-only
3	User, write-only
5	Admin, read-only, no trace rights
7	Admin, read and write, no trace rights
9	Admin, read-only

Attribute	Access rights
11	Admin, read and write
15	Supervisor

 All other values are mapped by the device to 'No access'.

However, it could be that the RADIUS server additionally needs to transfer privileges, or that attribute 136 is already used for other purposes or for vendor-specific authorization attributes. If this is the case, you should select Vendor-Specific attributes. These attributes are specified as follows, based on the vendor ID '2356':

- Access rights ID: 11
- Privileges ID: 12

The values transferred for access rights are identical to those mentioned above. If the RADIUS server should also transfer privileges, you achieve this as follows:

1. You open the console of the device.
2. Go to the directory **Setup > Config > Admins**.
3. The command `set ?` shows you the current mapping of privileges to the corresponding hexadecimal code (e.g. `Device-Search (0x80)`).
4. In order to combine privileges, you add their hex values.
5. Convert the hexadecimal value to a decimal number.
6. You can use this decimal value as the Privileges ID to transfer the corresponding privileges.

SNMP ID:

2.11.81.2

Telnet path:

Setup > Config > Radius

Possible values:

**Vendor specific
Mapped
Shell privilege**

Default:

Vendor specific

Shell-Priv.-Level

This field contains a vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept.

SNMP ID:

2.25.10.7.21

Telnet path:

Setup > RADIUS > Server > Users

Possible values:

0 ... 4294967295

Default:

0

5.4 RADIUS client: Alternative input of hostnames instead of IP addresses

As of LCOS version 9.00, a RADIUS server address can be optionally specified as an IPv4 or IPv6 address, or as a DNS name.


This upgrade changes the following paths in the Setup part of the LCOS menu tree:

- **2.2.22.11: Server-Hostname** replaces **2.2.22.2: Server address**
- **2.12.29.16: Server-Hostname** replaces **2.12.29.1: Server address**
- **2.12.29.17: Backup-Server-Hostname** replaces **2.12.29.4: Backup-Server-IP-Address**
- **2.12.45.17.8: Hostname** replaces **2.12.45.17.2: Server address**
- **2.24.3.13: Auth.-Server-Hostname** replaces **2.24.3.2: Auth.-Server-Address**
- **2.24.3.14: Acc.-Server-Hostname** replaces **2.24.3.5: Acc.-Server-Address**
- **2.25.10.3.13: Hostname** replaces **2.25.10.3.2: IP address**
- **2.25.10.3.14: Hostname** replaces **2.25.10.3.8: Accnt.-IP-Address**
- **2.30.3.8: Host-Name** replaces **2.30.3.2: IP address**

5.4.1 Additions to the Setup menu

Server-Hostname

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server to be used to centrally manage the users.

 The RADIUS client automatically detects which address type is involved.




SNMP ID:

2.2.22.11

Telnet path:**Setup > WAN > RADIUS****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Default:***empty*

Server-Hostname

Here you enter the IP address (IPv4, IPv6) or hostname of the RADIUS server used by the RADIUS client to check the authorization of WLAN clients by means of the MAC address (authentication).


-
-  The RADIUS client automatically detects which address type is involved.
-
-  To use the RADIUS function for WLAN clients, in LANconfig navigate to **Wireless-LAN > Stations** and set the parameter **Filter stations** to "Transfer data from the listed stations, authenticate all other data via RADIUS or filter it out". You must also specify the general values for repetitions and timeouts in the RADIUS section.
-
-  In the RADIUS server, you must enter the WLAN clients as follows:
 - The username is the MAC address in the format AABBCD-DEEFF.
 - The password for all users is identical with the key (shared secret) for the RADIUS server.

SNMP ID:

2.12.29.16

Telnet path:**Setup > WLAN > RADIUS-Access-Check****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Default:***empty***Backup-Server-Hostname**

Here you enter the IP address (IPv4, IPv6) or hostname of the backup RADIUS server used by the RADIUS client to check the authorization of WLAN clients by means of the MAC address (authentication).


-
-  The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.12.29.17

Telnet path:**Setup > WLAN > RADIUS-Access-Check****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Default:***empty***Auth.-Server-Host-Name**

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server which the Public Spot contacts for authentication with this provider.


 The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.24.3.13

Telnet path:**Setup > Public-Spot-Module > Provider-Table****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-:%`**Default:***empty***Acc.-Server-Host-Name**

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server which the Public Spot contacts for accounting of the access for this provider.


 The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.24.3.14

Telnet path:**Setup > Public-Spot-Module > Provider-Table****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-:%`**Default:***empty***Host name**

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server to which the RADIUS client forwards requests from the WLAN client.

 The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.25.10.3.13

Telnet path:**Setup > RADIUS > Server > Forward-Servers**

Possible values:


Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Default:

empty

Host name

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server to which the RADIUS client forwards accounting data packets.

 The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.25.10.3.14

Telnet path:

Setup > RADIUS > Server > Forward-Servers

Possible values:


Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Default:

empty

Host name

Enter the IP address (IPv4, IPv6) or the hostname of the RADIUS server.

 The RADIUS client automatically detects which address type is involved.

SNMP ID:

2.30.3.8

Telnet path:

Setup > IEEE802.1x > RADIUS-Server

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Default:

empty

Special values:**DEFAULT**

The name "DEFAULT" is reserved for all WLAN networks that use IEEE 802.1x for authentication and that do not have their own RADIUS server. Every WLAN that uses authentication by IEEE 802.1x can use its own RADIUS server after specifying appropriate values for 'Key1/Passphrase'.

5.5 EAP-SIM module in the RADIUS server

The RADIUS server contains an EAP-SIM module, which enhances the device with the ability to simulate the home location register (HLR) of a mobile provider. An HLR usually generates the keys for registered SIM cards so that a RADIUS server can authenticate a client by means of EAP-SIM.

The required keys can be manually specified and stored on the RADIUS server, which makes an HLR unnecessary. EAP-SIM is used in connection with Hotspot 2.0, for example.

5.5.1 Additions to the Setup menu

EAP-SIM

802.11u networks make it possible for WLAN clients in the area of coverage to automatically log in to the provider's hotspot with the login data of the provider's own SIM card.

In this directory you specify the SIM access credentials for automatic authentication.

SNMP ID:

2.25.10.10.18

Telnet path:

Setup > RADIUS > Server > EAP

Card-Keys

Using this table you configure the SIM cards for automatic authentication with EAP SIM.

SNMP ID:

2.25.10.10.18.1

Telnet path:

Setup > RADIUS > Server > EAP > EAP-SIM

User name

Enter the user name for the EAP-SIM authentication here. The user name for the EAP-SIM consists of

- a leading 1,
- the Mobile Country Code (MCC),
- the Mobile Network Code (MNC),
- the International Mobile Subscriber Identity (IMSI) and

- the @realm.

This results in the following syntax:

```
Syntax: 1<MCC><MNC><IMSI>@<Realm> Example:
1262011234567890@wlan.mnc001.mcc262.3gppnetwork.org
```

SNMP ID:

2.25.10.10.18.1.1

Telnet path:

Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys

Possible values:

Max. 48 characters from `[A-Z][a-z][0-9]@{ | } ~ ! $ % & ' () * + - , / : ; < = > ? [\] ^ _ . # ` ~`

Default:

empty

Calling Station ID Mask

This mask restricts the validity of the entry to certain IDs. The ID is sent by the calling station (WLAN client). During the authentication by 802.1X, the MAC address of the calling station is transmitted in ASCII format (uppercase only). Each pair of characters is separated by a hyphen (e.g. 00-10-A4-23-19-C0).

SNMP ID:

2.25.10.10.18.1.5

Telnet path:

Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys

Possible values:

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

Special values:

*

The wildcard * can be used to include whole groups of IDs to act as a mask.

Default:

empty

Called Station ID Mask

This mask restricts the validity of the entry to certain IDs. The ID is sent by the called station (BSSID and SSID of the AP). During the authentication by 802.1X, the MAC address (BSSID) of the called station is transmitted in ASCII format (uppercase only). Each pair of characters is separated by a hyphen; the SSID is appended after a separator, a colon (e.g. 00-10-A4-23-19-C0:AP1).

SNMP ID:

2.25.10.10.18.1.6

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**Max. 64 characters `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`**Special values:**

*

The wildcard * can be used to include whole groups of IDs to act as a mask.

With the mask * : `AP1*`, for example, you define an entry that applies to a client in the radio cell with the name `AP1`, irrespective of which AP the client associates with. This allows the client to switch (roam) from one AP to the next while always using the same authentication data.

Default:*empty***Rand1**

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

SNMP ID:

2.25.10.10.18.1.7

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**Max. 32 characters from `0123456789abcdef`**Default:**

00000000000000000000000000000000

SRES1

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

SNMP ID:

2.25.10.10.18.1.8

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**Max. 8 characters from `0123456789abcdef`

Default:

00000000

Kc1

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

SNMP ID:

2.25.10.10.18.1.9

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**

Max. 16 characters from 0123456789abcdef

Default:

0000000000000000

Rand2

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

SNMP ID:

2.25.10.10.18.1.10

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**

Max. 32 characters from 0123456789abcdef

Default:

00000000000000000000000000000000

SRES2

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

SNMP ID:

2.25.10.10.18.1.11

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**

Max. 8 characters from 0123456789abcdef

Default:

00000000

Kc2

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

SNMP ID:

2.25.10.10.18.1.12

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**

Max. 16 characters from 0123456789abcdef

Default:

0000000000000000

Rand3

The authentication via GSM is based on a challenge-response mechanism with random numbers and authentication keys. In this field you specify a 128-bit random number, which is sent to the client to create the two keys (authentication, encryption of payload data).

SNMP ID:

2.25.10.10.18.1.13

Telnet path:**Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys****Possible values:**

Max. 32 characters from 0123456789abcdef

Default:

00000000000000000000000000000000

SRES3

This field contains the SRES key (Signed RESponse) which the client must generate from the 128-bit random number in order to correctly authenticate.

SNMP ID:

2.25.10.10.18.1.11

Telnet path:

Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys

Possible values:

Max. 8 characters from 0123456789abcdef

Default:

00000000

Kc3

This field contains the Kc key (Ciphering Key) which the client must generate from the 128-bit random number in order to encrypt the payload data.

SNMP ID:

2.25.10.10.18.1.15

Telnet path:

Setup > RADIUS > Server > EAP > EAP-SIM > Card-Keys

Possible values:

Max. 16 characters from 0123456789abcdef

Default:

0000000000000000

6 Public Spot

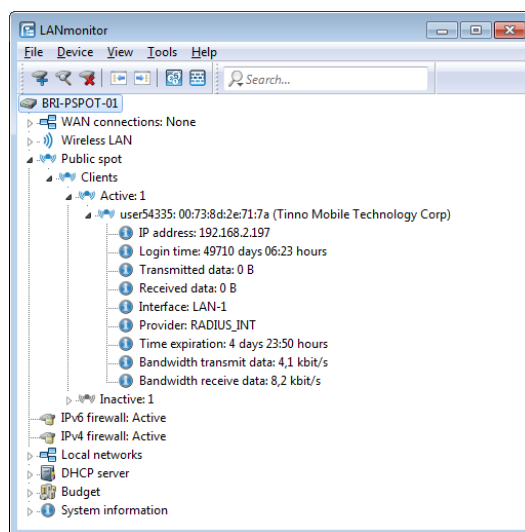
6.1 Number format for Smart Ticket

Starting with version 9.00, LCOS checks the entered phone number for invalid characters. Only numbers between 0 and 9 are allowed. The user must enter 5 to 15 numbers (excluding the country code).

6.2 Viewing Public Spot clients

LANmonitor can optionally display detailed information about the clients associated with the Public Spot.

1. Open the menu item **Public Spot > Clients**.
2. Double-click on **Active** to display the active clients, or on **Inactive** to display inactive clients.
3. Double-click on a client to retrieve detailed information about it.



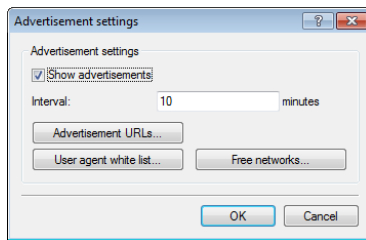
6.3 Displaying advertising to Public Spot users

You can optionally display advertising to Public Spot users at configurable time intervals. The Public Spot shows the advertisement in the normal browser window of the user and not using a pop-up, since all modern browsers normally block pop-ups. In the Public Spot station table, a client can have one of three states:

- **Authenticated:** The client is logged on and can surf in Internet.
- **Unauthenticated:** The client is not logged on and cannot surf in Internet.
- **Advertisement:** The next time a client calls a URL, it is redirected to an advertisement URL.

You have the option to exclude certain networks and user agents from the display of advertisements by means of a whitelist.

1. In the device configuration, select the menu branch **Public Spot > Server** and click on **Advertisement settings**.
2. Enable the **Show advertisements** checkbox.



You can now change the interval between advertisement displays, and also other settings.

3. Under **Interval** you specify the time in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.
4. Click on **Advertisement URLs** to add an advertisement URL. If you add multiple URLs, the Public Spot displays them in sequence after the specified interval.
5. Optional: Click on **User agent white list** to add user agents, which the Public Spot excludes from the display of advertisements.
6. Optional: Click on **Free networks** to add networks, which the Public Spot excludes from the display of advertisements. This can be used in various ways, for example to enter the automatic search URLs used by the browser, e.g. `*.google.com`. Typically, a browser sends keyboard input at the address bar to a search engine; by setting the exception, the advertisement page does not responding to this.



Login-free networks are generally ad-free networks. There is no need to explicitly include these networks into the whitelist.

7. Close all dialog windows by clicking on **OK**.

Public Spot users will be redirected to an advertisement URL after the specified time interval unless they are using a whitelisted user agent or they are located in a free network.

The timing of the advertisements refers to the session time of the active Public Spot clients. If a client stop sending data for a certain time, then the interval before the Public Spot displays advertising again will be delayed by this time.

6.3.1 Additions to the Setup menu

Advertisement

This menu gives you the option to enable or disable advertising pop-ups, and to edit these.

SNMP ID:

2.24.43

Telnet path:

Setup > Public-Spot-Module

Active

This menu switches the advertisements on or off.

SNMP ID:

2.24.43.1

Telnet path:**Setup > Public-Spot-Module > Advertisement****Possible values:****No**
Yes**Default:**

No

Interval

This item allows you to specify the interval after which the Public Spot redirects a user to an advertisement URL.

SNMP ID:

2.24.43.2

Telnet path:**Setup > Public-Spot-Module > Advertisement****Possible values:**

0 ... 65535 Minutes

Default:

10

Special values:**0**
Redirection takes place directly after signing on.**URL**

This item is used to enter the advertisement URLs. If multiple URLs are entered, the Public Spot displays them in sequence after the specified interval.

SNMP ID:

2.24.43.3

Telnet path:**Setup > Public-Spot-Module > Advertisement****Possible values:**Max. 150 characters from `#[A-Z][a-z][0-9]@{ }~!$%&'()+,-./:;<=>?[\]^_`~``**Default:***empty*

Contents

This parameter specifies the advertisement URL(s).

SNMP ID:

2.24.43.3.1

Telnet path:

Setup > Public-Spot-Module > Advertisement > URL

Possible values:

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

Default:

empty

User-Agent-White-List

This item is used to add user agents which the Public Spot excludes from advertising.

SNMP ID:

2.24.43.4

Telnet path:

Setup > Public-Spot-Module > Advertisement

Possible values:

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

Default:

empty

User-Agent

Name of the user agent you included in the white list.

SNMP ID:

2.24.43.4.1

Telnet path:

Setup > Public-Spot-Module > Advertisement > User-Agent-White-List

Possible values:

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

Default:

empty

Process-WISPr-Redirect-URL

If the access-accept message from the RADIUS server contains the attribute 'WISPr-Redirection-URL', the Public Spot client is redirected to this URL after successful authentication. This scenario behaves in the same way as if the RADIUS server were to return 'LCS-Advertisement-URL=any' and 'LCS-Advertisement-Interval=0'. There is no need to set the **Operating** switch. The attribute 'WISPr-Redirection-URL' is sufficient. This configuration is useful if, after authentication (e.g. by MAC authentication), a client is to be redirected to a page just once.

SNMP ID:

2.24.43.5

Telnet path:**Setup > Public-Spot-Module > Advertisement****Possible values:**

No
Yes

Default:

No

Free networks

This item is used to add networks which the Public Spot excludes from advertising.

SNMP ID:

2.24.43.6

Telnet path:**Setup > Public-Spot-Module > Advertisement****Host name**

Enter the IP address of the additional server or network that your Public Spot users are to be given advertisement-free access to.

Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow advertisement-free access to all of the subdomains of a particular domain. The entry *.google.com allows the addresses mail.google.com, and maps.google.com, etc.

SNMP ID:

2.24.43.6.1

Telnet path:**Setup > Public-Spot-Module > Advertisement > Free-Networks****Possible values:**

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

Default:*empty***Mask**

Enter the netmask of the additional server or network that your Public Spot users are to be given advertisement-free access to.

If you wish to authorize a domain or just a single workstation with the address named earlier, set 255 . 255 . 255 . 255 as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value 0 . 0 . 0 . 0), the device ignores the table entry.

SNMP ID:

2.24.43.6.2

Telnet path:**Setup > Public-Spot-Module > Advertisement > Free-Networks****Possible values:**

Max. 15 characters from [0–9] .

Default:

0.0.0.0

6.3.2 Extensions to the RADIUS attributes

The Public Spot additionally evaluates the following vendor-specific RADIUS attributes in the Access Accept of the RADIUS authentication server.



The **Advertisement enabled** switch does not have to be set. It is sufficient if the attribute is present in the RADIUS message.

26

Vendor 2356(LCS) ID 13**LCS-Advertisement-URL**

Specifies a comma-separated list of advertisement URLs.

26

Vendor 2356(LCS) ID 14**LCS-Advertisement-Interval**

Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.

6.4 Additional attributes for the XML interface

With LCOS 9.00 the scope of the attributes that are available for creating a new user via the XML interface has been extended. The attributes below mostly correspond to the parameters which are also configurable over the RADIUS user table.

The XML interface can now process the following XML elements in the **login request**:

VLAN_ID (optional)

Custom VLAN ID assigned by the device to the Public Spot user upon login. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the XML interface.

The value 0 disables use of a VLAN.

PROVIDER (occasionally required)

Name of the RADIUS server used by the Public Spot for user authentication and accounting. If you do not specify a RADIUS server, the Public Spot uses the server configured globally for the module.

This XML element is mandatory if you

- have configured multiple RADIUS servers for the Public Spot module.
- want to use the XML interface without RADIUS authentication but with RADIUS accounting.

Specifying this XML element is otherwise optional.



The referenced RADIUS server must be present in the configuration.

TXRATELIMIT (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the uplink.

RXRATELIMIT (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the downlink.

SECONDSEXPIRE (optional)

The maximum online time for a user account in seconds. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

The value 0 switches off the monitoring of the time budget.

TRAFFICEXPIRE (optional)

Maximum data volume for a user account in bytes. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

The value 0 switches off the monitoring of the data volume.

6.5 Dynamic change of a user session via the XML interface

If a Public Spot user has to authenticate only and no further changes are required throughout the login, then the parameter **RADIUS_LOGIN** will meet your needs. On the other hand, if you need to change the attributes of an ongoing session for a Public Spot user, you have the option of using **RADIUS_CoA**. To implement a change, your external hotspot gateway sends a **RADIUS-CoA-Request** to the Public Spot, which directly transfers the changes in it to the **Station table** under **Status > Public-Spot**.

One application for CoA messages is the automatic throttling of bandwidth: If a Public Spot user has consumed his/her volume budget, an external hotspot gateway is able to throttle the user's bandwidth by evaluating the accounting data and sending a CoA message to the Public Spot.

The XML messages for negotiations between the hotspot gateway and the Public Spot appear as follows:

RADIUS-CoA-Request

The external gateway sends the data with the session change to the Public Spot. The Public Spot then changes the session data in the station table for the authenticated user 'user2350'.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In the example above, the user is assigned a session duration of 3,600 seconds, a transferable data volume of 10,000,000 bytes, and a transmit and receive bandwidth of 100 kbps.

RADIUS-CoA-Response:

The XML interface sends a confirmation to the external hotspot gateway that the session data was changed:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In case of throttling, the change to the user session always affects the quota that is still available to the user. For instance, if the user was logged on for one hour already, then a change of the time quota to six hours means that just five hours remain. If the time quota is less than the time the user is already logged on, the Public Spot logs out the user and sends a logout message to the hotspot gateway.

7 WLAN

7.1 Support of 802.11ac WLAN interfaces

As of version 9.00, LCOS provides support of the 802.11ac standard for devices with the appropriate hardware.

7.1.1 Additions to the Status menu

Rx-STBC-HT

Indicates whether and how many streams the corresponding WLAN client can receive using the STBC technique when data transmission is in the 802.11n (HT) mode.

SNMP ID:

1.3.32.68

Telnet path:

Status > WLAN > Station-table

Possible values:

None
One
Two
Three

Rx-STBC-VHT

Indicates whether and how many streams the corresponding WLAN client can receive using the STBC technique with data transmission in the 802.11ac-(VHT) mode.

SNMP ID:

1.3.32.69

Telnet path:

Status > WLAN > Station-table

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the corresponding WLAN client supports the use of the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.32.70

Telnet path:

Status > WLAN > Station-table

Possible values:**None**

The WLAN client does not support LDPC or it does not provide information about it.

HT

The WLAN client supports LDPC in the 802.11n (HT) mode. HT = high throughput.

VHT

The WLAN client supports LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Tx-STBC

Indicates whether and in which mode the detected network is capable of transmitting with STBC (space time block coding).

SNMP ID:

1.3.34.49

Telnet path:

Status > WLAN > Scan-Results

Possible values:**None**

The detected WLAN does not support STBC or provides no information about the mode.

HT

The detected WLAN permits data packets to be sent with STBC in the 802.11n (HT) mode. HT = high throughput.

VT

The detected WLAN permits data packets to be sent with STBC in the 802.11ac (VHT) mode. VHT = very high throughput.

Rx-STBC-HT

Indicates whether and how many streams the detected WLAN can receive using the STBC technique with data transmission in the 802.11n (HT) mode.

SNMP ID:

1.3.34.50

Telnet path:

Status > WLAN > Scan-Results

Possible values:

None

One

Two

Three

Rx-STBC-VHT

Indicates whether and how many streams the detected WLAN can receive using the STBC technique with data transmission in the 802.11ac (VHT) mode.

SNMP ID:

1.3.34.51

Telnet path:

Status > WLAN > Scan-Results

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the detected WLAN supports the use of the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.34.52

Telnet path:

Status > WLAN > Scan-Results

Possible values:

None
The detected WLAN does not support LDPC or it does not provide information about it.
HT
The detected WLAN supports LDPC in the 802.11n (HT) mode. HT = high throughput.
VHT
The detected WLAN supports LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Rx-STBC-HT

Indicates whether and how many streams the P2P partner can receive using the STBC technique when data transmission is in the 802.11n (HT) mode.

SNMP ID:

1.3.36.1.48

Telnet path:

Status > WLAN > Interpoints > Access-point-list

Possible values:

None
One
Two
Three

Rx-STBC-VHT

Indicates whether and how many streams the P2P partner can receive using the STBC technique when data transmission is in the 802.11ac (VHT) mode.

SNMP ID:

1.3.36.1.49

Telnet path:

Status > WLAN > Interpoints > Access-point-list

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the AP for the P2P connection uses the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.36.1.50

Telnet path:

Status > WLAN > Interpoints > Access-point-list

Possible values:**None**

The AP is not using LDPC either because the P2P partner does not support LDPC or it does not provide information about the mode.

HT

The AP uses LDPC in the 802.11n (HT) mode. HT = high throughput.

VHT

The AP uses LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Rx-STBC-HT

Indicates whether and how many streams the physical WLAN interface can receive using the STBC technique with data transmission in the 802.11n (HT) mode.

SNMP ID:

1.3.43.51.42

Telnet path:

Status > WLAN > Client > Interfaces

Possible values:

None
One
Two
Three

Rx-STBC-VHT

Indicates whether and how many streams the physical WLAN interface can receive using the STBC technique with data transmission in the 802.11ac (VHT) mode.

SNMP ID:

1.3.43.51.43

Telnet path:

Status > WLAN > Client > Interfaces

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the physical WLAN interface uses the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.43.51.44

Telnet path:

Status > WLAN > Client > Interfaces

Possible values:

None
The physical WLAN interface does not use LDPC.

HT
The physical WLAN interface uses LDPC in the 802.11n (HT) mode. HT = high throughput.

VHT
The physical WLAN interface uses LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Channel bandwidths

Indicates which channel bandwidths are supported by the corresponding network.

SNMP ID:

1.3.44.44

Telnet path:

Status > WLAN > Competing-networks

Possible values:

20MHz
Channels bundled at 20MHz.

40MHz
Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidth

Indicates which channel bandwidths are currently being used by the corresponding network.

SNMP ID:

1.3.44.45

Telnet path:

Status > WLAN > Competing-networks

Possible values:**20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Tx-STBC

Indicates whether and in which mode the detected remote station is capable of transmitting with STBC (space time block coding).

SNMP ID:

1.3.44.49

Telnet path:

Status > WLAN > Competing-networks

Possible values:**None**

The detected remote station does not support STBC or provides no information about the mode.

HT

The detected remote station permits data packets to be sent with STBC in the 802.11n (HT) mode. HT = high throughput.

VT

The detected remote station permits data packets to be sent with STBC in the 802.11ac (VHT) mode. VHT = very high throughput.

TX STBC HT

Indicates whether and how many streams the detected remote station can receive using the STBC technique with data transmission in the 802.11n (HT) mode.

SNMP ID:

1.3.44.50

Telnet path:

Status > WLAN > Competing-networks

Possible values:**None****One****Two****Three****TX STBC VHT**

Indicates whether and how many streams the detected remote station can receive using the STBC technique with data transmission in the 802.11ac (VHT) mode.

SNMP ID:

1.3.44.51

Telnet path:

Status > WLAN > Competing-networks

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the detected remote station supports the use of the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.44.52

Telnet path:

Status > WLAN > Competing-networks

Possible values:**None**

The corresponding remote station does not support LDPC or it does not provide information about it.

HT

The remote station supports LDPC in the 802.11n (HT) mode. HT = high throughput.

VHT

The remote station supports LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Channel bandwidths

Shows which channel bandwidth the WLAN supports.

SNMP ID:

1.3.55.39

Telnet path:

Status > WLAN > WLAN-Parameter

Possible values:**20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidth

Shows which channel bandwidth the WLAN is using.

SNMP ID:

1.3.55.40

Telnet path:

Status > WLAN > WLAN-Parameter

Possible values:**20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Rx-STBC-HT

Indicates whether and how many streams an AP on the WLAN can receive using the STBC technique when data transmission is in the 802.11n (HT) mode.

SNMP ID:

1.3.55.42

Telnet path:

Status > WLAN > WLAN-Parameter

Possible values:

None
One
Two
Three

Rx-STBC-VHT

Indicates whether and how many streams an AP on the WLAN can receive using the STBC technique when data transmission is in the 802.11ac (VHT) mode.

SNMP ID:

1.3.55.43

Telnet path:

Status > WLAN > WLAN-Parameter

Possible values:

None
One
Two
Three
Four
Five
Six
Seven

LDPC

Indicates whether the corresponding WLAN supports the use of the low density parity check (LDPC) in relation to 802.11n/802.11ac bit rates.

SNMP ID:

1.3.55.44

Telnet path:

Status > WLAN > WLAN-Parameter

Possible values:

None
The corresponding WLAN does not support LDPC or it does not provide information about it.

HT
The WLAN supports LDPC in the 802.11n (HT) mode. HT = high throughput.

VHT
The WLAN supports LDPC in the 802.11ac (VHT) mode. VHT = very high throughput.

Channel bandwidth

Shows which channel bandwidth is configured for the physical WLAN interface.

SNMP ID:

1.3.57.19

Telnet path:

Status > WLAN > Radios

Possible values:**20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidth

Shows which channel bandwidth is configured for the corresponding frequency band.

SNMP ID:

1.3.63.1.18

Telnet path:

Status > WLAN > Noise-immunity > Current-parameters

Possible values:**20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

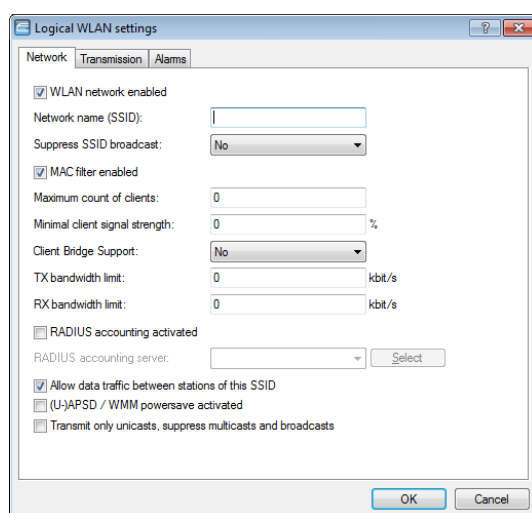
T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

7.2 Specifying client-bridge mode and bandwidth limit for each SSID

As of LCOS 9.00 you have the option of specifying the client-bridge mode and bandwidth limits for individual SSIDs.

Changes to stand-alone APs



The following settings are made in LANconfig in **Wireless LAN > General > Logical WLAN settings > Network**.

- **Client-bridge support**

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

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

- **TX bandwidth limit**

With this setting, you define the overall bandwidth that is available for transmission within this SSID (limit in kbps). A value of 0 disables the limit.

- **RX bandwidth limit**

With this setting, you define the overall bandwidth that is available in the reception direction within this SSID (limit in kbps). A value of 0 disables the limit.

The settings of this name are thus removed from LANconfig under **Wireless LAN > General > Physical WLAN settings. > Client mode** and also from the following menu items in WEBconfig:

- **Setup > Interfaces > WLAN > Client-Modes > Cl.-Brg.-Support**
- **Setup > Interfaces > WLAN > Client-Modes > Tx-Limit**
- **Setup > Interfaces > WLAN > Client-Modes > Rx-Limit**

Changes to WLCs


The explanations added for a stand-alone AP to the changes in LANconfig also apply in the same manner to a WLC under **WLAN Controller > Profiles > Logical WLAN networks**.

7.2.1 Additions to the Setup menu

Cl.-Brg.-Support

While the address adaption can only make the MAC address of just one connected device visible for the access point, client-bridge support enables all MAC addresses of the stations in the LAN behind the client stations to be transmitted transparently to the access point.

In this operation mode, not three MAC addresses are taken (in this example for server, access point and client station) as is normal for client mode, but four addresses as with point-to-point connections (additionally the MAC address of the station in the client station's LAN). The fully transparent connection of a LAN to the client station allows targeted transmission of data packets in the WLAN and hence functions such as TFTP downloads, which are initiated via broadcast.

 The client-bridge mode can only be used between two LANCOM devices.

SNMP ID:

2.23.20.1.11

Telnet path:

Setup > Interfaces > WLAN > Network

Possible values:**Yes**

Activates client-bridge support for this logical WLAN.

No

Deactivates client-bridge support for this logical WLAN.

Exclusive

Only accepts clients that also support the client-bridge mode.

Default:

No

Tx limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID.

SNMP ID:

2.23.20.1.20

Telnet path:

Setup > Interfaces > WLAN

Possible values:

0 ... 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

Rx limit

With this setting, you define the overall bandwidth that is available for reception within this SSID.

SNMP ID:

2.23.20.1.21

Telnet path:

Setup > Interfaces > WLAN

Possible values:

0 ... 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

Tx limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID.

SNMP ID:

2.37.1.1.44

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

0 ... 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

Rx limit

With this setting, you define the overall bandwidth that is available for reception within this SSID.

SNMP ID:

2.37.1.1.45

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

0 ... 4294967295 kbps

Special values:

0

This value disables the limit.

Default:

0

7.3 Separation of P2P and WLAN/SSID configuration


As of LCOS 9.00, the transmission and encryption settings for P2P connections can be configured separately from the settings for the first logical WLAN network of the corresponding physical WLAN interface. P2P devices no longer use a configured SSID as an administrative network for connection establishment and for availability checks ("Alive") of a point-to-point partner. Instead, they now use the fixed SSID ***** P2P INFO *****.

This feature, among others, forms the basis for the structure of *AutoWDS networks*.

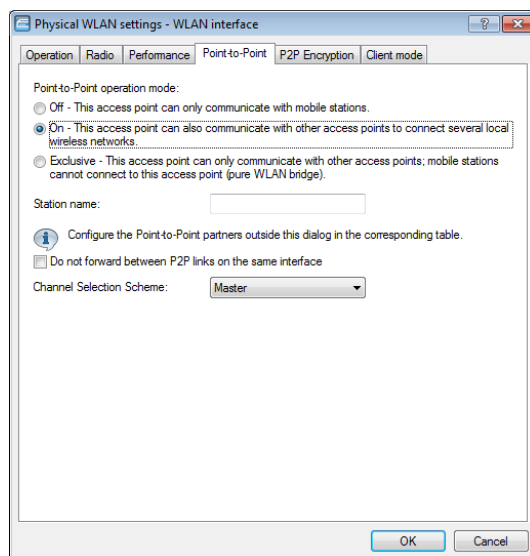
7.3.1 Configuration of P2P connections

In the configuration of point-to-point (P2P) connections, enter the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names of the remote sites. The configuration can be done in LANconfig either by using the Setup wizard **Configure WLAN** or manually using the configuration dialog.

The following steps show you how you create an encrypted or unencrypted P2P basic configuration.

 Along with a P2P connection, each of the APs automatically operates an SSID ***** P2P INFO *****. This SSID works purely as an administrative network for establishing the connection and for the availability check ("Alive") of a point-to-point partner. It is not possible for the WLAN clients to connect to this network.

1. Open the configuration dialog for the device that is to operate as the P2P master or P2P slave, and navigate to the page **Wireless LAN > General > Physical WLAN settings**.
2. Select the WLAN interface which you want to use explicitly for the P2P connection and move to the tab **Point-to-Point**.



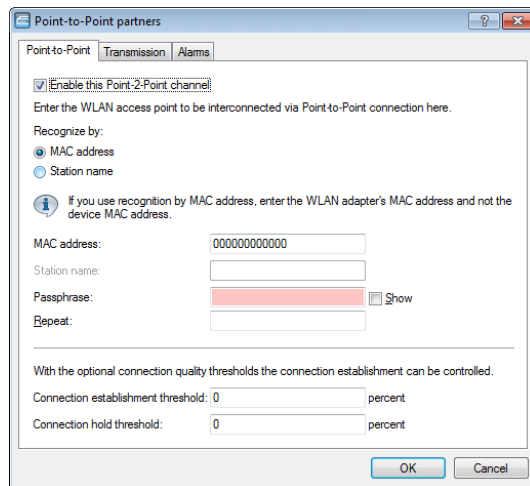
3. Enable the desired **Point-to-point operation mode**, such as **On**.
4. Set the **Channel selection scheme** to **Master** or **Slave**.
5. Optional: If the remote site should identify the physical interface by an alias and not the MAC address, then enter a corresponding descriptor into the field **Station name**, for example **P2P_MASTER** or **P2P_SLAVE**.
6. Optional: Adjust the settings on the tab **P2P encryption** for the IEEE 802.11i encryption of the P2P connection, if necessary.

IEEE 802.11i can attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the LANCOM Enhance Passphrase Security (LEPS).

The setting options are practically identical with those of the physical WLAN interfaces, . By default, P2P encryption is enabled and filled-out with meaningful values.

- i** In LCOS versions prior to 9.00, the settings for encryption are tied to the settings for the first logical WLAN network on the corresponding physical WLAN interface (i.e. WLAN-1 if you are using the first WLAN module for the P2P connection, WLAN-2 if you are using the second WLAN module for an access point with two WLAN modules). In this case, you find the settings under **Wireless LAN > 802.11i/WEP > WPA or private WEP settings**.

7. Close the dialog with **OK** and under **Point-to-Point partners** on the same page of the configuration dialog select a logical P2P connection, such as **P2P-1-1**.



8. Enable the selected P2P channel on the **Point-to-Point** tab and specify whether the device identifies the remote station using a **MAC address** or a **Station name**. Here you then enter either the MAC address of the physical WLAN interface which the remote station uses for the P2P connection, or its station name accordingly. You will find the WLAN MAC address on a sticker located under each of the antenna connectors on the housing of the device. Only use the string that is marked as the "WLAN-MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.

Alternatively, you will also find the MAC address in the status menu under **WLAN > Interfaces > MAC-Address**.

9. In **Passphrase**, enter a shared secret of at least 8 characters (recommended: 32 characters), which is used to additionally encrypt the P2P connection. The P2P encryption must be enabled for this (see above). When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.
10. Optional: Move to the **Transmission** tab to enter the limits and settings for packet transmission.

The setting options are practically identical with those of the logical WLAN networks . By default, all parameters are adjusted for optimization and automatic operation.

11. Close the dialog with **OK** and save the configuration to your device.
12. You continue by performing the corresponding configuration steps for the remote station (slave or master).

7.3.2 Additions to the Setup menu

Interpoint transmission

This table contains the transmission settings for the individual P2P links.

SNMP ID:

2.23.20.19

Telnet path:

Setup > Interfaces > WLAN

Ifc

Name of the logical P2P interface which you selected.

SNMP ID:

2.23.20.19.1

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Select from the available P2P links.

Packet size

Select the maximum size of data packets on a P2P link.

Smaller data packets cause fewer transmission errors than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load. Increase the factory value only if your wireless network is largely free from interference and very few transmission errors occur. Reduce the value to reduce the occurrence of transmission errors.

SNMP ID:

2.23.20.19.2

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

600 ... 2347

Default:

1600

Min-Tx-Rate

Specify the minimum transmission rate in the direction of transmission.

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients (Auto). The access point adjusts the transmission speeds to the reception conditions. You also have the option of preventing dynamic speed adjustment by entering a fixed transmission speed.

SNMP ID:

2.23.20.19.3

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

Max-Tx-Rate

Specify the maximum transmission rate in the direction of transmission.

Normally the access point negotiates the data transmission speeds continuously and dynamically with the connected WLAN clients (Auto). The access point adjusts the transmission speeds to the reception conditions. You also have the option of preventing dynamic speed adjustment by entering a fixed transmission speed.

SNMP ID:

2.23.20.19.9

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M

Default:

Auto

EAPOL-Rate

Set the data rate for EAPOL transmission.

WLAN clients use EAP over LAN (EAPOL) to login to the access point by WPA and/or 802.1x. With this method, the EAP packets used for exchanging authentication information are encapsulated within Ethernet frames, which in turn facilitates EAP communication over a Layer-2 connection.

In some cases, it makes sense to select a lower data rate for the transmission of the EAPOL packets than for payload data. For example, in the case of mobile WLAN clients, high data rates can cause the loss of EAPOL packets, which in turn leads to considerable delays in client association. This procedure can be stabilized by selecting specific data rates for EAPOL.

SNMP ID:

2.23.20.19.19

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:**Like-Data**

In this setting, the device transmits the EAPOL data at the same rate as payload data.

1M
2M
5.5M
11M
6M
9M
12M
18M
24M
36M
48M
54M
HT-1-6.5M
HT-1-13M
HT-1-19.5M
HT-1-26M
HT-1-39M
HT-1-52M
HT-1-58.5M
HT-1-65M
HT-2-13M
HT-2-26M
HT-2-39M
HT-2-52M
HT-2-78M
HT-2-104M
HT-2-117M
HT-2-130M

Default:

Like-Data

Soft retries

Enter the number of transmission attempts that the device tries if the hardware cannot send a data packet. The total number of transmission attempts results from the calculation $(\text{Soft-Retries} + 1) * \text{Hard-Retries}$.

The advantage of soft retries over hard retries is that, owing to the rate adaptation algorithm, the next set of hard retries immediately starts at a lower rate.

SNMP ID:

2.23.20.19.11

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

0 ... 255

Default:

10

Hard retries

Enter the number of transmission attempts that the device attempts before the hardware reports a Tx error. The smaller the value you choose, the shorter is the time that an unsendable packet will block the transmitter. If the hardware cannot send a data packet, you have the option to continue the attempts on the software side. For more information, see the parameter **Soft-Retries**.

SNMP ID:

2.23.20.19.12

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

0 ... 255

Default:

10

11b-Preamble

Specify whether your device uses a long preamble in 802.11b mode.

Normally every WLAN client (in this case the P2P slave) independently negotiates the necessary length of the preamble for communication with the base station (in this case the P2P master). However, in some rare cases it is necessary to ignore this handshake process and use the long WLAN preamble, although this is less advantageous.

Only enable the long WLAN preamble if it precisely resolves your wireless problems.

SNMP ID:

2.23.20.19.7

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Transmission****Possible values:****Auto**

The P2P slave automatically negotiates the length of the preamble (short/long) required to communicate with the P2P-master.

Long

The P2P slave does not negotiate and always uses a long preamble.

Default:

Auto

Min. HT MCS

MCS (Modulation Coding Scheme) is used for automatic speed adjustment and defines a series of variables in the 802.11n standard, which, for example, specifies the number of spatial streams, the modulation, and data transfer rate of each data stream.

In the factory settings, the station automatically selects the optimal MCS for the corresponding stream according to the current channel conditions. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You still have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

SNMP ID:

2.23.20.19.16

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

Max. HT MCS

MCS (Modulation Coding Scheme) is used for automatic speed adjustment and defines a series of variables in the 802.11n standard, which, for example, specifies the number of spatial streams, the modulation, and data transfer rate of each data stream.

In the factory settings, the station automatically selects the optimal MCS for the corresponding stream according to the current channel conditions. If interference arises during operation and the channel conditions change, for example due to movement of the transmitter or signal deterioration, the MCS is dynamically adjusted to suit the new conditions.

You still have the option of setting the MCS to a constant value. This may facilitate testing, or it may be useful in particularly dynamic environments to avoid unnecessary parameterizing where an optimal value simply cannot be expected.

SNMP ID:

2.23.20.19.17

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
MCS-0/8
MCS-1/9
MCS-2/10
MCS-3/11
MCS-4/12
MCS-5/13
MCS-6/14
MCS-7/15

Default:

Auto

Use STBC

Here you enable Space Time Block Coding (STBC).

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

 This parameter cannot be set to **Yes** if the WLAN chipset does not support STBC.

SNMP ID:

2.23.20.19.23

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

No
Yes

Default:

Yes

Use LDPC

Enable Low Density Parity Check (LDPC) here.

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

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. Therefore, LDPC encoding already provides a higher data rate due to having a better ratio of usage to checksum data.



If the WLAN chipset does not support STBC, you cannot set this value to **Yes**.

SNMP ID:

2.23.20.19.24

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

No
Yes

Default:

Yes

Short guard interval

Enable or disable the short guard interval.

In rough terms, the guard interval is used to minimize the disturbance from intersymbol interference (ISI) when operating with multiplexing (OFDM). The option reduces the transmission pause between two signals from 0.8 μ s (default) to 0.4 μ s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

SNMP ID:

2.23.20.19.13

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:**Auto**

The device activates the short guard interval in automatic mode, provided that the remote station supports this.

No

Disables the short guard interval.

Default:

Auto

Min.-Spatial-Streams

Enter the minimum number of allowed spatial streams.

In principle, the spatial streams add a 3rd dimension—space—to the existing frequency-time matrix. An array of multiple antennas provides the receiver with spatial information that the device can use for spatial multiplexing, a technique that increases transmission rates. This allows parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This improves the performance of the entire radio system.

In the factory settings, the device automatically has the spatial streams turned on in order to optimize use of the radio system. Alternatively you have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

SNMP ID:

2.23.20.19.18

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
One
Two
Three

Default:

Auto

Max. spatial streams

Enter the maximum number of allowed spatial streams.

In principle, the spatial streams add a 3rd dimension—space—to the existing frequency-time matrix. An array of multiple antennas provides the receiver with spatial information that the device can use for spatial multiplexing, a technique that increases transmission rates. This allows parallel transmission of multiple data streams over a single radio channel. Multiple transmitter and receiver antennas can be operated at the same time. This improves the performance of the entire radio system.

In the factory settings, the device automatically has the spatial streams turned on in order to optimize use of the radio system. Alternatively you have the option of limiting the spatial streams to one or two to reduce the load on the radio system.

SNMP ID:

2.23.20.19.14

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

Auto
One
Two
Three

Default:

Auto

Send aggregates

With this setting you configure the transmission of aggregated data packets. Frame aggregation is an official standard and, according to the 802.11n standard, it is intended to be vendor-independent. This is similar to the well-known burst mode.

For frame aggregation, the device combines multiple data packets (frames) to a larger packet—by increasing the length of the WLAN frame—and sends them together. The method shortens the waiting time between data packets and also reduces the overhead, so increasing the data throughput.

However, with increased frame length, the probability increases that the device must resend the packets, for example, due to radio interference. Other stations must also wait for a free channel and collect their data packets until they have multiple packets that they can send at one time.

Frame aggregation is enabled in the factory settings. This option makes sense if you want to increase the throughput for your device and others on this medium are not important. Frame aggregation is not suitable when working with mobile receivers or real-time data transmissions such as voice over IP.

SNMP ID:

2.23.20.19.15

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

No
Yes

Default:

Yes

Receive-Aggregates

With this setting you configure the reception of aggregated data packets. Frame aggregation is an official standard and, according to the 802.11n standard, it is intended to be vendor-independent. This is similar to the well-known burst mode.

For frame aggregation, the device combines multiple data packets (frames) to a larger packet—by increasing the length of the WLAN frame—and sends them together. The method shortens the waiting time between data packets and also reduces the overhead, so increasing the data throughput.

However, with increased frame length, the probability increases that the device must resend the packets, for example, due to radio interference. Other stations must also wait for a free channel and collect their data packets until they have multiple packets that they can send at one time.

Frame aggregation is enabled in the factory settings. This option makes sense if you want to increase the throughput for your device and others on this medium are not important. Frame aggregation is not suitable when working with mobile receivers or real-time data transmissions such as voice over IP.

SNMP ID:

2.23.20.19.22

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Transmission****Possible values:****No**
Yes**Default:**

Yes

Max.-Aggr.-Packet-Count

Using this parameter, you define the maximum number of packets the device may combine into one aggregate. Aggregation in IEEE 802.11n WLAN transmissions combines multiple data packets into one large packet, so reducing the overhead and speeding up the transmission.

SNMP ID:

2.23.20.19.20

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

0 ... 11/16/24 (device dependent)

Special values:**0**

The device automatically uses the highest value allowed on the hardware side.

Default:

0

RTS threshold

Use this field to define the RTS threshold. If the size of the RTS packets for transmission exceeds this value, the device uses the RTS/CTS protocol in order to prevent the increased probability of collisions and the associated "hidden station" phenomena.

Since the RTS packets are generally very short and the use of RTS/CTS increases the overhead, using this method only pays off if you are using longer data packets where collisions are likely. This value has to be determined in a trial in the respective environment.



The RTS/CTS threshold should also be set in the WLAN clients, in as far as the driver or the operating system allow this.

SNMP ID:

2.23.20.19.6

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

60 ... 2347

Default:

2347

Min.-Frag.-Length

Using this input field you define the minimum length of packet fragments, below which the device rejects data packet fragments.

SNMP ID:

2.23.20.19.10

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Transmission

Possible values:

0 ... 65535

Special values:

0, 1

The device allows for packet fragments of any length.

Default:

16

Interpoint-Encryption

This table contains the encryption settings of the physical WLAN interface for P2P links.

SNMP ID:

2.23.20.20

Telnet path:**Setup > Interfaces > WLAN****Ifc**

Name of the physical WLAN interface

SNMP ID:

2.23.20.20.1

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Encryption**

Enables or disables the WPA/WEK encryption for P2P connections over the respective interface.

SNMP ID:

2.23.20.20.2

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Possible values:****No**
Yes**Default:**

Yes

Default-Key

WEK keys with which the device encrypts the packets sent over this interface.

SNMP ID:

2.23.20.20.3

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption**

Possible values:

0 ... 9

Default:

1

Method

Selects the encryption method or, for WEP, the key length which the device uses for the encryption of P2P data packets.



Please note that not every client (or their hardware) supports every encryption method.

SNMP ID:

2.23.20.20.4

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Possible values:****802.11i-WPA-PSK****WEP-128-bit****WEP-104-bit****WEP 40-bit****Default:**

802.11i-WPA-PSK

WPA version

WPA version that the device offers a client for WPA encryption.

SNMP ID:

2.23.20.20.9

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Possible values:****WPA1****WPA2****WPA1/2****Default:**

WPA1/2

WPA1 session key types

Select the method or methods that the device offers the remote station for generating the WPA session or group key for WPA1. The device can provide the Temporal Key Integrity Protocol (TKIP) method, the Advanced Encryption Standard (AES) method, or both.

SNMP ID:

2.23.20.20.12

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Encryption

Possible values:

TKIP
AES
TKIP/AES

Default:

TKIP

WPA2-Session-Key

Select the method or methods that the device offers the remote station for generating the WPA session or group key for WPA2. The device can provide the Temporal Key Integrity Protocol (TKIP) method, the Advanced Encryption Standard (AES) method, or both.

SNMP ID:

2.23.20.20.13

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Encryption

Possible values:

TKIP
AES
TKIP/AES

Default:

AES

WPA-Rekeying-Cycle

Specify the intervals at which the device repeats the WPA key handshake.

For WPA1/2, authentication on a network is performed with a pre-shared key (PSK), which is part of a 128-bit individual key. The device (as authenticator) generates this key with a 48-bit initial vector (IV), which makes it difficult for attackers

to calculate the WPA key. The repetition of the key that consists of the IV and WPA keys only occurs after 2^{48} data packets, which no WLAN will reach within a foreseeable time.

To prevent the (theoretical) repetition of the real key, the WPA allows for an automatic renegotiation of the key with the WLAN client (the supplicant) in regular intervals (rekeying). This prevents the repetition of the real key. By setting an individual cycle, you have the option of shortening the rekeying intervals.

SNMP ID:

2.23.20.20.11

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Possible values:**

0 ... 4294967295 Seconds

Special values:**0**

This value disables the preliminary negotiation of a new WPA key at the device. Rekeying can still be triggered by the supplicant.

Default:

0

WPA2-Key-Management

You can configure the WPA2 key management with this option.



Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients deny the connection if an option other than **Standard** is enabled.

SNMP ID:

2.23.20.20.19

Telnet path:**Setup > Interfaces > WLAN > Interpoint-Encryption****Possible values:****SHA256**

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Default:

Standard

7.4 Flexible WLAN capture format

As of LCOS 9.00, different formats are available for storing WLAN packet-capture data.

7.4.1 Additions to the Setup menu

Packet-Capture

This menu contains the settings for packet capturing.

SNMP ID:

2.12.86

Telnet path:

Setup > WLAN

WLAN-Capture-Format

With this setting you specify the format used by the packet capture function to store the WLAN-specific information in the capture file.

The selection of the appropriate capture format depends on the transmission standard in your WLAN network and the scope of the information that you would like to capture. The IEEE 802.11 standard with its numerous extensions has grown over many years. However, the capture formats that were developed in parallel are not flexible enough to cater optimally for every extension (particularly 802.11n). For this reason there is no universal capture format which is equally suitable for all standards. However, there are recommendations that cover a wide spectrum of standards: [Radiotap](#) and [PPI](#).

SNMP ID:

2.12.86.1

Telnet path:

Setup > WLAN > Packet-Capture

Possible values:

Radiotap

Uses the radiotap header. Radiotap is a widely accepted format on Linux and BSD WLAN drivers which enables the creation of compact captures due to its flexible structure. With radiotap you can record a large amount of WLAN-specific information with a high compression rate. This also applies to data packets from 802.11n compliant connections. Limitations only arise when recording antenna-specific RSSI and signal strength as well as aggregations (A-MPDU). If you do not require detailed WLAN-specific information for this, choose the PPI format instead.

AVS

Uses the AVS header. The AVS header is a newer development of the PRISM header, and is used by LCOS as the standard header up to version 8.60. However, since AVS is also unable to process information from 802.11n compliant connections, you should choose the more powerful radiotap header.

PPI

Uses the proprietary Wireshark PPI header. Use this setting if you want to analyze the capture file with Wireshark. PPI offers similar functions as radiotap but can also bypass its limitations on the recording of information about 802.11n compliant connections. A disadvantage to radiotap is, however, the weaker compression and less detailed header structure.

PRISM

Uses the classic PRISM header. Only use this setting if you want to analyze the capture file with a program which does not support any of the other formats. PRISM is not suitable for recording information from 802.11n compliant connections. In the meantime this is considered obsolete and should no longer be used.

Plain

Disables all headers. Use this setting if you are only interested in the packet data itself.

Default:

Radiotap

7.5 Band steering with delayed scan at 2.4 GHz

As of LCOS version 9.00 you can delay the band steering to the 2.4-GHz band under **Wireless LAN > Band steering**.

Using band steering, WLAN clients are directed to a preferred frequency band. For this, the same SSID has to be active on both WLAN modules.

☐ Band steering activated

Preferred frequency band: 5 GHz

Probe request ageout time: 120 seconds

Initial blocking period: 10 seconds

Initial block time

If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a WLAN client to a preferred 5-GHz band. Instead, the 2.4-GHz radio module would answer the client request and forward it to the 2.4-GHz band.

By setting an initial block time, the radio module that is configured to 2.4-GHz only responds to client requests after the specified delay. The default value is 10 seconds.

The delayed response to the 2.4GHz probes causes WLAN clients, which would otherwise expect to find an access point in the 2.4GHz band, to scan again in the 5GHz band.



Registration of a purely 2.4-GHz WLAN client also occurs after this delay time. If no 5-GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

7.5.1 Additions to the Setup menu

Initial block time

If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a

WLAN client to a preferred 5-GHz band. Instead, the 2.4-GHz radio module would respond to the client request and direct it to the 2.4-GHz band.

By entering an initial block time, the access point's 2.4-GHz radio module only starts after the delay set here.



Registration of a purely 2.4-GHz WLAN client also occurs after this delay time. If no 5-GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

SNMP ID:

2.12.87.5

Telnet path:

Setup > WLAN > Client-Steering

Possible values:

Max. 10 characters from 0123456789

Special values:

0

This value disables the delay.

Default:

10

7.6 Advanced wireless LAN traces

As of LCOS version 9.00, management frame classes can be separately selected for a WLAN data trace. The settings can be found in WEBconfig under **Setup > WLAN**. The menu item **Setup > WLAN > Trace-Beacons** is no longer available as of LCOS 9.00.

Trace-Mgmt-Packets

With this selection it is possible to set which type of management frames should automatically appear in the WLAN-DATA trace

Possible values:

Association: (Re)Association Request/Response, Disassociate

Authentication: Authentication, Deauthentication

Probes: Probe Request, Probe Response

Action

Beacon

Other: all other management frame types

Default:

Association

Authentication

Probes

Action

Other

7.6.1 Additions to the Setup menu

Trace-Mgmt-Packets

With this selection it is possible to set which type of management frames should automatically appear in the WLAN-DATA trace

SNMP ID:

2.12.124

Telnet path:

Setup > WLAN

Possible values:

Association

(Re)association request/response

Disassociate

Authentication

Authentication

Deauthentication

Probes

Probe request

Probe response

Action

Beacon

Other

All other management frame types

Default:

Association

Authentication

Probes

Action

Other

Trace-Data-Packets

With this selection it is possible to set which type of data frames should automatically appear in the WLAN-DATA trace

SNMP ID:

2.12.125

Telnet path:**Setup > WLAN****Possible values:****Normal**

All normal data packets

NULL

All empty data packets

Other

All other data packets

7.7 Fast roaming as per IEEE 802.11r

As of LCOS 9.00, access points support fast roaming according to the standard IEEE 802.11r.

7.7.1 Fast roaming

By operating authentication according to the IEEE 802.1X standard and key management according to the IEEE 802.11i standard, modern WLAN installations offer a high degree of security and confidentiality for the transmitted data. However, these standards require transmission of additional data packets during the connection negotiation as well as additional computing power on the client and server.

Currently, WLAN devices have hardware accelerators, which perform the real-time encryption and decryption of payload data during a connection without noticeable delays or conspicuous network loading. In the meantime, because sufficient computing power is available, the creation of keys on the client side no longer causes any noticeable delays.

The delays when connecting via EAP/802.1X or WPA are therefore mostly related to the time that the client and server require to negotiate the security protocol during login.

The original IEEE 802.11 only required up to six data packets to establish a data connection between a WLAN client and an access point. The standard extension IEEE 802.11i improved on weak points of WEP encryption; however, depending on the authentication method, it substantially increased the length of the login process.

This extra time for the WLAN client to login to the access point is not a problem for non-time-critical applications. However, for smooth, loss-free roaming of a WLAN client from one access point to the next (as required, for example, for Voice-over-IP applications or in industrial, real-time environments), a delay of more than 50 ms is not acceptable.

Methods such as pair-wise master key caching (PMK caching), pre-authentication, opportunistic key caching (OKC) and the use of central WLAN controllers for key management improve the time for the key negotiation between the WLAN client and access point during login. Despite this, the comparatively long time required for key negotiation between the WLAN client and the access point has still not been reduced to a viable extent.

Along with the improved encryption protocols, IEEE 802.11e makes it possible to reserve additional bandwidth with the access point. This allows the WLAN client to prevent interruptions, for example for VoIP connections at times of high network loads at the access point. For roaming from one access point to the next, the WLAN client must again reserve this additional bandwidth on the new access point. However, the additional management frames required for this considerably increase the login time.

The IEEE 802.11r standard provides a simplified authentication process for mobile WLAN clients to roam trouble-free from one access point to the next. The goal is to once again reduce the number of data packets for the login on the access point to the four to six packets known from 802.11.


Similar to opportunistic key caching (OKC), a centralized key management (preferably by a WLAN controller) supplies the access points connected to it with the credentials of the WLAN clients. In contrast to OKC, the WLAN client performing fast roaming can detect whether the access point supports 802.11r

Access points managed by the WLAN controller transmit the mobility domain information element (MDIE) to inform the WLAN clients about which "mobility group" the access point belongs to, among other things. Based on this information, the WLAN client detects whether it belongs to the same domain and can therefore authenticate without delay. This mobility domain is announced to a WLAN client the first time it authenticates at an access point.

The domain identifier and other special keys generated during the initial authentication and transmitted to all managed access points now reduce the stages of negotiation to the desired four to six steps when authenticating at a new access point.

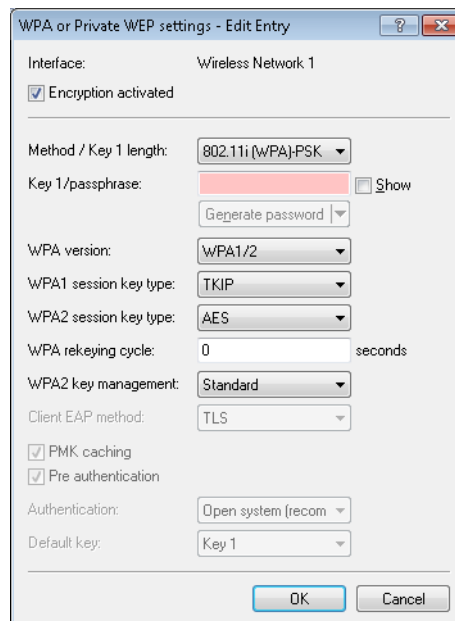
To avoid futile and thus time-wasting login attempts with expired PMKs, IEEE 802.11r provides additional information about the validity periods of keys. In this manner, the client negotiates a new PMK while connected to the current access point. This is also valid on the access point that the WLAN client wants to connect to next.

Additionally, IEEE 802.11r uses "resource requests" to reserve additional bandwidth on the new access point, so that there is no need to cause added delay by transferring unnecessary data packets during the IEEE 802.11e authentication.

 Older WLAN clients may have trouble establishing a connection to an SSID with enabled 802.11r. Therefore, it is advisable to use two SSIDs here: One SSID for older clients without 802.11r support and another SSID with enabled 802.11r for clients that support 802.11r.

Fast roaming is setup in LANconfig under **Wireless LAN > 802.11i/WEP > WPA or private WEP settings**.

7.7.2 Configuration



WPA2 key management

Here you specify which standard the WPA2 key management should follow. Possible values are:

- Standard: Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.
- SHA256: Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.
- Fast roaming: Enables fast roaming as per 802.11r

- Combinations of the three settings



Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than **Standard** is enabled.

7.7.3 Additions to the Status menu

Fast roaming

Indicates whether the wireless client uses fast roaming.

SNMP ID:

1.3.32.63

Telnet path:

Status > WLAN > Station-table

WPA2-Key-Management

Indicates which WPA2 key management the wireless client is using.

SNMP ID:

1.3.32.64

Telnet path:

Status > WLAN > Station-table

WPA2-Key-Management

Indicates which WPA2 key management is used by the P2P access point.

SNMP ID:

1.3.36.1.44

Telnet path:

Status > WLAN > Interpoints > Access-point-list

WPA2-Key-Management

Indicates which WPA2 key management is used by the access point in client mode.

SNMP ID:

1.3.43.51.40

Telnet path:

Status > WLAN > Client > Interfaces

7.7.4 Additions to the Setup menu

WPA2-Key-Management

You configure the WPA2 key management with this option.



Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients deny the connection if an option other than **Standard** is enabled.

SNMP ID:

2.23.20.3.19

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

Fast roaming

Enables Fast Roaming via 802.11r

SHA256

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Default:

Standard

WPA2-Key-Management

You can configure the WPA2 key management with this option.



Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients deny the connection if an option other than **Standard** is enabled.

SNMP ID:

2.23.20.20.19

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Encryption

Possible values:**SHA256**

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Default:

Standard

WPA2-Key-Management

You configure the WPA2 key management with this option.



Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients deny the connection if an option other than **Standard** is enabled.

SNMP ID:

2.37.1.1.41

Telnet path:

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

Possible values:**Fast roaming**

Enables Fast Roaming via 802.11r

SHA256

Enables key management according to the IEEE 802.11w standard with keys based on SHA-256.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Default:

Standard

7.8 WPA2 with AES as factory setting

As of LCOS 9.00, WPA2 encryption in LANconfig and LCOS uses the session key type AES by default.

7.9 WLAN protected management frames (PMF)

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

To enable protected management frames for a logical WLAN interface, in LANconfig you navigate to **Wireless LAN > 802.11i/WEPWPA or Private WEP settings**, open the configuration of the appropriate WLAN interface and click the appropriate option in the selection list **Encrypt mgmt. frames**.

WPA or Private WEP settings - Edit Entry

Interface: Wireless Network 1

☒ Encryption activated

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

Key 1/passphrase: XXXXXXXXXX ☐ Show

WPA version: WPA2

WPA1 session key type: TKIP

WPA2 session key type: AES

WPA rekeying cycle: 0 seconds

WPA2 key management: Standard

Client EAP method: TLS

☒ PMK caching

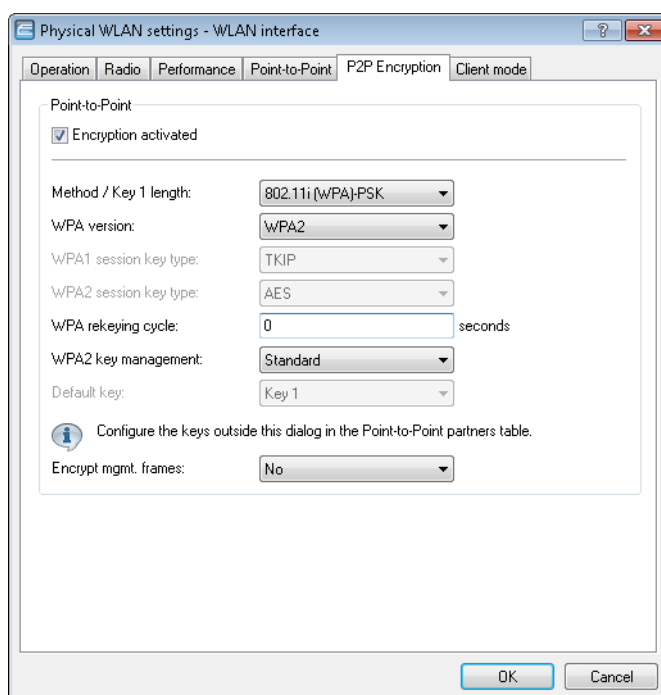
☒ Pre authentication

Authentication: Open system (recom)

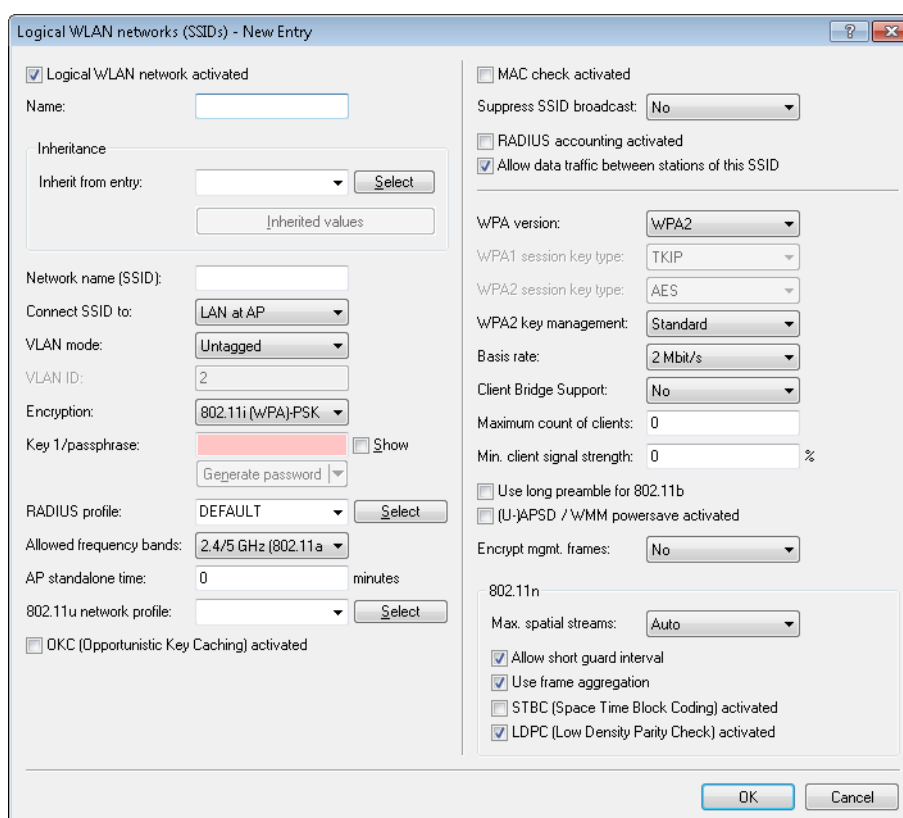
Default key: Key 1

Encrypt mgmt. frames: No

To encrypt the management frames for P2P connections between base stations, in LANconfig you navigate to **Wireless LAN > General**, click on **Physical WLAN settings** and click the appropriate option in the selection list **Encrypt mgmt. frames**.



To manage the encryption of management frames for a WLAN controller, in LANconfig you navigate to **WLAN Controller > Profiles**, click on **Logical WLAN networks (SSIDs)** and click the appropriate option in the selection list **Encrypt mgmt. frames**.



The following options are available in each of these configurations:

No

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

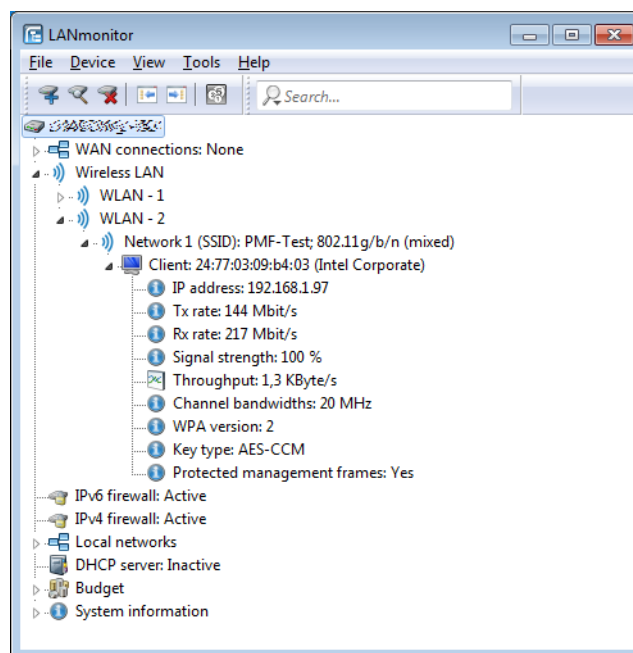
Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

LANmonitor displays information about WLAN management frame encryption below each client.



7.9.1 Additions to the Status menu

Prot.-Mgmt-Frames

Indicates whether the WLAN client has established a PMF-protected connection.

SNMP ID:

1.3.32.67

Telnet path:

Status > WLAN > Station-table

Possible values:

No
Yes

Prot.-Mgmt-Frames

Indicates whether the corresponding network supports PMF.

SNMP ID:

1.3.34.47

Telnet path:

Status > WLAN > Scan-Results

Possible values:

No
Yes
Optional

Prot.-Mgmt-Frames

Indicates whether PMF is enabled on the corresponding P2P link.

SNMP ID:

1.3.36.1.47

Telnet path:

Status > WLAN > Interpoints > Access-point-list

Possible values:

No
Yes

Key type

Shows the session key type for the P2P connection.

SNMP ID:

1.3.36.3.3

Telnet path:

Status > WLAN > Interpoints > Key-list

Possible values:

None
Unknown
WEP 40-bit
WEP-104-bit
WEP-128-bit
TKIP
AES-OCB
AES-CCM
BIP

The type "Broadcast Integrity Protection" indicates that the AP secures the management frames that are sent as broadcasts or multicasts to several clients.

RSC-MGMT

Shows the sequence counter of the last received encrypted management frame. This value is use for protection from replay.

SNMP ID:

1.3.36.3.24

Telnet path:

Status > WLAN > Interpoints > Key-list

Key type

Shows the session key type for the P2P connection.

SNMP ID:

1.3.41.3

Telnet path:

Status > WLAN > Group-encryption-keys

Possible values:

None
Unknown
WEP 40-bit
WEP-104-bit
WEP-128-bit
TKIP
AES-OCB
AES-CCM
BIP

The type "Broadcast Integrity Protection" indicates that the AP secures the management frames that are sent as broadcasts or multicasts to several clients.

RSC-MGMT

Shows the sequence counter of the last received encrypted management frame. This value is use for protection from replay.

SNMP ID:

1.3.41.24

Telnet path:

Status > WLAN > Group-encryption-keys

RSC-MGMT

Shows the sequence counter of the last received encrypted management frame. This value is use for protection from replay.

SNMP ID:

1.3.42.23

Telnet path:

Status > WLAN > Channel-scan-results

Prot.-Mgmt-Frames

Indicates whether the corresponding WLAN interface in client mode has established a PMF-protected connection.

SNMP ID:

1.3.43.51.41

Telnet path:

Status > WLAN > Client > Interfaces

Possible values:

No
Yes

Prot.-Mgmt-Frames

Indicates whether the corresponding network supports PMF.

SNMP ID:

1.3.44.47

Telnet path:

Status > WLAN > Competing-networks

Possible values:

No
Yes
Optional

Key type

Shows the session key type for the P2P connection.

SNMP ID:

1.3.47.3

Telnet path:

Status > WLAN > Pairwise-keys

Possible values:

None
Unknown
WEP 40-bit
WEP-104-bit
WEP-128-bit
TKIP
AES-OCB
AES-CCM
BIP

The type "Broadcast Integrity Protection" indicates that the AP secures the management frames that are sent as broadcasts or multicasts to several clients.

RSC-MGMT

Shows the sequence counter of the last received encrypted management frame. This value is use for protection from replay.

SNMP ID:

1.3.47.24

Telnet path:

Status > WLAN > Pairwise-keys

Prot.-Mgmt-Frames

Indicates whether the corresponding WLAN interface supports PMF.

SNMP ID:

1.3.55.41

Telnet path:**Status > WLAN > Competing-networks****Possible values:****No****Yes**

7.9.2 Additions to the Setup menu

Prot.-Mgmt-Frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

SNMP ID:

2.23.20.3.14

Telnet path:**Setup > Interfaces > WLAN > Encryption****Possible values:****No**

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

Prot.-Mgmt-Frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an

access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

SNMP ID:

2.23.20.20.14

Telnet path:

Setup > Interfaces > WLAN > Interpoint-Encryption

Possible values:**No**

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

Prot.-Mgmt-Frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

Here you can specify whether the corresponding WLAN interface supports protected management frames (PMF) as per IEEE 802.11w.

SNMP ID:

2.37.1.1.43

Telnet path:

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

Possible values:**No**

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

Default:

No

7.10 Redundant connections using PRP

Applications that are sensitive to connection failures require uninterrupted communications. Examples are to be found in automation, transport and mobile applications.

As of LCOS 9.00, you have the option of operating redundant connections in your WLAN by means of the parallel redundancy protocol (PRP). Redundant point-to-point links offer you a high level of failover reliability.

PRP achieves high failover reliability by sending twin packets over 2 independent WLANs. While 1 WLAN is active, PRP transports data packets.



7.10.1 Basic function

PRP devices act as the sender and receiver of PRP packets, whereby PRP devices are capable of assuming both roles.

The sender operates as follows:

1. It duplicates packets to produce twin packets, and sends them over 2 independent (W)LANs.
2. Each packet is given a redundancy control trailer (RCT).

The RCT provides the following information for the recipient:

- It identifies the packet as a PRP packet.
- It contains a sequence ID.
- It shows which (W)LAN the packet arrived from.
- It contains the packet size.

The sequence ID is a consecutive incremented number. The sequence ID together with the the source MAC address allow the receiver to detect duplicate packets. Duplicate detection causes the packet arriving later to be discarded.

The receiver operates as follows:

- It reads the RCT.
- It forwards the first of the duplicated packets without its RCT.
- Through duplicate detection, the receiver discards the packet that arrives later.

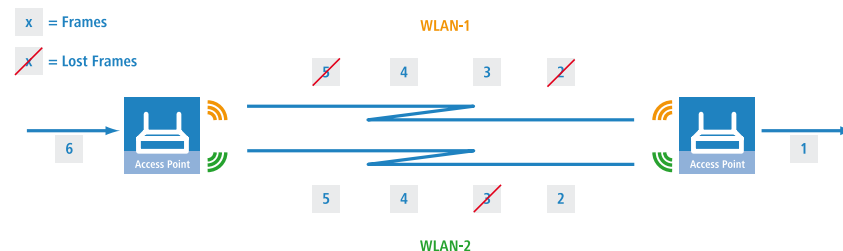
7.10.2 Advantages of WLAN PRP

The functions of PRP offer you significant advantages for your WLAN. In practice, PRP improves the 3 most important quality indicators for a network: Jitter, latency and packet loss.

With PRP, the receivers will accept and forward the first copy of the PRP packets and discard those that arrive later. Because the devices always forward the first incoming packet, latency is reduced. In practice, significant improvements were seen to average and maximum jitter.

Like Ethernet, WLAN is designed to be a shared medium. Within a single WLAN connection, the devices hold back packets if the medium is busy. Because the devices with PRP transport the data via 2 different WLANs, in effect 2 media are available thanks to frequency division.

Because the devices send each packet twice, PRP can to some extent compensate for unsystematic packet loss. As long as the receiver receives one of the packets, then communication was successful. Under certain circumstances there is no need to retransmit lost packets, which also positively affects jitter.



7.10.3 Implementation of PRP in the access points

Any access point (AP) with at least 3 interfaces can be used to setup a PRP network. The AP handles all of the functions necessary for establishing a PRP network.

The devices offer the following options:

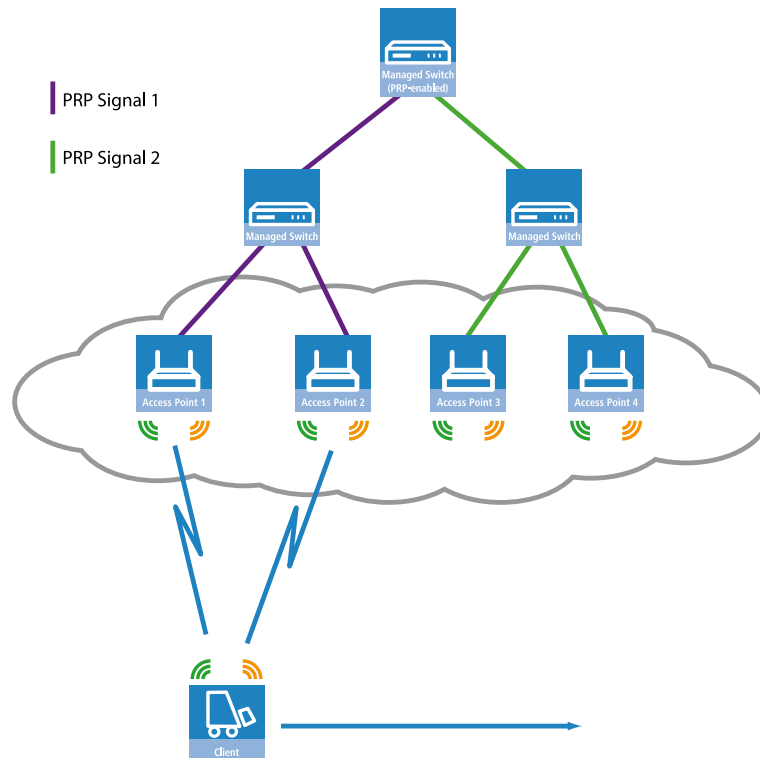
1. PRP networks can be implemented via wireless interfaces
2. Each device can implement up to 2 PRP networks
3. In addition to a PRP network, connect additional clients to an AP
4. Activate dual roaming so that the 2 WLAN modules can roam asynchronously with PRP.
5. Comprehensive diagnostic options

7.10.4 Dual roaming

A device with just 1 WLAN module will lose its connection to the infrastructure in a handover scenario.

However, a device with 2 WLAN modules can use PRP to reduce interruptions if the corresponding LANconfig setting prevents both WLAN modules from roaming at the same time. This mode is called dual roaming.

A practical example is a client moving past an access point. Due to the design of the network, one WLAN module stays connected and receives PRP packets, while the other WLAN module can already associate with the next AP.



A concrete example would be for materials management, and for the real-time monitoring of inventory flow in particular.

Another example is the railway. An AP in a train connects to the trackside APs throughout the journey.

In addition, you can specify the block time in LANconfig. The block time specifies the minimum time that passes before the different WLAN modules of the same device can perform roaming operations.

7.10.5 Diagnostic options

Recipients of PRP packets discard duplicates during normal operation and remove the RCT from packets that they pass on to their bundled output port.

LCOS provides you the following options to assist you in network diagnostics:

1. Forwarding packet duplicates without RCT
2. Forwarding single packets with RCT
3. Forwarding packet duplicates with RCT


LCOS also features the following trace options:

1. trace # PRP-DATA
2. trace # PRP-NODES

PRP-DATA contains information about packets that are sent and received. Information included: Name of the interface group transporting the packet: Direction of transport of the packet (RX|TX): Trailer sequence number: MAC address of the partner device: Interface within the PRP group (A|B) transporting the packet: Treatment of the packet (accept|discard)

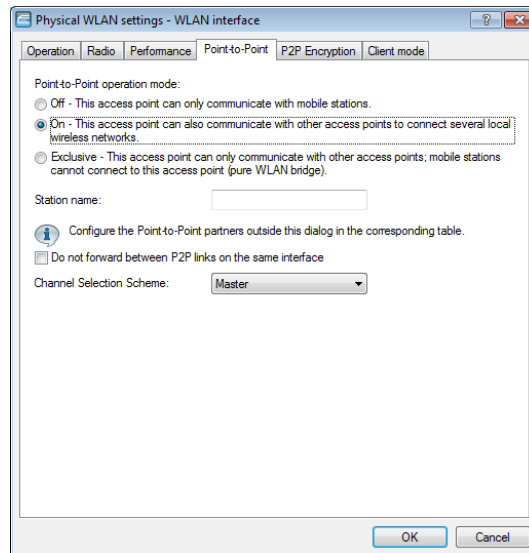
PRP-NODES contain the following information: Removed new address (proxy) node table address from the table (proxy) node, node type an address has changed.

7.10.6 Tutorial: Setting up a PRP connection over a point-to-point network (P2P)


 The following steps must be conducted for both P2P partners.

Proceed as follows to set up a P2P connection between two PRP-enabled APs:

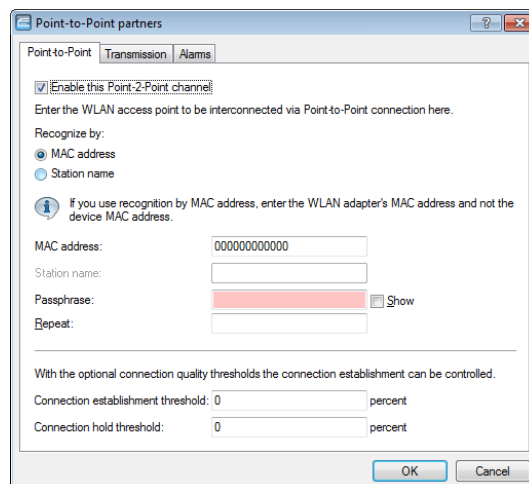
1. Under **Wireless LAN > General > Physical WLAN settings**, go to the **Operation** tab for each physical WLAN interface (WLAN interface 1, WLAN interface 2) and, on the **Point-to-point** tab, enable the **Point-2-Point operation mode**.



2. In the field **Station name**, give each of the physical WLAN interfaces a name that is unique on the WLAN. If the P2P partner can or should identify this interface using the MAC address, leave this field blank.

 In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

3. Under **Wireless LAN > General > Point-to-point partners**, enable the point-to-point channels "P2P-1-1" and "P2P-2-1" and specify the interface identifier for each point-to-point partner (**MAC address** or **Station name**).



Specify either the MAC address or the station name of the corresponding WLAN interface of the P2P partner. You set these station names in the previous step.

4. Open the PRP configuration under **Interfaces > LAN** with a click on **PRP interfaces**.

Network adapter

MAC address:

Ethernet switch settings

This is where you can program further settings for each Ethernet interface.

Ethernet ports

LAN bridge settings

Select, how to connect the different LAN, wireless LAN and tunnel interfaces:

☒ Connect by using a bridge (default)

☐ Connect by using the router (isolated mode)

Bridge parameters for each LAN port can be configured separately in this table.

Port table...

LAN interface bundling

The Parallel Redundancy Protocol (PRP) enables the transmission on two bundled interfaces. For this purpose outgoing packets are duplicated and transmitted on each of both interfaces. On reception, the duplicates are detected and dropped again. At the expense of bandwidth you get a lower packet error rate and reduced latency.

PRP interfaces

5. Enable the PRP interfaces and set the interfaces that the AP uses for bundling.

PRP interfaces - PRP-1

General Advanced

☒ Entry active

Protocol: Parallel Redundancy Protocol (PRP)

MAC address:

Interface A: P2P-1-1

Interface B: P2P-2-1

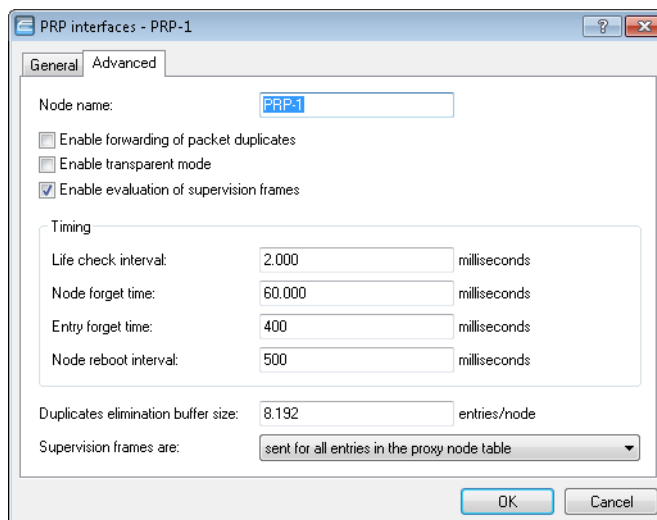
OK Cancel

Here you select the previously activated point-to-point interfaces "P2P-1-1" and "P2P-2-1".



In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

6. You can accept the advanced settings from the default configuration by clicking on **OK**.



This completes the setup of a PRP connection over a point-to-point network.

7.10.7 Tutorial: Roaming with a dual-radio client and PRP

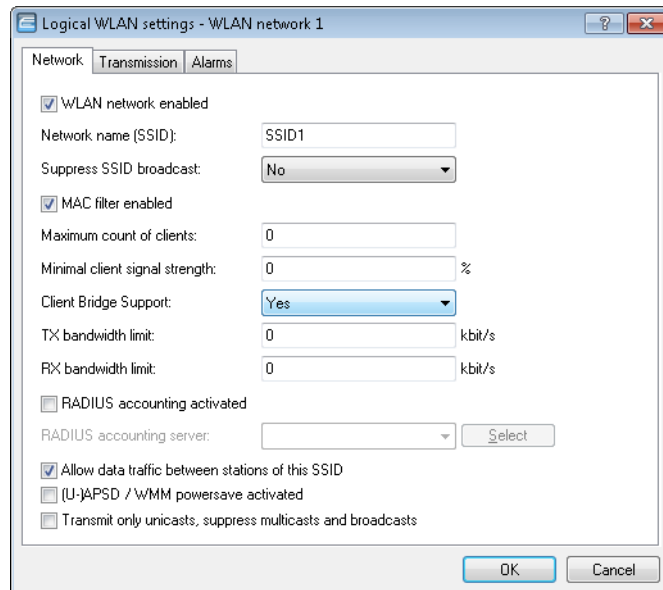
A common way to increase the resilience of a WLAN infrastructure is to operate the various APs in different frequency bands. One way to implement this is for the physical WLAN interfaces of the APs to operate SSID-1 on the 2.4-GHz band and SSID-2 on the 5-GHz band, for example. A PRP-capable dual-radio client moving from the radio cell of one physical WLAN interface to a neighboring cell of the same infrastructure can experience uninterrupted cell switching thanks to PRP.

To do this, the dual-radio client using PRP initially connects its physical WLAN interface WLAN-1 to SSID-1 and WLAN-2 to SSID-2. If the reception for SSID-1 deteriorates and another radio cell with better reception is within range, the dual-radio client will perform a cell change. During the cell change the dual-radio client continues to send the data via WLAN-2 on SSID-2, while WLAN-1 already starts sending the same data with better reception on SSID-1. A PRP-enabled switch filters out the duplicate PRP packets before forwarding the data to the LAN.

 In this scenario, the APs in the WLAN infrastructure do not have to be configured to operate PRP.

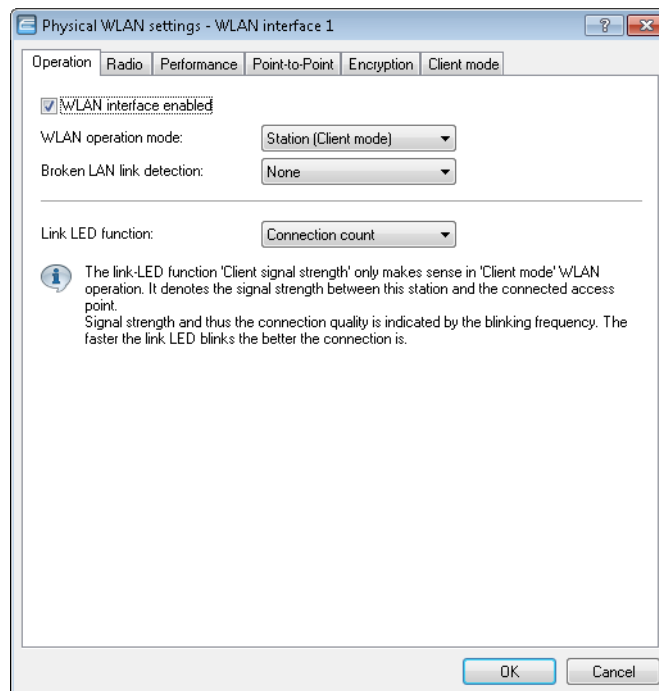
In order for the receiver to detect duplicate data packets, the APs in the WLAN infrastructure must be operating in client-bridge mode. The MAC address of the dual-radio client together with the RCT ensure that the receiver detects the duplicate packets. Without client-bridge support, an AP in the WLAN infrastructure would replace the MAC address of the dual-radio client with its own MAC address, so preventing the detection of duplicates.

Client-bridge support is enabled with LANconfig under **Wireless LAN > General > Logical WLAN settings** on the **Network** tab.



The PRP configuration of the dual-radio clients involves the following steps:

1. Under **Wireless LAN > General > Physical WLAN settings**, go to the **Operation** tab for each WLAN interface (WLAN interface 1, WLAN interface 2) and set the **WLAN operation mode** for each one to **Client**.

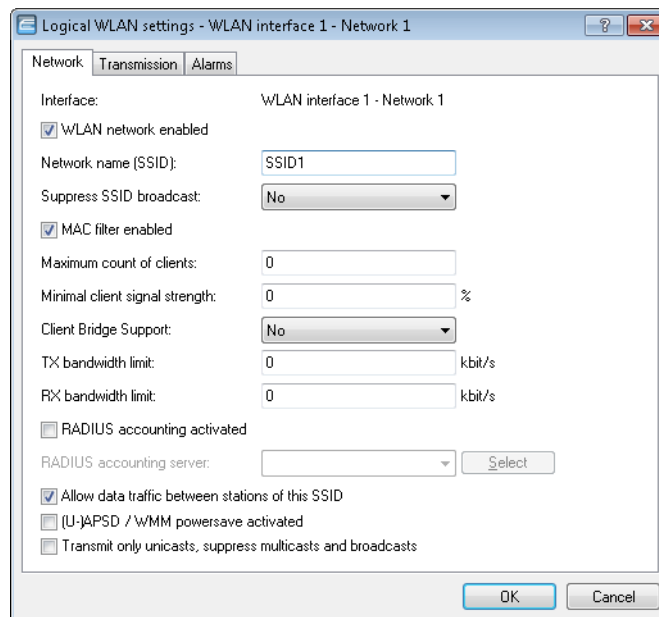


Specify the remaining WLAN parameters under **Radio**, **Performance**, **Encryption** and **Client mode** according to the requirements of the WLAN radio cells.

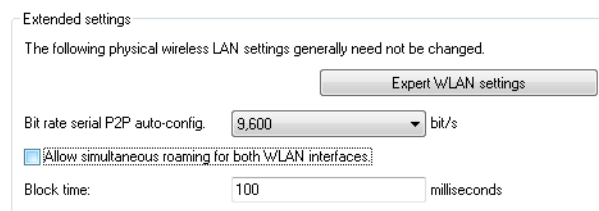


In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

2. To enter the SSID, switch to the view **Wireless LAN > General**, click **Logical WLAN settings** and, for each WLAN interface, select network 1.
3. In the field **Network name (SSID)**, enter the name of the WLAN which the WLAN interface is to be connected to.



4. Under **Wireless LAN > General** in the section **Extended settings**, disable the option **Allow simultaneous roaming for both WLAN interfaces**.



By deactivating the parallel roaming, you prevent the two physical WLAN interfaces from roaming at the same time or performing background scans. The result could be that both could lose connectivity to their radio cell.

When configured in this way, the dual-radio client can move past a line of APs and roam between the individual APs .

7.10.8 Additions to the Setup menu

Interface bundling

This table contains the settings for bundling the physical and logical interfaces.

By bundling interfaces, it is possible to transmit data packets on two paired interfaces. To do this, the device duplicates outgoing data packets and transmits them on each of the two interfaces simultaneously. When receiving packets, the device accepts the incoming packets; duplicates are detected and discarded by the device.

Using interface bundling makes it possible to reduce packet failure rates and latency times for data transmissions, although this does reduce the maximum bandwidth of the corresponding interface.

SNMP ID:

2.4.13.11.1

Telnet path:**Setup > LAN****Interfaces**

This menu contains the settings for interface bundling.

SNMP ID:

2.4.13.1

Telnet path:**Setup > LAN > Interface-Bundling****Interface**

This parameter indicates shows the logical cluster interface used for bundling the selected logical and physical interfaces of the devices.

SNMP ID:

2.4.13.1.1

Telnet path:**Setup > LAN > Interface-bundling > Interfaces****Possible values:****BUNDLE-1****BUNDLE-2****Operating**

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together under one shared logical bundle interface. In the disabled state the interfaces A and B that are selected in the corresponding table can still be used as individual interfaces.

SNMP ID:

2.4.13.1.2

Telnet path:**Setup > LAN > Interface-bundling > Interfaces**

Possible values:

Yes
No

Default:

No

Protocol

Set the protocol that is used for interface bundling using these parameters.

SNMP ID:

2.4.13.1.3

Telnet path:

Setup > LAN > Interface-bundling > Interfaces

Possible values:

PRP

Sets the Parallel Redundancy Protocol (PRP).

MAC address

Using this parameter you can set an alternative MAC address for use by the corresponding bundle interface.

SNMP ID:

2.4.13.1.4

Telnet path:

Setup > LAN > Interface-bundling > Interfaces

Possible values:

Max. 12 characters from `[a-f][0-9]`

Special values:

empty

If you leave this field empty, the device uses the system-wide MAC address.

Default:

Depends on the MAC address of your device

Interface-A

Using this parameter you select the 1st physical or logical link that this device bundles.

SNMP ID:

2.4.13.1.5

Telnet path:**Setup > LAN > Interface-bundling > Interfaces****Possible values:**

Select from the available interfaces.

Default:

WLAN-1

Interface-B

Using this parameter you select the 2nd physical or logical link that this device bundles.

SNMP ID:

2.4.13.1.6

Telnet path:**Setup > LAN > Interface-bundling > Interfaces****Possible values:**

Select from the available interfaces.

Default:

WLAN-2

Interfaces

This menu contains the settings for PRP as the bundling protocol.

SNMP ID:

2.4.13.11

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Interfaces**

This table contains the interfaces with all PRP-relevant settings.

SNMP ID:

2.4.13.11.1

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Interface**

The parallel redundancy protocol (PRP) makes redundant transmissions on two (bundled) interfaces. To use this, you select two interfaces which the device internally combines into one interface. The device duplicates outgoing packets so that the packets are transmitted on each of the two interfaces. On the receiving side, the device recognizes the duplicates and discards them. This leads to a reduced packet error rate and to lower latency on the bundled interface in comparison to transmission on a single interface. Enter the name for this interface here.

SNMP-ID:

2.4.13.11.1.1

Pfad Telnet:**Setup > LAN > Interface-bundling > PRP > Interfaces****Mögliche Werte:**Max. 18 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Duplicate-accept**

Switches the forwarding of packet duplicates on or off.

SNMP ID:

2.4.13.11.1.2

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Possible values:****Special values:**

Yes

No

Transparent-mode

Switches the transparent operation mode on/off. If the transparent operation mode is enabled, the recipient of the PRP packets forwards the packets with a redundancy control trailer.

SNMP ID:

2.4.13.11.1.3

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces**

Possible values:

Yes
No

Default:

No

Life-Check-Interval

Specifies how often the device sends control packets.

SNMP ID:

2.4.13.11.1.4

Telnet path:

Setup > LAN > Interface-bundling > PRP > Interfaces

Possible values:

100 ... 60000 Milliseconds

Default:

2000

Node-forget-time

Enters the time until the device deletes a node from its node table or proxy node table.

SNMP ID:

2.4.13.11.1.5

Telnet path:

Setup > LAN > Interface-bundling > PRP > Interfaces

Possible values:

1000 ... 3600000 Milliseconds

Default:

60000

Entry-forget-time

Specifies as of when the device deletes the entry from the duplicate-detection buffer.

SNMP ID:

2.4.13.11.1.6

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Possible values:**

10 ... 60000 Milliseconds

Default:

400

Node-Reboot-Interval

Specifies the time that a PRP device passively monitors a link until the device sends packets over the link.

SNMP ID:

2.4.13.11.1.7

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Possible values:**

0 ... 60000 Milliseconds

Default:

500

Dup-Elimination-Buffer-Size

Limits the number of entries in the duplicate-detection memory.

SNMP ID:

2.4.11.1.8

Telnet path:**Setup > LAN > Interface-bundling > PRP > Interfaces****Possible values:**

16 ... 65536 Entries/Nodes

Default:

8192

Send supervision packets

Specifies the settings for sending supervision packets.

SNMP ID:

2.4.13.11.1.9

Telnet path:**LAN > Interface-bundling > PRP > Interfaces****Possible values:****0**

None

1

Own-MAC-only

2

All-nodes

Default:

2

Node-Name

The node name is the identifier for the node. You can specify any name.

SNMP-ID:

2.4.13.11.1.10

Pfad Telnet:**Setup > LAN > Interface-bundling > PRP > Interfaces****Mögliche Werte:**

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

Evaluate-Sup.-Frames

Switches the monitoring of control packages on or off.

SNMP-ID:

2.4.13.11.1.11

Pfad Telnet:**Setup > LAN > Interface-bundling > PRP > Interfaces**

Mögliche Werte:

Yes
No

Default-Wert:

Yes

8 WLAN management

8.1 AutoWDS – wireless integration of APs via P2P connections

In a centrally managed WLAN network, access points (APs) are typically connected to the WLAN controller (WLC) via the LAN. The LAN connections simultaneously determine the topology of the managed network. Network extension by means of additional APs is restricted to the reach of the hard-wired network architecture and requires the extension of the corresponding infrastructure.

By means of **AutoWDS**, you have the option of extending a WLAN by means of point-to-point (P2P) connections for the cost-effective and fast installation of highly scalable networks. "AutoWDS" stands for "automatic wireless distribution system". This feature enables you to create a radio network from several APs, which are interconnected via wireless only: a logical connection is all you need. Potential applications include the seamless connection of smaller properties or even entire districts to the Internet, or the establishment of a company network where connections via LAN are impracticable.

In the simplest case, all you need is a WLC connected via LAN to an AutoWDS-enabled AP. The AP supports the managed network and at the same time acts as an "anchor AP". Using this anchor AP, unassociated AutoWDS-enabled APs connect to the WLC, which transmits a configuration to them by means of CAPWAP. After obtaining the configuration and being incorporated into the managed WLAN, the individual APs use P2P links to forward user data, to communicate with one another, and to support the topology. Additional APs that join later are able to use the associated APs as their anchor APs. In this manner, several APs can be chained together to establish meshed networks, which can optionally feature

redundant connections via RSTP. From the perspective of an unassociated AP, associated APs are master APs. From the perspective of the master AP, unassociated APs are slave APs.

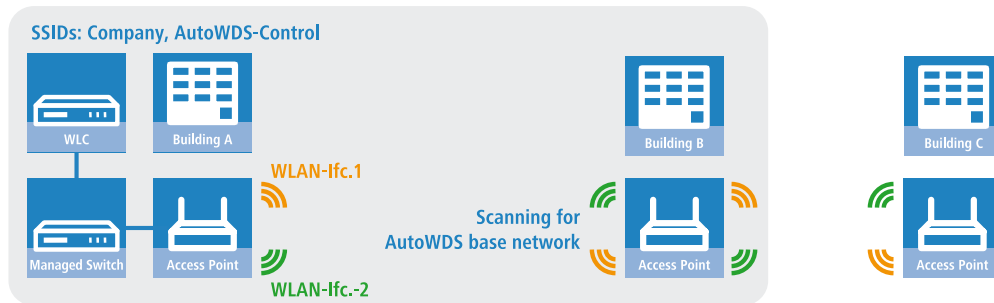


Figure 1: Phase 1 – unassociated AP in building B seeks AutoWDS base network and finds anchor AP in building A

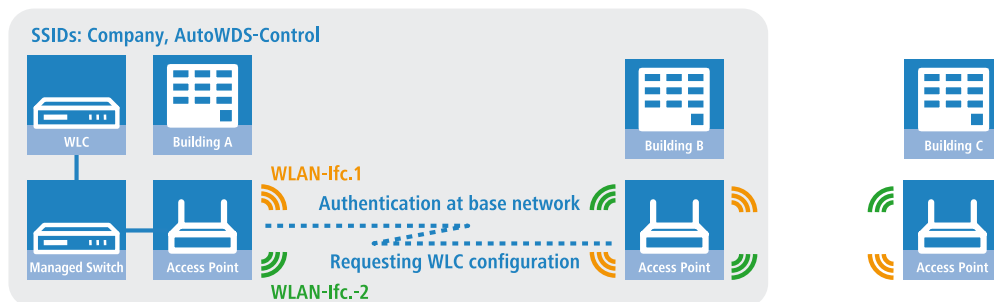


Figure 2: Phase 2 – unassociated AP in building B finds WLC and retrieves AP configuration via CAPWAP

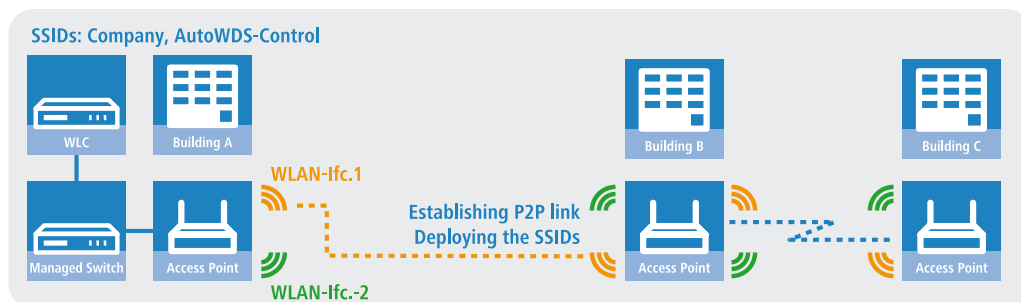


Figure 3: Phase 3 – unassociated AP in building B joins the managed WLAN. Unassociated AP in building C seeks AutoWDS base network and finds anchor AP in building B

Precise information about the integration process and the operating modes for topology management can be found in the following sections, which describe how AutoWDS functions.

- ❗ AutoWDS is suitable for static infrastructure only, not for mobile APs. If an AP should move out of range of its P2P partner and lose the connection to the network, there is a temporary downtime and a subsequent *reconfiguration*. However, the roaming of WLAN clients between individual AutoWDS APs is no different than the roaming between conventional APs.
- ❗ AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.
- ❗ The DFS processing by an AP in 5-GHz operation is unaffected by AutoWDS and has a higher priority. DFS radar recognition may cause the AP to suddenly change the channel during operation. It can even completely deactivate the WLAN for a period if radar recognition is running on different channels and the available frequencies drop

out. The impacted AP can cause interference to the entire AutoWDS group, and may not be able to deploy any SSIDs for some time. Within buildings you have the option of counteracting interference by enabling the indoor mode.

- i** If you operate AutoWDS on a device with a single physical WLAN interface, its data rate will be reduced to just a third, since the device must send incoming/outgoing data multiple times: To the WLAN clients, to a master AP and, if applicable, to a slave AP. This effect is mitigated by operating only devices that have multiple WLAN physical interfaces and using these to divide up the data traffic. You do this by reserving one physical WLAN interface for connecting the APs and one physical WLAN interface for connecting the clients.

8.1.1 Notes on operating AutoWDS

Owing to technical restrictions, the applications of AutoWDS are limited to certain specific application scenarios. Please carefully observe the general remarks in this chapter to avoid possible complications. The items listed here are intended to supplement the remarks elsewhere in the AutoWDS chapter, so some redundancies are possible.

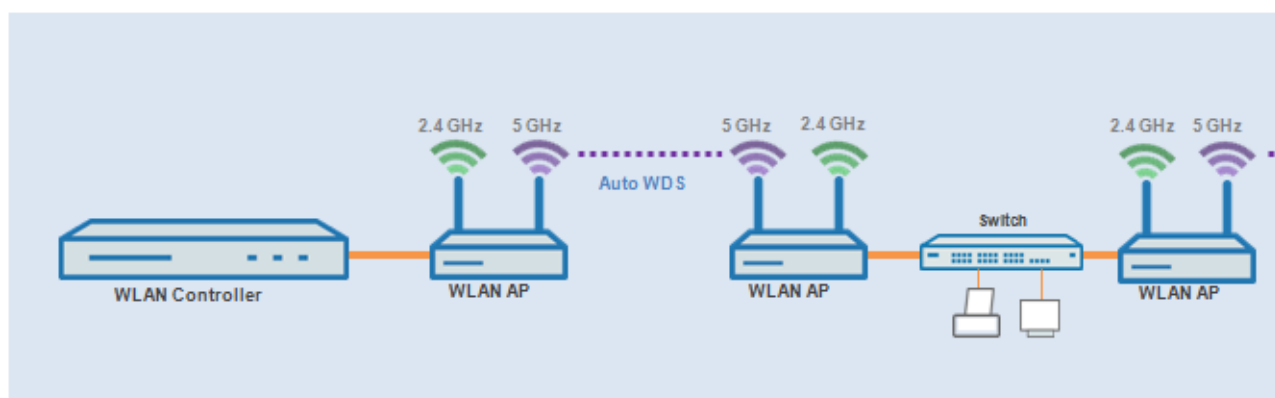
- APs must switch channels when radar is detected (5-GHz band, outdoor and DFS). This can potentially lead to temporary interruptions to the WLAN due to necessary changes of channel.
- In general, we recommend a maximum of 3 hops for AutoWDS operations.
- When operating AutoWDS on one radio channel only, problems with multiple transfers and hidden stations can occur. For this reason we recommend the use of APs with two physical WLAN interfaces (dual radio) operating on separate radio channels.
- AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.

The following is a overview of the **suitability of AutoWDS** for certain application scenarios.

Suitable:

Use of a **dedicated** physical WLAN interface for the P2P links.

- Use of different channels for the P2P links (indoor)
- Use of AutoWDS with up to 3 hops

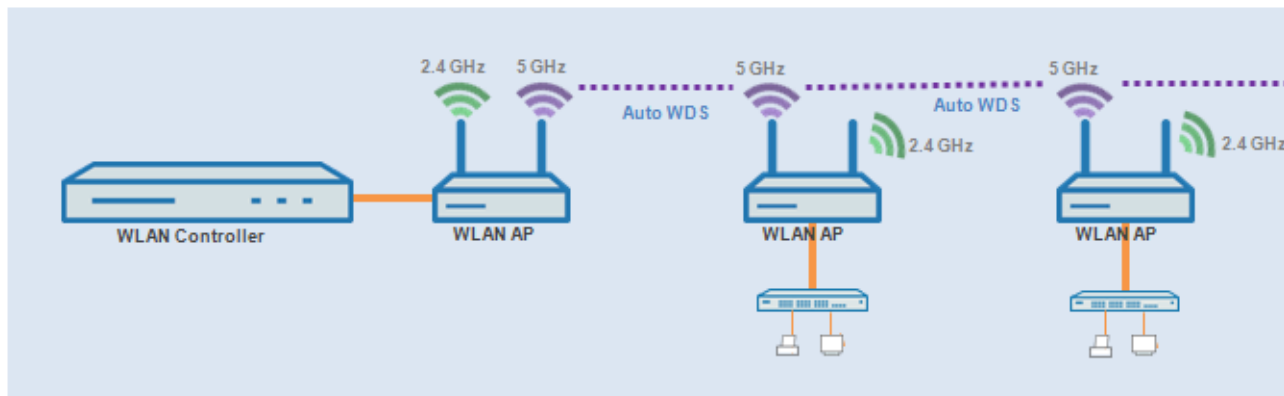


Partly suitable:

Use of single physical WLAN interface **simultaneously** for the AutoWDS uplink and downlink (repeater mode) where all P2P links operate on the same radio channel.

- Use for operation without DFS (indoor)

- Use of AutoWDS with up to 3 hops



Difficulties can arise from the hidden station problem or throughput loss due to multiple transmissions.

- **Hidden station problem:** Over larger distances, widely separated APs on the same network may not be able to "see" each other. In this case, several APs could end up transmitting simultaneously to cause interference for the APs between them. These collisions lead to multiple transmissions and performance losses.

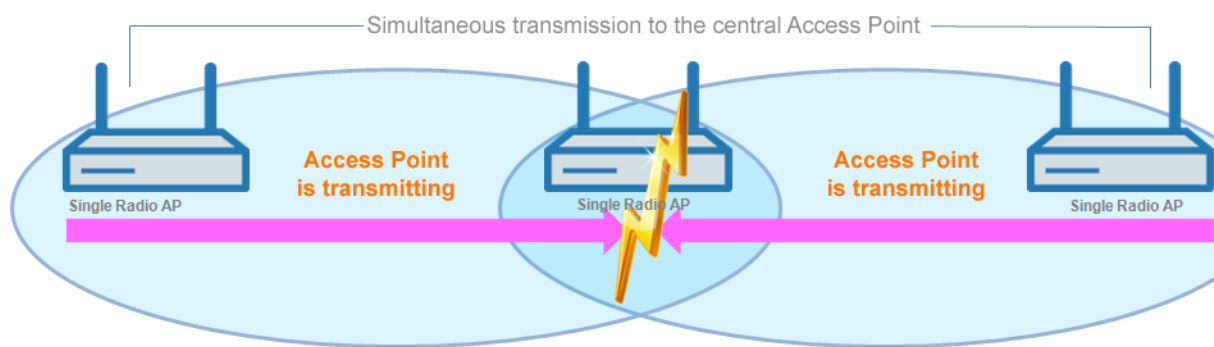


Figure 4: Simultaneous transmissions to the middle AP: The two outer APs are unaware of the collision.

- **Throughput-loss due to multiple transmissions:** An AP transmitting data packets multiple times on the same channel leads to a reduction of the maximum available throughput (by half per hop).

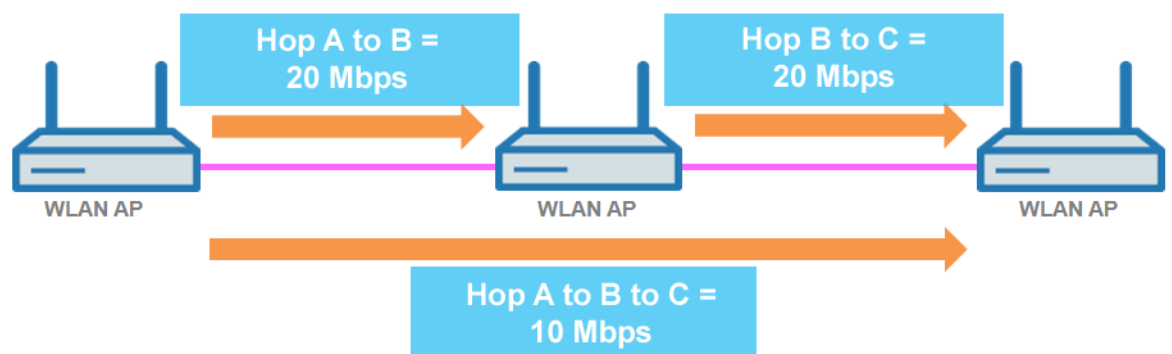
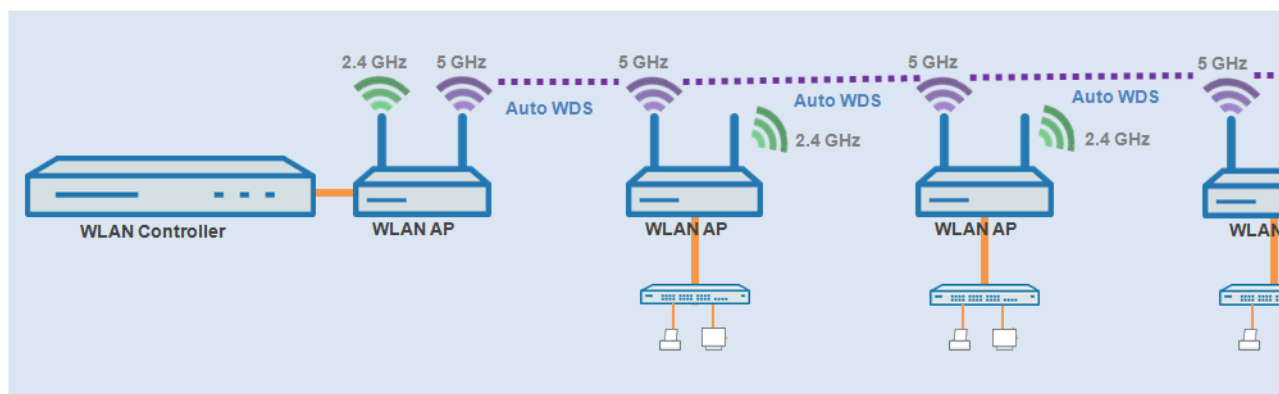


Figure 5: Transmission of data packets on every hop

Unsuitable:

Use of a physical WLAN interface **simultaneously** for AutoWDS uplink and downlink (repeater mode) during outdoor operations with more than one hop in the 5-GHz band.



In repeater mode, the physical WLAN interface has a dual role: In the direction of the WLC the interface operates as a master, while in the direction of neighboring APs it operates as a slave. For this purpose, all APs necessarily operate on the same radio channel. However, if the DFS feature detects signals, the APs are required to stop transmitting on the affected frequencies. This means that the APs cannot inform the WLC about the DFS event and the WLC cannot initiate a change of frequency for the network. As a result, the affected APs are potentially permanently separated from the network.

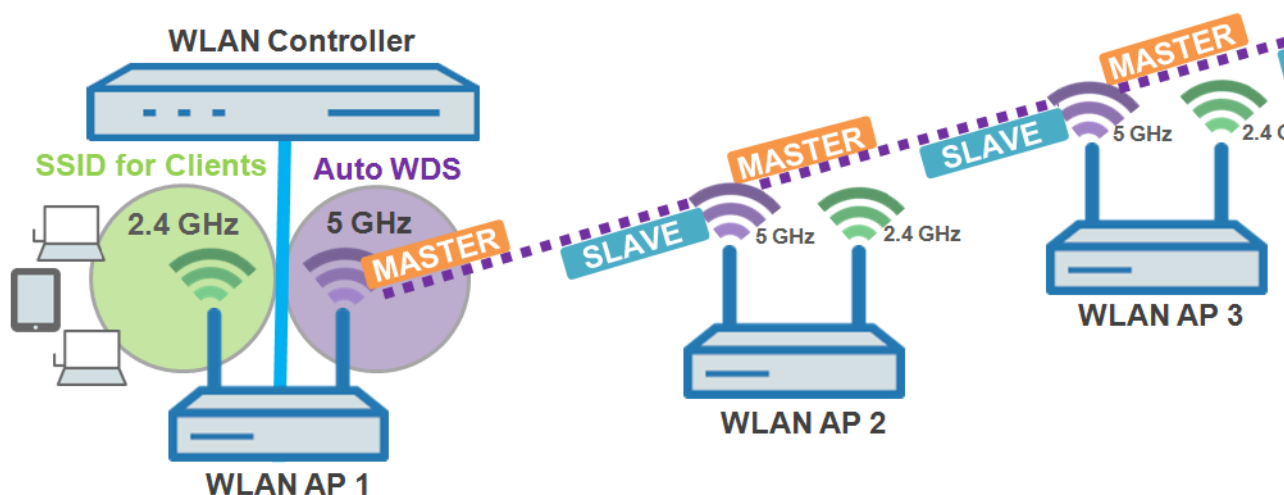


Figure 6: Connection lock after DFS detection

8.1.2 How it works

Deploying the AutoWDS base network

AutoWDS provides different integration modes for managing P2P links for meshed networks. The majority of the configuration is performed on the WLC which manages the individual logical WLAN networks. You add an active AutoWDS profile to the existing WLAN profile for your managed WLAN. The AutoWDS profile groups the settings and limits to form the P2P topology and of the AutoWDS base network.

The AutoWDS base network and its associated SSID (default name: **AutoWDS-Rollout**) is a management network only. It serves two purposes: The first is to authenticate an AP during the preconfigured integration, and the second is to establish the WLC tunnel for configuration exchange. In this way, unassociated APs remain isolated from operations while they are being integrated into the managed WLAN. As soon as there is a P2P connection to a master AP, an unassociated AP is considered to be integrated and it processes further communications via the bridge on Layer 2. Similar to conventional P2P links, the P2P partners set up a management SSID, which they use to process the data traffic and the CAPWAP tunnel to the WLC (see [Updating the AP configuration and establishing the P2P link](#) on page 166).



The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within the WLAN infrastructure.

After assigning an active AutoWDS profile to your managed WLAN, the corresponding anchor APs deploy the AutoWDS base network and transmit their beacons with an additional manufacturer-dependent identifier. This identifier, also known as an "AutoWDSInfoFlag", signals the general support of the feature to unassociated AutoWDS-capable APs and informs them...

- whether AutoWDS is enabled/disabled for the detected SSID;
- whether the AP of the corresponding SSID has an enabled/disabled WLC connection;
- whether the WLC accepts or prohibits the express mode for unassociated APs; and
- whether integration requires the APs to connect to the equivalent physical WLAN interface of the anchor AP (strict interface pairing, i.e. with WLAN-1 to WLAN-1 and with WLAN-2 to WLAN-2), or whether mixed interface pairs are allowed.

An AP automatically becomes the unassociated AP as soon as you activate the AutoWDS feature in its configuration and its physical WLAN interface is in **Managed** mode. This access point then temporarily switches its operating mode to **Client** mode and scans each WLAN until it detects a suitable anchor AP. The scan is carried out in the 2.4-GHz and 5-GHz frequency bands.

If your device has two physical WLAN interfaces and both are enabled, both WLAN interfaces simultaneously scan for a suitable AutoWDS base network. If a physical WLAN interface detects a suitable SSID, then it associates with the anchor AP, assuming that the interface pairing mentioned above permits this. The other physical WLAN interface continues to scan in case the already associated physical WLAN interface loses the connection again. Until then, this physical WLAN interface does not connect to any other AutoWDS base network. Once your device has received the WLC configuration, the two physical WLAN interfaces behave as specified in the profile, i.e. they deploy the SSIDs assigned to them and the AutoWDS base network.

The procedure for searching for an AutoWDS base network is identical with that of the reconfiguration in the case that the WLAN connection is lost (see [Connectivity loss and reconfiguration](#) on page 166).

Differences between the integration modes

When integrating unassociated APs into your managed WLAN, you have the choice of two different integration modes. The integration mode determines the conditions under which your WLC accepts an unassociated AP:

- **Preconfigured integration** is the controlled and preferred method to integrate an unassociated AP into a managed WLAN over a point-to-point link. In this mode, the WLC only allows the integration of APs that have a local, preconfigured SSID and a valid WPA2 passphrase for the AutoWDS base network.

This mode is suitable for all productive environments, and is used to create a predefined relationship between an unassociated AP and an AutoWDS base network. As soon as the AP obtains a configuration from the WLC, the AP gives this configuration a higher priority than its own local AutoWDS configuration. This remains so until the WLC revokes the configuration via CAPWAP or you reset the device.

- **Express integration** is the quick way to integrate an unassociated AP into a managed WLAN via a point-to-point link. In this mode, the WLC allows both the integration of preconfigured devices as well as devices that are not configured at all. Unconfigured APs have neither a registered SSID nor an individual WPA2 passphrase for the AutoWDS base network. Instead, APs can authenticate with any AutoWDS base network by using a pre-shared key hard-coded in the firmware.

This mode is suitable for the easy integration of new APs into a managed WLAN. The choice of AutoWDS base network is automatic and is outside your control. As soon as the corresponding APs obtain configurations from the WLC, these devices save the settings as default values until the WLC revokes the configuration via CAPWAP, the device executes the express [reconfiguration](#) after an interruption in the connection, or you reset the device.

-
- ❗ For the express integration make sure that no other AutoWDS base network is in range. Otherwise it is possible for an external WLC to take control of your AP and revoke your remote access. Generally you should use the express mode as little as possible to minimize any vulnerabilities.
-
- ❗ For the security reasons name above, LANCOM recommends a preconfigured integration. Through the pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. Learn more about this in section [Accelerating preconfigured integration by pairing](#) on page 171.
-

After successful authentication on the AutoWDS base network, the unassociated APs scan the network for a WLC. As soon as they have detected a WLC, they attempt to connect with it and retrieve a configuration. In LANmonitor, these APs are shown as unassociated devices. To include these in the managed WLAN, the administrator must still confirm them and assign WLAN profiles to them. Assigning profiles in this way is no different from accepting normal APs. Alternatively, assignment can be handled by the WLC if you

- set up a default WLAN profile and activate its automatic assignment; or
- enter the associated AP into the access point table and link it with a WLAN profile.

-
- ❗ By simultaneously setting the automatic acceptance of unassociated APs by the WLC ("Auto Accept"), the integration of unassociated APs can be fully automated. However, for express integration you should ensure that you disable this setting in order to maintain a minimum level of security and hinder rogue AP intrusion.
-
- i The procedures for certificate generation, certificate checks, and the automatic acceptance or rejection of connection requests by the WLC are identical to a WLAN scenario with cable-connected APs. Refer to the Reference Manual.
-

Designing the topology

When the WLAN profile is assigned by the WLC, the slave APs simultaneously receive information about how the topology of the meshed network is structured. The topology results directly from the hierarchy of the P2P connections established between the APs. The WLC offers the following management modes for this:

- **Automatic:** The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.
- **Semi-automatic:** The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.
- **Manual:** The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Normally, the WLC handles the automatic calculation of the topology, where a slave AP generally connects with the closest master AP. Calculated in real-time, the topology is recorded by the WLC in the status table

AutoWDS-Auto-Topology. If you use semi-automatic or manual management, you define the static P2P links in the setup table **AutoWDS-Topology**. To achieve this, you specify the relationships between the individual master APs and slave APs in a similar manner to a normal P2P connection. For more on this, see the section [Manual topology management](#) on page 172.

-
- i The automatic generation of a P2P configuration (e.g., for initial connection or reconnection of an AP) replaces any existing entry in the AutoWDS-Auto-Topology table.
-
- i The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.
-

Updating the AP configuration and establishing the P2P link

If an unassociated AP has received the full WLAN profile with all its settings from the WLC via CAPWAP, as a slave it attempts to establish a P2P link to the master AP assigned to it. The AP simultaneously changes its WLAN operation mode from **Client** back to **Managed**.

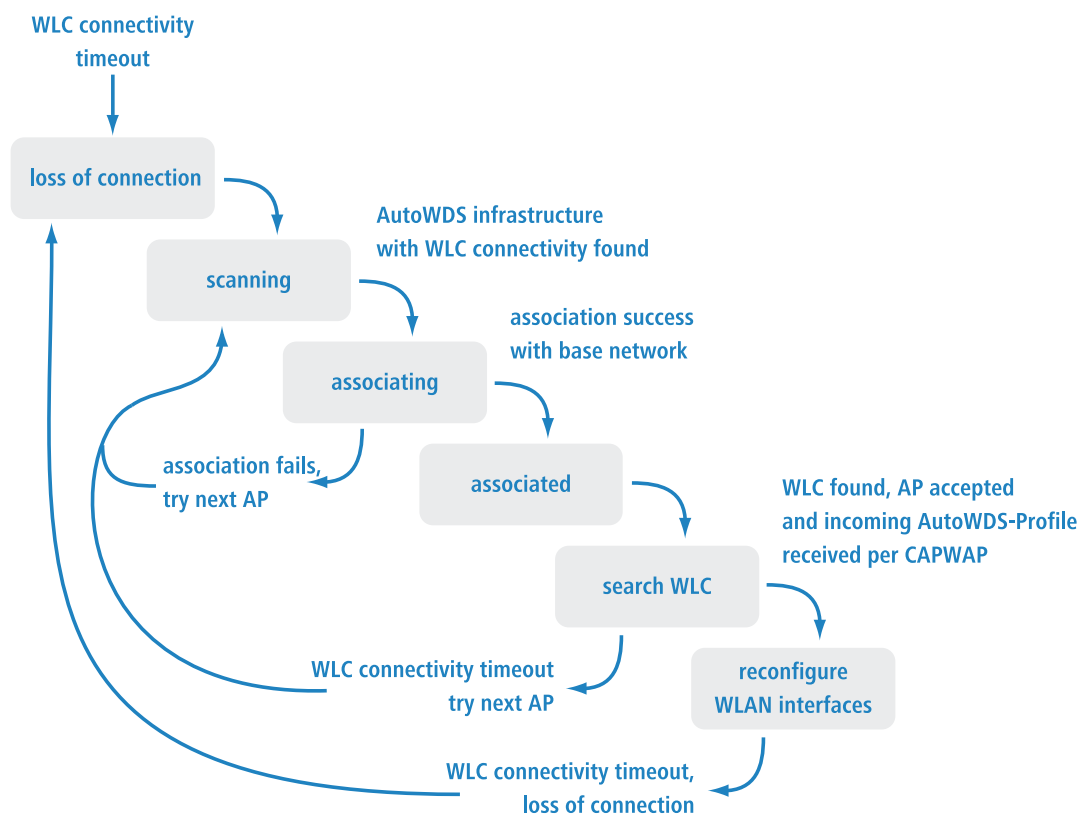
Since the master AP is already in managed mode, it obtains only an update to its P2P configuration from the WLC via CAPWAP. This update enables P2P on the physical WLAN interface, sets the channel selection scheme to **Master**, and informs the AP of the WPA2 passphrase and the peer identification of the AP. For an automatically generated P2P configuration, the peer identification corresponds to the MAC address; for a manual P2P configuration, it corresponds to the name of the slave AP. The master AP labels the SSIDs with ***** P2P Info *****.

Once both APs are successfully interconnected over a P2P link, the AutoWDS integration process is concluded. The unassociated AP can then be used by clients (smartphones, laptops, other APs in client mode looking for a master, etc.).

i As long as the unassociated AP is in client mode, bridging between a physical WLAN interface and a LAN interface or another physical radio interface is disabled throughout the integration process. The device automatically puts all physical WLAN interfaces on different bridges. Not until successful creation of a P2P connection does the AP switch the bridging back to the original state.

Connectivity loss and reconfiguration

An automatic process of (re-)configuration is triggered as soon as you enable AutoWDS on an unassociated AP, if authentication at an anchor AP fails, or if an associated AP loses contact to the WLC. This process follows the scheme shown here:



An AP does not run the (re-)configuration process if it is in client mode and can connect to an anchor AP but not to the WLC. The AP waits for 5 minutes after connecting to the AutoWDS base network to see whether the WLC performs a configuration of the device. If no configuration is performed by the WLC by then (e.g., because no administrator accepts the AP), the AP disconnects from the AutoWDS base network and scans for further suitable SSIDs. If there is only one SSID in range, the AP contacts it again to repeat the integration process.



If there is a connection to a LAN, the AP tries to reach the WLC by broadcast over the LAN for the duration of the downtime. If the AP finds the WLC via LAN, then no new P2P link is set up and the WLC deletes all automatically generated P2P links that set the AP to be a slave.

Configuration timeouts

The initial configuration and the reconfiguration of an unassociated AP are triggered by various timeouts, which together control the behavior of the device. This includes, if specified:

1. The duration of standalone P2P-link operation if the CAPWAP connection is lost (except for reconfiguration);
2. The wait time until the start of the automatic (re-)configuration for the preconfigured integration; as well as
3. The wait time until the start of the automatic (re-)configuration for the express integration.

The continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards the P2P part of the WLC configuration. If the standalone continuation time is specified as 0, the AP discards this part of the configuration immediately.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the wait times for the preconfigured and express integration—as a basis to count down the preset time until the start of the (re-)configuration for the preconfigured integration. After this wait time expires, the device switches its physical WLAN interface(s) into client mode and scans the available SSIDs for the last detected AutoWDS base network. At the same time, the timer starts the countdown to the start of the automatic (re-)configuration for the express integration.

If the device has not found the expected AutoWDS base network when the express timer expires, the device automatically switches to express integration. It then searches for any AutoWDS-enabled network until a suitable anchor AP is detected.

By adjusting the interaction between the various wait times, you can allow the device to react flexibly to unforeseen events. This facilitates the implementation of a fallback solution, for example in the case that you change the pre-shared key for the AutoWDS base network. If the change should fail on an unassociated AP, the device becomes inaccessible as it has an invalid configuration. Please observe the notes under [Differences between the integration modes](#) on page 164.

The relevant counters are configured on the AP (e.g. via LANconfig) and also on the WLC (Setup menu only). The counters are only observed by the AP if no WLC configuration (initial configuration) is available. As soon as a configuration is available, then the values specified in the AutoWDS profile apply (reconfiguration). Learn more about the setting the priorities for configurations under [Differences between the integration modes](#) on page 164.



If you disable the express timer or the preconfiguration timer, the device skips the corresponding integration step. The automatic reconfiguration can be switched off by disabling both timers. This means that, after being disconnected for long enough, the device can no longer be reached by AutoWDS. However, the device remains accessible over the LAN interface and searches the LAN for a WLC.

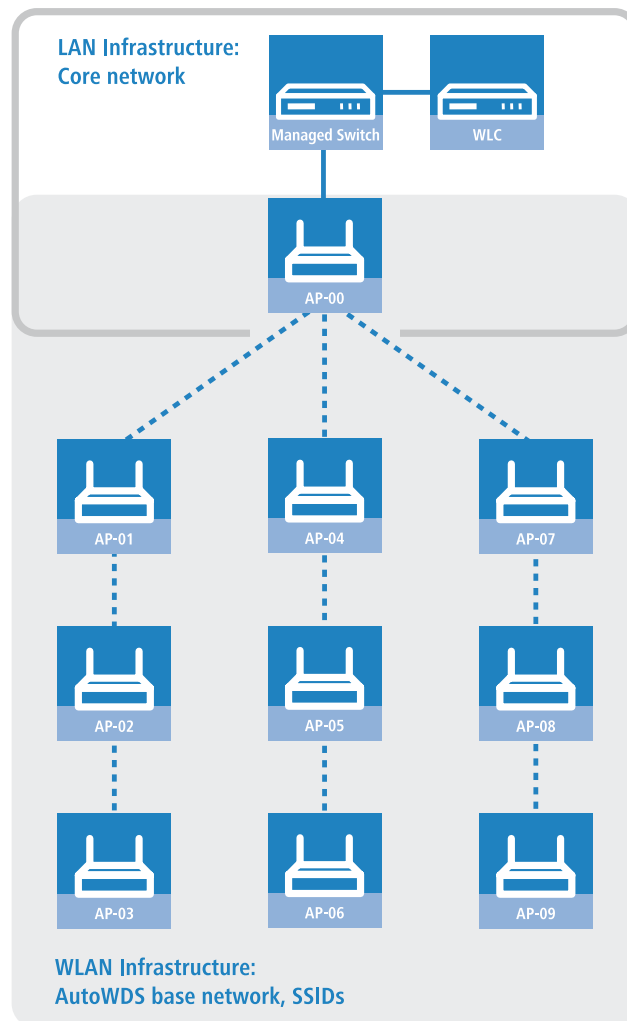


The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.

Example: Failure of an AP

Each AP maintains its CAPWAP connection by issuing echo requests to the WLC at a specified interval. If an AP fails or its connection is interrupted, these requests will be lost. If the APs repeat the echo request and receive no response from

the WLC, the CAPWAP connection is considered to be lost and the APs start the reconfiguration process described under *Connectivity loss and reconfiguration* on page 166.



For the infrastructure illustrated above, a failure of AP-01 would have the following impact, assuming that automatic topology management is enabled:

1. AP-01 is defective.
2. AP-02 and AP-03 repeat their echo-requests; all repeats fail.
3. AP-02 and AP-03 start the standalone operation of their P2P link (if configured) and continue to try to reach the WLC (over wireless and LAN, assuming connectivity exists).
4. AP-02 and AP-03 stop their autonomous operation of P2P connections.
5. AP-02 and AP-03 count down the wait time until the start of the preconfigured integration.
6. After the wait time expires, AP-02 and AP-03 switch into client mode and scan the WLAN for the last known AutoWDS base network.
7. AP-02 and AP-03 find a new anchor AP (e.g. B. AP-05 or AP-06) and login as clients.
8. AP-02 and AP-03 restore the CAPWAP connection via the **WLC-TUNNEL-AUTOWDS** and inform the WLC about the new anchor AP and the physical WLAN interfaces they are using.
9. The WLC generates a P2P link for the corresponding physical WLAN interfaces and delivers the configuration to the APs by CAPWAP.
10. The APs set up the new P2P link to the master APs assigned to them and stop communicating with the WLC via the **WLC-TUNNEL-AUTOWDS**; they are bridged to the LAN instead.

8.1.3 Setup by means of preconfigured integration


The following sections show you how to set up an AutoWDS network by means of the preconfigured integration. Configuration relies on the automatic topology management of the WLC.

In this scenario, a company is expanding its business premises into a new building. The company wants to integrate the new business premises into its existing managed WLAN. The relevant APs should be connected exclusively via point-to-point link. Between building A (old) and B (new), no wired network connection can be installed.

To keep the configuration simple, a single WLC is used to configure all of the APs. The exact number of APs in building A and building B is immaterial. Particular features, such as multiple physical WLAN interfaces, are automatically taken into account by the WLC topology management.

The configuration itself is divided into two parts:

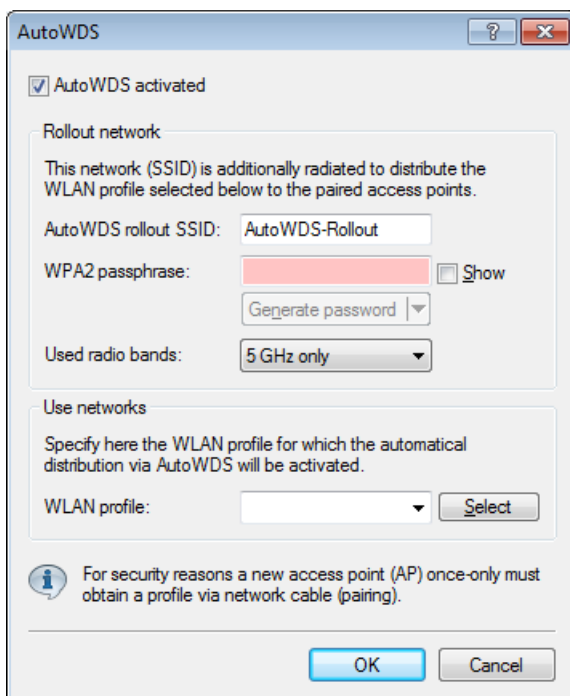
1. Configuration of the WLC in building A
2. Configuration of all APs in building B

 The example application requires a valid WLAN configuration with valid certificates in the WLC. Just how to set up a managed WLAN is described in the chapter on WLAN management.

Configuring the WLC


The following instructions describe how to configure the AutoWDS of a central WLC for preconfigured integration.

1. Open the configuration dialog in LANconfig and click on **WLAN controller > Profiles > AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Enter the name of the AutoWDS base network under **AutoWDS-Rollout-SSID**. By default LANconfig uses the identifier `AutoWDS-Rollout`.

The SSID specified here acts as the management network for all APs that are searching for the AutoWDS network and, apart from the passphrase, it offers no further options for configuration. The WLC internally connects the specified SSID automatically using a WLC tunnel (**WLC-TUNNEL-AUTOWDS**). Normal WLAN clients are unable to use this management network.

 Setting up this AutoWDS base network reduces the maximum number of SSIDs that your device can support on a physical WLAN interface by 1.

4. Under **WPA2 passphrase** you enter a key to secure the AutoWDS base network.

Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

5. Under **Used radio bands** you specify the frequency band used by the APs for the AutoWDS base network.

6. Select the **WLAN profile** with the SSID which is to be enhanced with AutoWDS.

The APs with this WLAN profile serve as anchor APs and support the AutoWDS base network. At the same time, associated APs receive this WLAN profile via AutoWDS as a default configuration, which they use to transmit the corresponding SSID.

7. Close the dialog window with **OK** and save the configuration to the device.

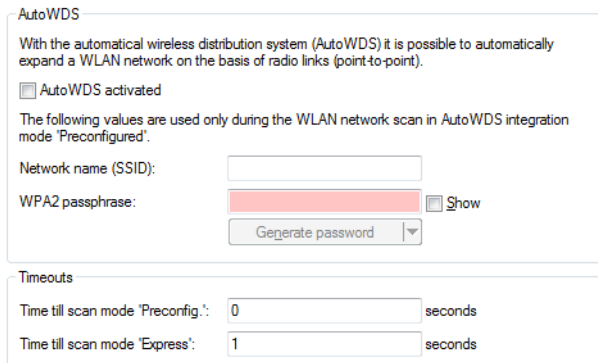
The WLC now assigns the AutoWDS settings to all managed AutoWDS-capable APs in your WLAN. These now form the basis for your AutoWDS base network. For future reconfiguration processes, the APs use only the SSID and passphrase stored here, unless configured otherwise (see [Differences between the integration modes](#) on page 164).

This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for preconfigured integration. The configuration steps are identical for all unassociated APs.

1. Open the configuration dialog in LANconfig and click on **Wireless LAN > AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Under **Network name (SSID)** enter the name of the AutoWDS base network that you configured on the WLC (e.g. AutoWDS-Rollout).
4. Enter the key for the AutoWDS base network under **WPA2 passphrase** that you have configured on the WLC (e.g. AutoWDS-Control).
5. Change the timeout values for the **Time till search mode 'Preconfig'** to 1 and for the **Time until search mode 'Express'** to 0.
6. Under **Wireless LAN > General > Physical WLAN settings**, make sure that at least one physical WLAN interface is in **Managed** mode.
Otherwise the device will never search for an AutoWDS base network.
7. Close the dialog window with **OK** and save the configuration to the device.

After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for the specified AutoWDS base network. To learn more about the procedure, refer to the [chapter about the function](#).

8.1.4 Accelerating preconfigured integration by pairing

Through the one-time pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. For pairing, you reset an AP and connect it via LAN to the WLC used for running your managed WLAN including AutoWDS. In the reset state, the AP is automatically in managed mode after being switching on. Once the AP finds the WLC and the WLC accepts the AP, the AP automatically receives all relevant certificates and partial configurations required to configure the parameters in the device. Pairing is then complete. On location, a coworker installs the AP and switches it on. Your device then searches for the preconfigured AutoWDS base network.

The following steps summarize the pairing procedure. They also include the steps for automatic configuration assignment, which further simplifies the pairing of a high number of APs.

1. Start LANconfig and, on your WLC, set up a managed WLAN with a valid WLAN profile, if you have not already done so. In LANconfig you configure this type of profile under **WLAN controller > Profiles > WLAN profiles**.
2. Activate AutoWDS for this WLAN profile as described in [Configuring the WLC](#) on page 169.
3. Create a profile that is valid for all APs under **WLAN controller > AP configuration > Access point table** with the button **Default**. Assign the **WLAN profile** you created earlier to this profile
4. Enable the option **Automatically provide APs with a default configuration** under **WLAN controller > General**.
5. **Optional:** To avoid having to manually accept unassociated APs in LANmonitor by allowing the WLC to do this automatically, you should additionally select the option **Automatically accept new APs (auto-accept)**.



For security reasons, you should only enable this option if you have connected the unassociated APs to the WLC via a LAN interface. To exclude the possibility of rogue AP intrusion, make sure that no other devices are connected with the WLC.

6. Send the configuration to the WLC.
7. Reset the unassociated AP and connect the device to the WLC via the LAN.
The device automatically starts to search for a WLC.
8. In LANmonitor, you accept the new AP under **Wireless LAN > New APs**, unless you have set up automatic acceptance. The WLC sends the device those parts of the configuration that it needs for its future operation in managed mode. After successful configuration, LANmonitor lists the device in the **Active APs**.

This completes the pairing and the AP is ready for AutoWDS operation.

8.1.5 Express integration

The following sections show you how to set up an AutoWDS network by means of the express integration. Configuration relies on the automatic topology management of the WLC.

The initial scenario is similar to the [preconfigured integration](#).



By default, AutoWDS is disabled on a reset AP and you must first use a wired access to activate the feature.



Express configuration has certain characteristics that are relevant to security. We recommend that you read the section [Differences between the integration modes](#) on page 164 carefully.

Configuring the WLC

The following instructions describe how to configure the AutoWDS of a central WLC for express integration.

1. Carry out each step under [Configuring the WLC](#) on page 169 for the preconfigured integration.
2. Log on to your device via WEBconfig or the console.
3. In the setup menu, navigate to the table **WLAN-Management > AP-Configuration > AutoWDS-Profiles**.
4. Edit the AutoWDS default profile by clicking on the entry **AUTOWDS_PROFILE**.
5. Change the **Allow-Express-Integration** parameter to **Yes** and save the settings by clicking on **Send**.

This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for express integration. The configuration steps are identical for all unassociated APs.

1. Open the configuration dialog in LANconfig and click on **Wireless LAN > AutoWDS** to access the AutoWDS dialog.

2. Click on **AutoWDS activated** to enable the feature on the device.
3. Under **Wireless LAN > General > Physical WLAN settings.**, make sure that at least one physical WLAN interface is in **Managed** mode.
Otherwise the device will never search for an AutoWDS base network.
4. Close the dialog window with **OK** and save the configuration to the device.

After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for any AutoWDS base network. For further information on this procedure please refer to [Deploying the AutoWDS base network](#) on page 163.

8.1.6 Switching from express to preconfigured integration

Following a network rollout and the express integration, the switch to a preconfigured integration is implemented by disabling the express integration on the WLC. There is no need to change anything on the APs because they have already received an AutoWDS configuration during the express integration, and this pre-configures an AutoWDS network for subsequent re-configuration procedures.

1. Log on to your device via WEBconfig or the console.
2. In the setup menu, navigate to the table **WLAN-Management > AP-Configuration > AutoWDS-Profiles**.
3. Edit the AutoWDS default profile by clicking on the entry **AUTOWDS_PROFILE**.
4. Change the **Allow-Express-Integration** parameter to **No** and save the settings by clicking on **Send**.

You have now disabled the express integration of further unassociated APs.

8.1.7 Manual topology management

The examples of AutoWDS installation rely upon automatic topology management by the WLC, which simplifies the configuration. Depending on the usage scenario, it may be necessary to setup individual or all of the P2P links manually.

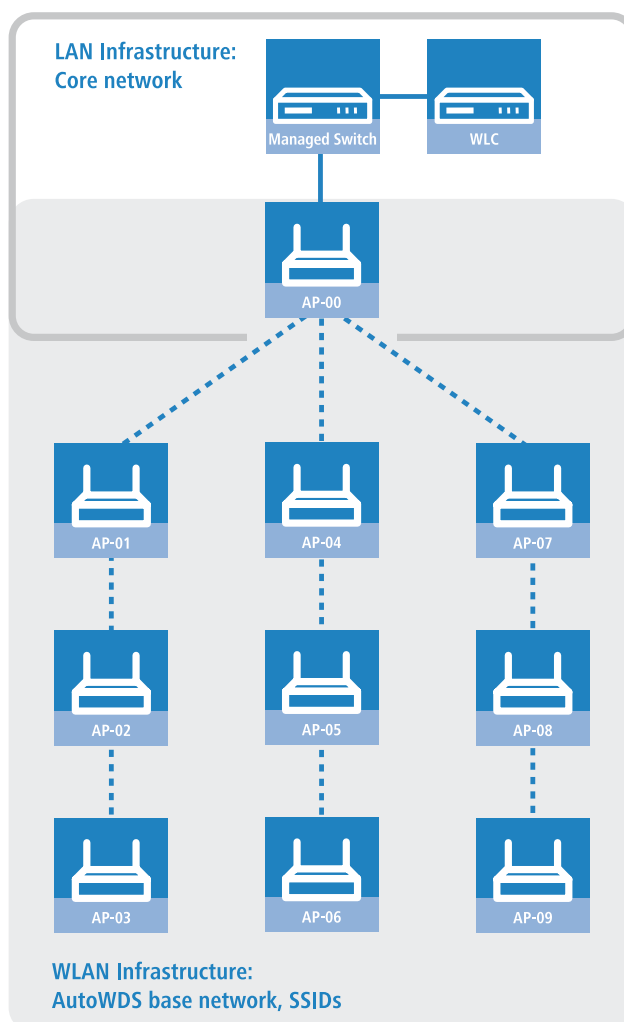
The following section shows you how to disable the automatic topology management on the WLC and create a manual P2P configuration. To configure the P2P links, you first assign unique names to each of the APs. Then link these names with the topology configuration and the physical WLAN interfaces being used. The chapter assumes that you have already performed the steps for the WLC under [Setup by means of preconfigured integration](#) on page 169, so that you can complete the basic configuration and enable AutoWDS on the WLC.



In general, we recommend a maximum of 3 hops for AutoWDS operations.

Changes to the initial scenario

The initial scenario is similar to the preconfigured integration. The entire infrastructure is based on dual-radio APs, which are arranged according to the illustration below. The managed WLAN initially consists of a single AP, which serves as the initial anchor AP for the unassociated APs.



Configuring the WLC

The following instructions describe how to disable the automatic topology management and the configuration of manual P2P links according to the scenario described under [Manual topology management](#) on page 172.

1. Open the configuration dialog in LANconfig and click on **WLAN controller > AP configuration > Access point table** to access the list of managed access points.

2. For each unassociated AP, enter the **MAC address** and a unique identifier under **AP name**. You will reference this name later in the topology configuration.

For the example scenario, the individual configuration entries are as follows:

Table 1: Configuring the unassociated APs in the access point table

Entry	MAC address	AP name
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

 The table entry AP-00 refers to your existing AP, which the unassociated APs use as an anchor AP.

3. Select the **WLAN profile** for which you have enabled AutoWDS.
By means of the corresponding WLAN profile, the APs automatically receive the settings for AutoWDS and hence for the P2P configuration.
4. Close the dialog window with **OK** and save the configuration to the device.
5. Log on to your device via WEBconfig or the console.
6. In the setup menu, navigate to the table **WLAN-Management > AP-Configuration > AutoWDS-Profiles**.
7. Edit the AutoWDS default profile by clicking on the entry **AUTOWDS_PROFILE**.

8. Change the **Topology-Management** parameter to **Manual** and save the settings by clicking on **Send**.
9. Navigate to the table **WLAN-Management > AP-Configuration > AutoWDS-Topology** and click on **Add**.
10. For each P2P pair, create a manual P2P configuration. The specified P2P link is always considered from the perspective of the slave AP.
 - a) In the field **AutoWDS-Profile**, specify the AutoWDS profile that applies for the manual P2P configuration, for example `AUTOWDS_PROFILE`.
 - b) Set the **Priority** of the P2P configuration to 0 (highest priority).
 - c) For the **Slave-AP-Name** and **Master-AP-Name**, enter the names of the APs according to your hierarchy.

For the example scenario, the individual configuration entries in the case of strict interface pairing are as follows:

Table 2: Configuring the P2P pairs in the AutoWDS topology table

Entry	Slave-AP-Name	Slave-AP-WLAN-Ifc.	Master-AP-Name	Master-AP-WLAN-Ifc.
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

- d) Under **Key** specify the WPA2 passphrase used by the P2P partners to encrypt the P2P link.

Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength. If you leave the field blank, the device automatically generates a passphrase with a length of 32 characters.

- e) Switch the entry **Enabled** to **Yes**.
- f) Save the entries by clicking on **Send**.

If APs were already connected, the WLC sends the new configuration to these APs, which triggers the reconfiguration procedure for each one. If no APs were connected, the WLC transmits the P2P configuration when the unassociated APs connect for the first time.

8.1.8 Redundant paths by means of RSTP

In combination with the rapid spanning tree protocol (RSTP), manual topology management allows you to set up redundant P2P links to improve the failover reliability of your entire AutoWDS base network. To do this, you must first enable RSTP in the Setup menu of each AP, because the WLC management settings do not include this part of the configuration. You can reduce the work involved by transmitting a script to all of the APs by means of the WLC script management.

The following steps show you how to do this. These steps assume that you have successfully set up an AutoWDS base network. After activation, RSTP automatically performs the path search.

1. Create a text file with the name `WLC_Script_1.lcs`.
2. Copy the following lines of code into the text file and save it.

```
# Script (8.890.0000 / 14.02.2013)

lang English
```

```

flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version      Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating            yes

flash Yes

# done
exit

```

3. Login to the WEBconfig interface of your WLC and navigate to **File management > Upload certificate or file**.
4. In the **File type** selection list, select **CAPWAP - WLC_Script_1.lcs** and use the **Browse** button to locate your script file. Then click on **Start upload**.
You can check if the file was successfully uploaded to the WLC in the Status menu under **File system > Contents**.
5. Navigate to the Setup menu item **WLAN management > Central firmware management > Script management** and click on **Add**.
6. Enter the **Profile** `AUTOWDS_PROFILE` and the **Name** `WLC_Script_1.lcs` to link the AutoWDS profile with the script name and to roll it out to the APs.
7. As described in section [Configuring the WLC](#) on page 173, assign unique names to the APs in the WLC and set up the manual P2P links.

You have now successfully completed the configuration.

8.1.9 Additions to the Status menu

AutoWDS

Indicates whether the connected client is an AutoWDS-capable AP in client mode, and which mode it is currently using to connect to your managed WLAN.

SNMP ID:

1.3.32.62

Telnet path:

Status > WLAN > Station-table

Possible values:

No

AutoWDS not enabled or not supported.

Preconfigured

AutoWDS is enabled; SSID and WPA2 passphrase are preconfigured.

Express

AutoWDS is enabled; SSID and WPA2 passphrase are not preconfigured.

AutoWDS

Indicates whether the detected WLAN is an AutoWDS base network.

SNMP ID:

1.3.34.42

Telnet path:**Status > WLAN > Scan-Results****Possible values:****No**
Yes**AutoWDS**

Indicates whether the detected WLAN is an AutoWDS base network.

SNMP ID:

1.3.44.42

Telnet path:**Status > WLAN > Competing-networks****Possible values:****No**
Yes**AutoWDS profile**

This table shows the settings for the AutoWDS profile received by your device from the WLC.

SNMP ID:

1.59.106

Telnet path:**Status > WLAN-Management****Name**

Name of the AutoWDS profile assigned to your device by the WLC.

SNMP ID:

1.59.106.1

Telnet path:**Status > WLAN-Management > AutoWDS-Profile**

SSID

The name of the logical WLAN network (SSID) that a managed access point 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 AutoWDS. The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc.

SNMP ID:

1.59.106.3

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Key

Displays the WPA2 passphrase used for the AutoWDS base network.

SNMP ID:

1.59.106.4

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Net-Number

Displays the internal representation of the common profile as a number.

SNMP ID:

1.59.106.5

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Active

Indicates whether the assigned AutoWDS is enabled or disabled.

SNMP ID:

1.59.106.6

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Possible values:

No
Yes

Allow-Express-Integration

Specifies whether your device allows the express integration of unassociated APs by means of the AutoWDS profile assigned to it.

SNMP ID:

1.59.106.7

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Possible values:

No
Yes

Time-till-Preconf-Scan

Displays the specified wait time after which the AP switches to client mode and scans for an AutoWDS base network according to the values from the preconfiguration (the SSID and passphrase that are stored in the AutoWDS profile). This occurs after all of the continuation times have expired. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase in order to subsequently perform the reconfiguration process.

Parallel to this process, the configured [wait time for the start of express integration](#) .

SNMP ID:

1.59.106.15

Telnet path:

Status > WLAN-Management > AutoWDS-Profile

Time-till-Express-Scan

Displays the specified wait time after which the AP switches to client mode and scans for any AutoWDS base networks, if all continuation times and also the [wait time for the start of the preconfigured integration](#) (if set) have expired. If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

SNMP ID:

1.59.106.16

Telnet path:**Status > WLAN-Management > AutoWDS-Profile****Interface-Pairing**

Indicates the type of interface pairings allowed by an anchor AP, based on the AutoWDS profile assigned to it.

The interface pairing influences the search by an AP in client mode for suitable anchor APs, while taking the participating WLAN interfaces into account. This specifies whether the unassociated AP has to connect to the equivalent physical WLAN interface of the anchor AP to integrate (i.e. with WLAN-1 to WLAN-1 or with WLAN-2 to WLAN-2), or whether it may pair with other physical interfaces. The definition of the interface pairing makes it possible to exclude invalid pairings, which may occur due to the assignment of different frequency bands due to the WLC configuration.

SNMP ID:

1.59.106.17

Telnet path:**Status > WLAN-Management > AutoWDS-Profile****Possible values:****Automatic**

The WLC checks if a problematic configuration can occur. If no problematic configuration occurs, it accepts the interface pairing via the anchor AP. Otherwise, the WLC rejects it and the unassociated AP must connect again.

Strict

An unassociated AP may only connect its physical WLAN interface X to the equivalent WLAN interface of the anchor AP.

Mixed

An unassociated AP may connect its physical WLAN interface X to any WLAN interface of the anchor AP.

AutoWDS-Topology

This table shows the topology or P2P configuration of the AutoWDS network provisioned to your device by the WLC. Using the information stored here, your device establishes the P2P link to its child slave APs and to its parent master APs.

SNMP ID:

1.59.107

Telnet path:**Status > WLAN-Management****AutoWDS profile**

Name of the AutoWDS profile that applies to the selected P2P configuration.

SNMP ID:

1.59.107.1

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Priority**

Shows the priority of a P2P connection from the perspective of a slave AP's physical WLAN interface.

SNMP ID:

1.59.107.2

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Slave-AP-Name**

Name of the AP with the role of slave in the WLC configuration.

SNMP ID:

1.59.107.3

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Slave-AP-WLAN-Ifc.**

Shows the physical WLAN interface used by the slave AP for the P2P link to the master AP.

SNMP ID:

1.59.107.4

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Possible values:**

Automatic
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC address of the slave AP.

SNMP ID:

1.59.107.5

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Master-AP-Name**

Name of the AP with the role of master in the WLC configuration.

SNMP ID:

1.59.107.6

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Master-AP-WLAN-Ifc.**

Shows the physical WLAN interface used by the master AP for the P2P link to the slave AP.

SNMP ID:

1.59.107.7

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Possible values:****Automatic**
WLAN-1
WLAN-2**Master-AP-WLAN-MAC**

MAC address of the master AP.

SNMP ID:

1.59.107.8

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Key**

WPA2 passphrase for the P2P link.

SNMP ID:

1.59.107.9

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Active**

Indicates whether the corresponding P2P configuration is enabled or disabled.

SNMP ID:

1.59.107.10

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Possible values:****No****Yes****Slave-Tx-Limit**

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from slave AP to master AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.59.107.12

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Master-Tx-Limit**

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from master AP to slave AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.59.107.13

Telnet path:**Status > WLAN-Management > AutoWDS-Topology**

Link-Loss-Timeout

Shows the time after which the AP tags the connection to its P2P partner as interrupted. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

SNMP ID:

1.59.107.14

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Continuation**

Shows the continuation time of the P2P configuration obtained from the WLC.

The continuation time mentioned above refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *reset time* until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

1.59.107.16

Telnet path:**Status > WLAN-Management > AutoWDS-Topology****Generated**

Indicates whether the received P2P configuration was generated automatically by the WLC or set manually in the WLC by the network administrator.

SNMP ID:

1.59.107.17

Telnet path:**Status > WLAN-Management > AutoWDS-Topology**

Possible values:

No
Yes

P2P index

This status value shows the static P2P port used by the APs (e.g. P2P-1-1).

SNMP ID:

1.59.107.19

Telnet path:

Status > WLAN-Management > AutoWDS-Topology

P2P-Role

This status value indicates whether your device assumes the role of slave or master for the listed P2P configuration.

SNMP ID:

1.59.107.20

Telnet path:

Status > WLAN-Management > AutoWDS-Topology

Possible values:

None
Slave
Master

AutoWDS operation

This menu displays the status values for the AutoWDS operation of your device.

SNMP ID:

1.59.109

Telnet path:

Status > WLAN-Management

Active scan mode

Indicates the AutoWDS integration mode currently used by your device, and whether the mode is active.

SNMP ID:

1.59.109.1

Telnet path:**Status > WLAN-Management > AutoWDS-Operation****Possible values:****No**

Your device is not currently searching for an AutoWDS base network.

Preconfigured

Your device is currently searching for the preconfigured AutoWDS base network.

Express

Your device is currently searching for any AutoWDS base network.

AutoWDS-Profile

This table shows the settings of the AutoWDS profiles that the WLC has assigned to the individual APs.

SNMP ID:

1.73.2.11

Telnet path:**Status > WLAN-Management > AP-Configuration****Name**

Name of of the AutoWDS profile assigned to the APs by the WLC.

SNMP ID:

1.73.2.11.1

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Commonprofile**

Then name of the WLAN profile assigned to the AutoWDS base network. All APs that have been assigned this WLAN profile support the AutoWDS base network at the same time.

SNMP ID:

1.73.2.11.2

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles**

SSID

The name of the logical WLAN network (SSID) that a managed access point 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 AutoWDS. The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc.

SNMP ID:

1.73.2.11.3

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Key

Displays the WPA2 passphrase used for the AutoWDS base network.

SNMP ID:

1.73.2.11.4

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Active

Indicates whether the corresponding AutoWDS is enabled or disabled.

SNMP ID:

1.73.2.11.6

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Possible values:

No
Yes

Allow-Express-Integration

Specifies whether the APs with the corresponding WLAN profile allow the express integration of unassociated APs via the AutoWDS base network.

SNMP ID:

1.73.2.11.7

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Possible values:

No
Yes

Topology-Management

Specifies which type of topology management the WLC uses for the respective AutoWDS profile.

For further information on this, see the corresponding setup parameters [2.37.1.15.8 Topology-Management](#) on page 211.

SNMP ID:

1.73.2.11.8

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Possible values:**Automatic**

The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.

semi-automatic

The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.

Manual

The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Slave-Tx-Limit

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from slave AP to master AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.11.10

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles

Master-Tx-Limit

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from master AP to slave AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.11.11

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Link-Loss-Timeout**

Shows the time after which the AP tags the connection to its P2P partner as interrupted. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

SNMP ID:

1.73.2.11.12

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Continuation**

Shows the continuation time of the automatically generated P2P configuration.

This continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

1.73.2.11.14

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Time-till-Preconf-Scan**

Displays the specified wait time after which the AP switches to client mode and scans for an AutoWDS base network according to the values from the preconfiguration (the SSID and passphrase that are stored in the AutoWDS profile). This occurs after all of the continuation times have expired. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase in order to subsequently perform the reconfiguration process.

Parallel to this process, the configured *wait time for the start of express integration* .

SNMP ID:

1.73.2.11.15

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Time-till-Express-Scan**

Displays the specified wait time after which the AP switches to client mode and scans for any AutoWDS base networks, if all continuation times and also the *wait time for the start of the preconfigured integration* (if set) have expired. If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

SNMP ID:

1.73.2.11.16

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Interface-Pairing**

Indicates the type of interface pairings allowed by an anchor AP, based on the AutoWDS profile assigned to it.

The interface pairing influences the search by an AP in client mode for suitable anchor APs, while taking the participating WLAN interfaces into account. This specifies whether the unassociated AP has to connect to the equivalent physical WLAN interface of the anchor AP to integrate (i.e. with WLAN-1 to WLAN-1 or with WLAN-2 to WLAN-2), or whether it may pair with other physical interfaces. The definition of the interface pairing makes it possible to exclude invalid pairings, which may occur due to the assignment of different frequency bands due to the WLC configuration.

SNMP ID:

1.73.2.11.17

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Possible values:****Automatic**

The WLC checks if a problematic configuration can occur. If no problematic configuration occurs, it accepts the interface pairing via the anchor AP. Otherwise, the WLC rejects it and the unassociated AP must connect again.

Strict

An unassociated AP may only connect its physical WLAN interface X to the equivalent WLAN interface of the anchor AP.

Mixed

An unassociated AP may connect its physical WLAN interface X to any WLAN interface of the anchor AP.

AutoWDS-Topology

This table shows manual components of the AutoWDS topology, or more specifically, the manual P2P links between the individual slave APs and master APs as sent to the individual APs by the WLC. The P2P links set up in this way should always be seen from the perspective of the slave AP's physical WLAN interface.

SNMP ID:

1.73.2.12

Telnet path:

Status > WLAN-Management > AP-Configuration

AutoWDS profile

Name of the AutoWDS profile that applies to the selected P2P configuration.

SNMP ID:

1.73.2.12.1

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Priority

Shows the priority of a P2P connection from the perspective of a slave AP's physical WLAN interface.

SNMP ID:

1.73.2.12.2

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Slave-AP-Name

Name of the AP with the role of slave in the WLC configuration.

SNMP ID:

1.73.2.12.3

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Slave-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the slave AP for the P2P link to the master AP.

SNMP ID:

1.73.2.12.4

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

Automatic
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC address of the slave AP.

SNMP ID:

1.73.2.12.5

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Master-AP-Name

Name of the AP with the role of master in the WLC configuration.

SNMP ID:

1.73.2.12.6

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Master-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the master AP for the P2P link to the slave AP.

SNMP ID:

1.73.2.12.7

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

Automatic
WLAN-1
WLAN-2

Master-AP-WLAN-MAC

MAC address of the master AP.

SNMP ID:

1.73.2.12.8

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Key

WPA2 passphrase for the P2P link.

SNMP ID:

1.73.2.12.9

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Active

Indicates whether the corresponding P2P configuration is enabled or disabled.



The WLC does not transmit disabled P2P configurations to the AP and, when evaluating the manual AutoWDS topology table in semi-automatic mode, it ignores disabled entries.

SNMP ID:

1.73.2.12.10

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

No
Yes

Slave-Tx-Limit

Shows the maximum transmission bandwidth which applies to the manual P2P link in the direction of transmission from slave AP to master AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.12.12

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Master-Tx-Limit

Shows the maximum transmission bandwidth which applies to the manual P2P link in the direction of transmission from master AP to slave AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.12.13

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Link-Loss-Timeout

Shows the time after which the AP tags the connection to its P2P partner as interrupted. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

SNMP ID:

1.73.2.12.14

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topology

Continuation

Shows the continuation time of the manual P2P configuration.

The continuation time mentioned above refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails

and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

1.73.2.12.16

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topology****Generated**

Indicates whether the P2P configuration was generated automatically by the WLC or set manually in the WLC by the network administrator.

SNMP ID:

1.73.2.12.17

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:****No**
Yes**State**

Displays the status of the corresponding P2P link.

SNMP ID:

1.73.2.12.18

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:****None**

The status of the corresponding P2P partners could not be recognized ('unknown').

Active

The corresponding P2P partners are connected to each other.

Idle

The corresponding P2P partners are not connected to each other.

AutoWDS-Auto-Topology

This table shows components of the AutoWDS topology that were automatically generated by the WLC, or more specifically, the generated P2P links between the individual slave APs and master APs as sent to the individual APs by the WLC. The P2P links generated in this way should always be seen from the perspective of the slave AP's physical WLAN interface.

SNMP ID:

1.73.2.13

Telnet path:**Status > WLAN-Management > AP-Configuration****AutoWDS profile**

Name of the AutoWDS profile that applies to the selected P2P configuration.

SNMP ID:

1.73.2.13.1

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology****Priority**

Shows the priority of a P2P connection from the perspective of a slave AP's physical WLAN interface.

SNMP ID:

1.73.2.13.2

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology****Slave-AP-Name**

Name of the AP with the role of slave in the WLC configuration.

SNMP ID:

1.73.2.13.3

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology**

Slave-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the slave AP for the P2P link to the master AP.

SNMP ID:

1.73.2.13.4

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Possible values:

Automatic
WLAN-1
WLAN-2

Slave-AP-WLAN-MAC

MAC address of the slave AP.

SNMP ID:

1.73.2.13.5

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Master-AP-Name

Name of the AP with the role of master in the WLC configuration.

SNMP ID:

1.73.2.13.6

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Master-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the master AP for the P2P link to the slave AP.

SNMP ID:

1.73.2.13.7

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Possible values:

Automatic
WLAN-1
WLAN-2

Master-AP-WLAN-MAC

MAC address of the master AP.

SNMP ID:

1.73.2.13.8

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Key

WPA2 passphrase for the P2P link.

SNMP ID:

1.73.2.13.9

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Active

Indicates whether the corresponding P2P configuration is enabled or disabled.



The WLC does not transmit disabled P2P configurations to the AP and, when evaluating the manual AutoWDS topology table in semi-automatic mode, it ignores disabled entries.

SNMP ID:

1.73.2.13.10

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Possible values:

No
Yes

Slave-Tx-Limit

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from slave AP to master AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.13.12

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Master-Tx-Limit

Shows the maximum transmission bandwidth which applies to the generated P2P link in the direction of transmission from master AP to slave AP (in kbps). The value 0 means 'unlimited'.

SNMP ID:

1.73.2.13.13

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Link-Loss-Timeout

Shows the time after which the AP tags the connection to its P2P partner as interrupted. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.

SNMP ID:

1.73.2.13.14

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology

Continuation

Shows the continuation time of the automatically generated P2P configuration.

This continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation

time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

1.73.2.13.16

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology****Generated**

Indicates whether the P2P configuration was generated automatically by the WLC or set manually in the WLC by the network administrator.

SNMP ID:

1.73.2.13.17

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Auto-Topology****Possible values:****No**
Yes**State**

Displays the status of the corresponding P2P link.

SNMP ID:

1.73.2.13.18

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:****None**

The status of the corresponding P2P partners could not be recognized ('unknown').

Active

The corresponding P2P partners are connected to each other.

Idle

The corresponding P2P partners are not connected to each other.

AutoWDS-Prof.-Errors

This table contains the error messages that occurred when an AutoWDS profile was assigned.

SNMP ID:

1.73.2.14

Telnet path:

Status > WLAN-Management > AP-Configuration

Index

Index number for table entries.

SNMP ID:

1.73.2.14.1

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Prof.-Errors

Name

Name of the AutoWDS profile where the error occurred.

SNMP ID:

1.73.2.14.2

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Prof.-Errors

Error

Content of the error message.

SNMP ID:

1.73.2.14.3

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Prof.-Errors

Network/AP-Parameters

WLAN and AP parameters pertaining to the error.

SNMP ID:

1.73.2.14.4

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Prof.-Errors****AutoWDS-Topo.-Errors**

This table contains the error messages that occurred when assigning a P2P configuration for AutoWDS.

SNMP ID:

1.73.2.15

Telnet path:**Status > WLAN-Management > AP-Configuration****Index**

Index number for table entries.

SNMP ID:

1.73.2.15.1

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors****AutoWDS profile**

Name of the AutoWDS profile where the error occurred.

SNMP ID:

1.73.2.15.2

Telnet path:**Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors****Priority**

Shows the priority of a P2P connection from the perspective of a slave AP's physical WLAN interface.

SNMP ID:

1.73.2.15.3

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Slave-AP-Name

Name of the AP with the role of slave in the WLC configuration.

SNMP ID:

1.73.2.15.4

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Slave-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the slave AP for the P2P link to the master AP.

SNMP ID:

1.73.2.15.5

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Slave-AP-WLAN-MAC

MAC address of the slave AP.

SNMP ID:

1.73.2.15.6

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Master-AP-Name

Name of the AP with the role of master in the WLC configuration.

SNMP ID:

1.73.2.15.7

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Master-AP-WLAN-Ifc.

Shows the physical WLAN interface used by the master AP for the P2P link to the slave AP.

SNMP ID:

1.73.2.15.8

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Master-AP-WLAN-MAC

MAC address of the master AP.

SNMP ID:

1.73.2.15.

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

Error

Content of the error message.

SNMP ID:

1.73.2.15.

Telnet path:

Status > WLAN-Management > AP-Configuration > AutoWDS-Topo.-Errors

AutoWDS-Integration

Indicates whether the unassociated AP established the CAPWAP connection via LAN or WLAN and which integration mode is being used.

SNMP ID:

1.73.9.3.7

Telnet path:

Status > WLAN-Management > AP-Status > New-AP

Possible values:

None

CAPWAP via LAN

Express

CAPWAP via WLAN

Preconfigured

CAPWAP via WLAN

8.1.10 Additions to the Setup menu

AutoWDS

This table contains the local factory settings of your device for the search for and the authentication at an AutoWDS base network. You use the timeout times to specify whether your device employs preconfigured integration, express integration, or a stepped combination of both.

As long as your device still has not received any AutoWDS settings from the WLC, the device uses the default settings specified here. However, as soon as your device receives an AutoWDS profile from a WLC, that configuration has a higher priority until the WLC revokes the configuration via CAPWAP or you reset the AP.



The parameters specified here exclusively effect the initial login of an unassociated slave AP to a master AP for a subsequent search for a WLC. They do not affect the P2P links to a master AP that are set up later; your device uses the WLC configuration it obtains then.

You can check whether the device has received an AutoWDS configuration from the WLC with the status table **AutoWDS-Profile** (SNMP-ID 1.59.106).

SNMP ID:

2.59.4

Telnet path:**Setup > WLAN-Management****Active**

Switches the AutoWDS function on your device on/off. In the disabled state, the device does not attempt to autonomously integrate itself into a managed WLAN and also does not perform scans for an active AutoWDS network.

SNMP ID:

2.59.4.1

Telnet path:**Setup > WLAN-Management > AutoWDS****Possible values:**

No
Yes


Default:

No

Preconf-SSID

Enter the SSID of the AutoWDS base network here. Your device will search here for a preconfigured integration. AutoWDS must be enabled and the [wait time until the preconfigured search](#) has to be set to higher than 0.

After the wait time expires, the device switches all physical WLAN interfaces to client mode and starts the search for the SSID. If the device finds a matching SSID, it attempts to authenticate with the WPA2 passphrase entered for the corresponding WLAN.


 The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.

SNMP ID:

2.59.4.2

Telnet path:**Setup > WLAN-Management > AutoWDS****Possible values:**Max. 32 characters from `[A-Z][0-9]@{ | }~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty***Preconf-Key**

Specify the WPA2 passphrase that your device uses for authentication on the preconfigured AutoWDS base network.

 The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.

SNMP ID:

2.59.4.3

Telnet path:**Setup > WLAN-Management > AutoWDS****Possible values:**Max. 63 characters from `[A-Z][a-z][0-9]#@{ | }~!$%&'()*+,-./:;<=>?[\]^_.`**Default:***empty***Time-till-Preconf-Scan**

Specify the wait time after which the AP switches to client mode and scans for an AutoWDS base network based on the corresponding values in the preconfiguration (the SSID and passphrase that are stored locally). This assumes that there are no configuration parts from a WLC available. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase and then perform the configuration procedure.

Parallel to this process, the configured [wait time for the start of express integration](#) is counted down.



The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.

SNMP ID:

2.59.4.4

Telnet path:**Setup > WLAN-Management > AutoWDS****Possible values:**

0 ... 4294967295 Seconds

Special values:**0**

This value disables the wait time and the preconfigured integration procedure. The device immediately starts to count down the wait time for starting the express integration.

Default:

0

Time-till-Express-Scan

Specify the wait time after which the AP switches to client mode and scans for any AutoWDS base networks. This assumes that there no configuration parts from a WLC available and the *wait time for the start of the preconfigured integration* (if set) has expired. If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

SNMP ID:

2.59.4.5

Telnet path:**Setup > WLAN-Management > AutoWDS****Possible values:**

0 ... 4294967295 Seconds

Special values:**0**

This value disables the wait time and the preconfigured integration procedure.

Default:

1

Configuration delay

This parameter specifies the delay time after which an AP executes the configuration update just rolled out by the WLC.

The delay time is primarily relevant for APs, which you are integrating into your managed WLAN via a point-to-point link (e.g. with AutoWDS). This reduces the probability of undelivered configuration updates leading only to a partial configuration of your network, so making the other APs unreachable. The higher you set the delay time, the more likely it is that all unassociated APs will receive the configuration update rolled out by the WLC.

A value of at least 1 second per (AutoWDS-) hop is recommended.

SNMP ID:

2.37.1.3.7

Telnet path:

Setup > WLAN-Management > AP-Configuration > Commonprofiles

Possible values:

0 ... 4294967295 Seconds

Special values:

0

This value disables the delayed configuration update.

Default:

0

AutoWDS-Profile

This table contains the parameters for the AutoWDS profile which you assign to the individual access points by means of the WLAN profile in order to implement meshed networks. The AutoWDS profile groups the settings and limits to form the P2P topology and of the AutoWDS base network.

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.

SNMP ID:

2.37.1.15.1

Telnet path:

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

Possible values:

Max. 31 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.

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 AutoWDS. 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.

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

Key

Enter the WPA2 passphrase for the AutoWDS base network supported by a managed AP. Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

SNMP ID:

2.37.1.15.4

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

min. 8 characters; max. 63 characters from

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

Specify whether the AutoWDS is enabled or disabled for the selected profile. Inactive profiles are not transmitted by the WLC to an AP.

SNMP ID:

2.37.1.15.6

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Possible values:****No****Yes****Default:**

No

Allow-Express-Integration

Here you specify whether the APs of the corresponding WLAN profile permit the express integration of unassociated APs via the AutoWDS base network. If you enable this setting, the affected master APs send an additional vendor-specific identifier in their beacons to signal the availability of this integration option to unassociated APs.

If you enable AutoWDS and prohibit express integration, the AutoWDS base network allows only the preconfigured integration of unassociated or already associated APs in client mode.

SNMP ID:

2.37.1.15.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles**

Possible values:**No**

The AutoWDS base network allows only the preconfigured integration for unassociated clients.

Yes

The AutoWDS base network allows preconfigured integration as well as express integration of unassociated APs.

Default:

No

Topology-Management

Enter which type of topology management the WLC uses for the respective AutoWDS profile.

Due to the assignment of the WLAN profile by the WLC, the slave APs simultaneously receive information about the topology of the meshed network. The topology results directly from the hierarchy of the P2P connections established between the APs. The two affected WLAN interfaces form a P2P pairing for this: The physical WLAN interface of the unassociated AP becomes the P2P slave; that of the selected anchor AP becomes the P2P master.

By default, the WLC accepts the automatic calculation of the topology where one slave AP generally connects with the nearest master AP. Calculated in real-time, the topology is recorded by the WLC in the status table

AutoWDS-Auto-Topology (SNMP-ID 1.73.2.13). If you use semi-automatic or manual management, you define the static P2P links in the setup table **AutoWDS-Topology**. For this, you specify the relationships between the individual master APs and slave APs in a manner similar to a normal P2P link.



The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.

SNMP ID:

2.37.1.15.8

Telnet path:

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

Possible values:**Automatic**

The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.

semi-automatic

The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.

Manual

The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Default:

Automatic

Slave-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from slave AP to master AP. The setting only affects P2P connections which the WLC has generated automatically.

SNMP ID:

2.37.1.15.10

Telnet path:

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

Possible values:

0 ... 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

Master-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from master AP to slave AP. The setting only affects P2P connections which the WLC has generated automatically.

SNMP ID:

2.37.1.15.11

Telnet path:

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

Possible values:

0 ... 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

Link-Loss-Timeout

Specify the time after which the AP tags the connection to its P2P partner as interrupted. The setting only affects P2P connections which the WLC has generated automatically. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.



The link-loss timeout is independent of the other timeouts. In the interests of stable connectivity of the overall AutoWDS base network, we recommend that you do not use a value less than the default value.

SNMP ID:

2.37.1.15.12

Telnet path:

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

Possible values:

0 ... 4294967295 Seconds

Default:

4

Continuation

Define the continuation time of the automatically generated P2P configuration.

The continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the [preset time](#) until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

2.37.1.15.14

Telnet path:

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

Possible values:

0 ... 9999 Minutes

Special values:

0

The AP immediately switches off its physical WLAN interface(s) as soon as contact to the WLC is lost. The device immediately deletes its configuration parameters so that the WLC must re-transmit them when reestablishing the connecting.

Select this setting to protect the configuration parameters that are relevant for security from unauthorized access and misuse (e.g., in case the AP is stolen).

9999

The configuration parameters are permanently stored in the device. The AP continues to operate regardless how long the contact to the WLC is lost.

Default:

0

Time-till-Preconf-Scan

Specify the wait time after which the AP switches to client mode and scans for an AutoWDS base network using the values in the preconfiguration (the SSID and passphrase that are stored in the AutoWDS profile), if all continuation times have expired. If the AP finds a matching SSID, the device attempts to authenticate with the respective WPA2 passphrase in order to subsequently perform the reconfiguration process.

Parallel to this process, the configured *wait time for the start of express integration* is counted down.



The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.

SNMP ID:

2.37.1.15.15

Telnet path:

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

Possible values:

0 ... 4294967295 Seconds

Special values:

0

This value disables preconfigured integration on the respective AP.

Default:

60

Time-till-Express-Scan

Specify the wait time after which the AP switches to client mode and scans for any AutoWDS base networks, if all continuation times and also the *wait time for the start of the preconfigured integration* have expired (if set). If the AP finds a suitable SSID, the device attempts to authenticate at the WLAN in order to subsequently perform the reconfiguration process. The device authenticates with an express pre-shared key, which is hard-coded in the firmware.

SNMP ID:

2.37.1.15.16

Telnet path:

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

Possible values:

0 ... 4294967295 Seconds

Special values:

0

This value disables express integration on the corresponding AP.

Default:

0

Interface-Pairing

Specify which type of interface pairings an anchor AP allows based on the AutoWDS profile assigned to it. The setting is mainly relevant for devices with more than one physical WLAN interface.

The interface pairing influences the search by the AP for suitable anchor APs in client mode, taking the participating WLAN interfaces into account. This specifies whether the unassociated AP has to connect to the equivalent physical WLAN interface of the anchor AP to integrate (i.e. with WLAN-1 to WLAN-1 or with WLAN-2 to WLAN-2), or whether it may pair with other physical interfaces. The definition of the interface pairing makes it possible to exclude invalid pairings, which may occur due to the assignment of different frequency bands by the WLC configuration.

For instance, the anchor APs of your AutoWDS base network might be operating with the physical WLAN interfaces WLAN-1 set to the 2.4GHz band and WLAN-2 on the 5GHz band: If, for example, an unassociated AP is using a physical WLAN interface to search on both frequency bands, the interface pairing **Strict** prevents it from selecting WLAN-1 in the 5 GHz band in order to connect with the WLAN-2 of the anchor AP. Although this connection would be legitimate for the WLC configuration, the different radio settings would make it impossible to establish the P2P connection. The unassociated AP would lose the connection and would have to start a reconfiguration process.

If, on the other hand, both physical WLAN interfaces transmit on the same band, the interface pairing **Mixed** is also permissible, as the problematic configuration described above cannot occur.

SNMP ID:

2.37.1.15.17

Telnet path:

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

Possible values:

Automatic

The WLC checks if a problematic configuration can occur. If no problematic configuration occurs, it accepts the interface pairing via the anchor AP. Otherwise, the WLC rejects it and the unassociated AP must connect again.

Strict

An unassociated AP may only connect its physical WLAN interface X to the equivalent WLAN interface of the anchor AP.

Mixed

An unassociated AP may connect its physical WLAN interface X to any WLAN interface of the anchor AP.

Default:

Automatic

Slave-Radio-Multi-Hop

This parameter determines whether connection requests from unassociated APs can be accepted on the same physical WLAN interface that the anchor APs in your AutoWDS base network are using as slaves to connect to the master.



Disabling this parameter can improve the stability and the load distribution within your AutoWDS base network. As a result of this however, single-radio APs can no longer function as anchor APs for extending your AutoWDS base network, and are the end of a hierarchy branch.

SNMP ID:

2.37.1.15.18

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Possible values:****No**

An anchor AP never accepts connection requests from unassociated APs on the same physical WLAN interface that it is using to connect to the AutoWDS base network as a slave. WLAN multi-hops are only possible on devices with two managed physical WLAN interfaces.

Yes

An anchor AP also accepts connection requests from unassociated APs on the same physical WLAN interface that it is using to connect to the AutoWDS base network as a slave. WLAN multi-hops are possible on devices with one or two managed physical WLAN interfaces.

Single-radio-AP-only

Case-specific setting:

The setting **Yes** applies to devices with one physical WLAN interface.

The setting **No** applies to devices with more than one physical WLAN interface.

Default:

No

Band

Specify the frequency band used by the APs for the AutoWDS base network.

SNMP ID:

2.37.1.15.19

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Profiles****Possible values:****2.4GHz/5GHz**

Both the 2.4-GHz and the 5-GHz bands are used for AutoWDS base network.

2.4GHz

Only the 2.4-GHz band is used for the AutoWDS base network.

5GHz

Only the 5-GHz band is used for the AutoWDS base network.

Default:

5GHz

Band

This parameter specifies whether or not the APs broadcast the SSID of the AutoWDS base network in their beacons.

SNMP ID:

2.37.1.15.20

Telnet path:

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

Possible values:**Yes**

The APs broadcast the SSID of the AutoWDS base network. The network is visible for other WLAN clients.

No

The APs hide the SSID of the AutoWDS base network. The network is invisible for other WLAN clients.

Default:

No

AutoWDS-Topology

In this table you specify the manual elements of the AutoWDS topology; or, more specifically, the P2P routes between the individual slave APs and master APs. The device only processes this table if you activated manual or semi-automatic [topology management](#).

SNMP ID:

2.37.1.16

Telnet path:

Setup > WLAN-Management > AP-Configuration

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-Profile**.

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

Default:*empty***Priority**

Enter the priority of a P2P connection from the viewpoint of the physical WLAN interface of the slave AP.



This setting is currently a placeholder as the evaluation of the priorities has not been implemented yet. Please always enter the value 0 for the priority.

SNMP ID:

2.37.1.16.2

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

0 ... 4294967295

Default:*empty***Slave-AP-Name**

Enter the name of the AP which takes on the role of the slave.

SNMP ID:

2.37.1.16.3

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:****Name** from **Setup > WLAN-Management > AP-Configuration > AutoWDS-Profile.**Max. 31 characters from `[A-Z][0-9]@{ | }~!$%&' ()+- , / : ; <=> ? [\] ^ _ .`**Default:***empty***Slave-AP-WLAN-Ifc.**

Here you set the physical WLAN interface used by the slave AP for the P2P link to the master AP.

SNMP ID:

2.37.1.16.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

Selection from the available physical WLAN interfaces. |

Default:

WLAN-1

Master-AP-Name

Enter the name of the AP which takes on the role of the master.

SNMP ID:

2.37.1.16.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

Name from **Setup > WLAN-Management > AP-Configuration > AutoWDS-Profile**.

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

Default:

empty

Master-AP-WLAN-Ifc.

Here you set the physical WLAN interface used by the master AP for the P2P link to the slave AP.

SNMP ID:

2.37.1.16.7

Telnet path:

Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology

Possible values:

Selection from the available physical WLAN interfaces. |

Default:

WLAN-1

Key

You can also enter an individual WPA2 passphrase for the P2P connection. If you leave the field empty, the device automatically generates a passphrase with a length of 32 characters.

SNMP ID:

2.37.1.16.9

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

min. 8 characters; max. 63 characters from

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

Specify whether the P2P configuration is enabled or disabled for the selected AutoWDS profile.



The WLC does not transmit disabled P2P configurations to the AP and ignores disabled entries when evaluating the manual AutoWDS topology table in semi-automatic mode

SNMP ID:

2.37.1.16.10

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:****No****Yes****Default:**

No

Slave-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from slave AP to master AP. This setting only affects P2P connections that you created manually.

SNMP ID:

2.37.1.16.12

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

0 ... 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

Master-Tx-Limit

Optionally, limit the maximum transmission bandwidth which applies to the P2P connections in the direction of transmission from master AP to slave AP. This setting only affects P2P connections that you created manually.

SNMP ID:

2.37.1.16.13

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

0 ... 4294967295 kbps

Special values:

0

This value disables the bandwidth limit.

Default:

0

Link-Loss-Timeout

Specify the time after which the AP tags the connection to its P2P partner as interrupted. This setting only affects P2P connections that you created manually. If the device has marked a P2P link as interrupted, its physical WLAN interface starts scanning the WLAN for the lost P2P partner.



The link-loss timeout is independent of the other timeouts. In the interests of stable connectivity of the overall AutoWDS base network, we recommend that you set the timeout to 4 seconds as a minimum.

SNMP ID:

2.37.1.16.14

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

0 ... 4294967295 Seconds

Special values:

0

For this value, the WLC retrieves the specified value for **Link-Loss-Timeout** from **Setup > WLAN-Management > AP-Configuration > AutoWDS-Profile**.

Default:

0

Continuation

Define the continuation time of the manual P2P configuration.

The continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards this part of the WLC configuration. If the standalone continuation time is specified as 0, the AP immediately discards this part of the configuration.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the timeout periods for the preconfigured and express integrations—as a basis to count down the *preset time* until the start of the automatic (re-)configuration for the preconfigured integration.

SNMP ID:

2.37.1.16.16

Telnet path:**Setup > WLAN-Management > AP-Configuration > AutoWDS-Topology****Possible values:**

0 ... 9999 Minutes

Special values:

0

The AP immediately switches off its physical WLAN interface(s) as soon as contact to the WLC is lost. The device immediately deletes its configuration parameters so that the WLC must re-transmit them when reestablishing the connecting.

Select this setting to protect the configuration parameters that are relevant for security from unauthorized access and misuse (e.g., in case the AP is stolen).

9999

The configuration parameters are permanently stored in the device. The AP continues to operate regardless how long the contact to the WLC is lost.

Default:

0

8.2 IP-dependent auto configuration and tagging of APs

The easiest way to manage all of the APs that you add to a managed network is to use a flat hierarchy. However, in the largest installations with hundreds of APs across several locations, this type of organization quickly becomes confusing and creates a high level of administrative effort. Setting up **Assignment groups** can help to simplify the management

of distributed APs. The WLC can automatically configure each new AP based on the IP addresses it receives. Manual assignment of an IP parameter profile, a WLAN profile and a Client-steering profile by an administrator is no longer required.

The following describes how an assignment group is used when an unassociated AP registers with a central WLC: After the new APs are installed on site (e.g. at a company or branch network), they try to establish a connection to the specified WLC and obtain a configuration via CAPWAP. The WLC detects the connection requests and, for each new AP, it checks the access point table for a suitable AP profile (e.g., the default profile) and/or whether a suitable assignment group has been defined. If one or more configuration options are available, the WLC checks them for the following states:

1. For a new AP there is an assignment group but no AP profile. In this case, the WLC assigns the profile specified in the assignment group to the new AP.
2. For a new AP there is both an assignment group as well as an AP profile. In this case, the WLC ignores the assignment group and assigns the profile defined in the AP profile to the new AP.
3. For a new AP, there is an AP profile but no assignment group. The behavior is the same as point (2).

If a new AP has neither an AP profile nor an assignment group, the WLC issues an alarm to notify the administrator of the incorrect configuration.

After successful group assignment, the WLC automatically creates an AP profile for every new AP in the access point table. In the **Groups** field, the WLC references the assignment group used when it added the new AP.

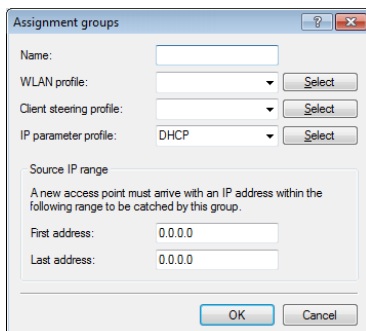
 An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups should overlap, LCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status > WLAN-Management > AP-Configuration**.

The group field also gives you the option of assigning individually definable tags to an AP. For example, these **Tag groups** can be used to act as filter criteria in order for the WLC to restrict the actions it performs to a selection of APs.

8.2.1 Setting up assignment groups for IP-dependent auto configuration

The following tutorial shows you how you setup assignment groups on a WLC for the IP-dependent automatic configuration of new APs.

1. Open the configuration dialog for your device and select **WLAN controller > AP configuration > Assignment groups**
2. Click on **Add** to create a new group.



3. Enter under **Name** a unique descriptor for the assignment group, for example, *Berlin_branch*.
4. Select the **WLAN profile** that the WLC automatically assigns to a new AP if the IP address of the new AP is within the source IP range.
5. Enter the **IP parameter profile** if the new AP should receive a manual network configuration. Otherwise, leave the value as **DHCP**, whereby the AP automatically gets a network configuration from the DHCP server. The DHCP server must be configured to do this.

If you wish to assign a manual network configuration in which a new AP receives a different IP address, you specify the appropriate address range in the **IP parameter profile** under **Address assignment pool**.

6. **Optional:** Specify a **Client-steering profile** in order to forward future WLAN clients to the ideal AP in case there are several new APs within transmission range.



If you activate client steering, this must be activated for every AP in the managed infrastructure. Refer to section [Client-steering by the WLC](#) on page 265 for further information on this.

7. Enter the start and end of the **Source IP range** relevant to the assignment group.
A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.
8. Close all dialog windows with **OK** and save the configuration to your device.

From now on, the WLC assigns the profiles referenced in the assignment groups to all new APs. The LCOS console can now provide you with information about the categorization, see [Overview of CAPWAP parameters with the show command](#) on page 235.

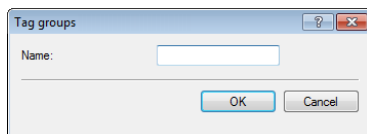


Please ensure that the access point table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.

8.2.2 Setting up tag groups for the detailed selection of APs

The following tutorial shows you how a tag group can be added to an AP configuration on a WLC. To do this, you first create a tag group and then assign it to a WLAN profile.

1. Open the configuration dialog for your device and select **WLAN controller > AP configuration > Tag groups**
2. Click on **Add** to create a new group.



3. Under **Name** you enter the new tag and save the entry with **OK**.
4. Navigate to the dialog with **WLAN controller > AP configuration > Access point table**.
5. Select an existing access point profile with **Edit** or add a new one, if necessary.
6. Under **Groups** select the tag group(s) created earlier.
Multiple tag groups can be specified in a comma-separated list.



The tag groups are independent of the assignment groups, the assignment of which is specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. The manual allocation of an assignment group has no effect on the AP configuration, which is in line with the state check described under [IP-dependent auto configuration and tagging of APs](#) on page 222. The only effects are on the filtering in the command `show capwap group` at the console



The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

7. Close all dialog windows with **OK** and save the configuration to your device.

From now on the WLC gives the tags in the edited WLAN profile to those APs that received it.

8.2.3 Additions to the Status menu

Netw.-Prof.-Errors

This table contains the error messages that occurred when assigning the network profiles.

SNMP ID:

1.73.2.5

Telnet path:**Status > WLAN-Management > AP-Configuration****Index**

Index number for table entries.

SNMP ID:

1.73.2.5.1

Telnet path:**Status > WLAN-Management > AP-Configuration > Netw.-Prof.-Errors****Name**

Name of the network profile.

SNMP ID:

1.73.2.5.2

Telnet path:**Status > WLAN-Management > AP-Configuration > Netw.-Prof.-Errors****Error**

Content of the error message.

SNMP ID:

1.73.2.20.3

Telnet path:**Status > WLAN-Management > AP-Configuration > Netw.-Prof.-Errors****AP-Conf.-Errors**

This table contains messages about any configuration errors that occurred in the access point table under **Setup > WLAN-Management > AP-Configuration > Access-Points**.

SNMP ID:

1.73.2.8

Telnet path:**Status > WLAN-Management > AP-Configuration****Index**

Index number for table entries.

SNMP ID:

1.73.2.8.1

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors****Name**

Name of the AP with the error.

SNMP ID:

1.73.2.8.2

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors****Error**

Content of the error message.

SNMP ID:

1.73.2.8.3

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors****Profile**

Name of the WLAN profile where the error occurred.

SNMP ID:

1.73.2.8.4

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors**

MAC address

MAC address of the AP.

SNMP ID:

1.73.2.8.5

Telnet path:

Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors

Group

Name of the assignment group where the error occurred.

SNMP ID:

1.73.2.8.6

Telnet path:

Status > WLAN-Management > AP-Configuration > AP-Conf.-Errors

AP-Intranet-Errors

This table contains the error messages that occurred when assigning the IP parameter profiles.

SNMP ID:

1.73.2.10

Telnet path:

Status > WLAN-Management > AP-Configuration

Index

Index number for table entries.

SNMP ID:

1.73.2.10

Telnet path:

Status > WLAN-Management > AP-Configuration > AP-Intranet-Errors

Name

Name of the IP parameter profile.

SNMP ID:

1.73.2.10.2

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Intranet-Errors****Error**

Content of the error message.

SNMP ID:

1.73.2.10.3

Telnet path:**Status > WLAN-Management > AP-Configuration > AP-Intranet-Errors****Config-Assignment-Groups**

This table shows the assignment groups that the WLC has transmitted to the individual access points.

SNMP ID:

1.73.2.19

Telnet path:**Status > WLAN-Management > AP-Configuration****Name**

Name of the assignment group.

SNMP ID:

1.73.2.19.1

Telnet path:**Status > WLAN-Management > AP-Configuration > Config-Assignment-Groups****Profile**

Name of the WLAN profile that the WLC automatically assigned to an unassociated AP via the assignment group.

SNMP ID:

1.73.2.19.2

Telnet path:

Status > WLAN-Management > AP-Configuration > Config-Assignment-Groups

AP-Intranet

Name of the IP parameter profile that the WLC automatically assigned to an unassociated AP via the assignment group.

SNMP ID:

1.73.2.19.3

Telnet path:

Status > WLAN-Management > AP-Configuration > Config-Assignment-Groups

IPv4-Reference-Pool-Start

Start of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

SNMP ID:

1.73.2.19.4

Telnet path:

Status > WLAN-Management > AP-Configuration > Config-Assignment-Groups

IPv4-Reference-Pool-End

End of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

SNMP ID:

1.73.2.19.5

Telnet path:

Status > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Groups-Config-Errors

This table contains messages about any configuration errors that occurred within the assignment groups specified under **Setup > WLAN-Management > AP Configuration > Config-Assignment-Groups**.

SNMP ID:

1.73.2.20

Telnet path:**Status > WLAN-Management > AP-Configuration****Index**

Index number for table entries.

SNMP ID:

1.73.2.20.1

Telnet path:**Status > WLAN-Management > AP-Configuration > Groups-Config-Errors****Group**

Name of the assignment group.

SNMP ID:

1.73.2.20.2

Telnet path:**Status > WLAN-Management > AP-Configuration > Groups-Config-Errors****Error**

Content of the error message.

SNMP ID:

1.73.2.20.3

Telnet path:**Status > WLAN-Management > AP-Configuration > Groups-Config-Errors****Tag groups**

This table shows the tag groups that the WLC has transmitted to the individual access points.

SNMP ID:

1.73.2.21

Telnet path:**Status > WLAN-Management > AP-Configuration**

Name

Name of the tag group.

SNMP ID:

1.73.2.21.1


Telnet path:


Status > WLAN-Management > AP-Configuration > Tag-Groups

8.2.4 Additions to the Setup menu

Groups

Using this parameter, you optionally assign the corresponding AP profile to one or more tag groups. If you edit an AP profile, this parameter may additionally contain those assignment groups assigned by the WLC to the corresponding AP during the IP-dependent auto-configuration. For more information, see the Reference Manual.

 The tag groups are independent of the assignment groups that are specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. Manually assigning an assignment group has no effect on the AP configuration. The only effects are on the filtering in the command `show capwap group` at the console.

 The manual addition of assignment groups for filtering purposes is not recommended. You should create separate tag groups instead.

SNMP ID:

2.37.1.4.24

Telnet path:

Setup > WLAN-Management > AP-Configuration > Base stations

Possible values:

Name from **Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups**. Multiple entries can be provided in a comma-separated list.

Name from **Setup > WLAN-Management > AP-Configuration > Tag-Groups**. Multiple entries can be provided in a comma-separated list.

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

Default:

empty

IPv4-Config-Pool-Start

The start of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the access-point table.

SNMP ID:

2.37.1.9.9

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

0.0.0.0 ... 255,255,255,255

Default:*empty***IPv4-Config-Pool-End**

The end of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the access-point table.

SNMP ID:



2.37.1.9.10

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

0.0.0.0 ... 255,255,255,255

Default:*empty***Config-Assignment-Groups**

This table contains the assignment groups. Based on these, the WLC automatically assigns the network configuration, a WLAN profile and a client-steering profile to the unassociated APs. For this purpose, you specify an IP address range for each individual assignment group. For example, in a centrally managed WLAN you can use IP address ranges to automatically assign a location-specific configuration to unassociated APs (e.g., Branch A, Branch B, etc.).

-
-  An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups should overlap, LCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status > WLAN-Management > AP-Configuration**.
 -  Please ensure that the access point table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.
-

SNMP ID:

2.37.1.18

Telnet path:**Setup > WLAN-Management > AP-Configuration**

Name

Name of the assignment group which you reference from other tables.

SNMP ID:

2.37.1.18.1

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

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

Default:

empty

Profile

Name of the WLAN profile that the WLC automatically assigns to an unassociated AP via the assignment group.

SNMP ID:

2.37.1.18.2

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

Name from **Setup > WLAN-Management > AP-Configuration > Commonprofiles.**

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

Default:

empty

AP-Intranet

Name of the IP parameter profile that the WLC automatically assigns to an unassociated AP via the assignment group.

SNMP ID:

2.37.1.18.3

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

Name from **Setup > WLAN-Management > AP-Configuration > AP-Intranets.**

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

Special values:**DHCP**

The AP retrieves its network configuration via DHCP.

Default:

empty

IPv4-Reference-Pool-Start

Start of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

SNMP ID:

2.37.1.18.4

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

0.0.0.0 ... 255,255,255,255

Default:

empty

IPv4-Reference-Pool-End

End of the IPv4 address range for the corresponding assignment group. A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

SNMP ID:

2.37.1.18.5

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

0.0.0.0 ... 255,255,255,255

Default:

empty

Client-Steering-Profile

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.

SNMP ID:

2.37.1.18.6

Telnet path:**Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups****Possible values:****Name** from **Setup > WLAN-Management > Client-Steering > Profiles**Max. 31 characters from `[A-Z][0-9]@{ }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`**Default:***empty***Tag groups**

This table contains the tag groups that the WLC automatically assigns to the APs belonging to a WLAN profile. Among other things, tag groups allow actions performed on the WLC to be restricted to a selection of APs.

SNMP ID:

2.37.1.20

Telnet path:**Setup > WLAN-Management > AP-Configuration****Name**

You use this parameter to specify the name of the tag being created.

SNMP ID:

2.37.1.20.1

Telnet path:**Setup > WLAN-Management > AP-Configuration > Tag-Groups****Possible values:**Max. 31 characters from `[A-Z][0-9]@{ }~!$%&'() +- , / : ; < = > ? [\] ^ _ .`**Default:***empty***8.2.5 Enhancements to command-line commands****Overview of CAPWAP parameters with the show command**

The following information about the CAPWAP service can be viewed using the command line:

Table 3: Overview of all CAPWAP parameters with the show command

Parameters	Meaning
-addresses [<IfcNum>]	Shows the address tables of an individual or all WLC tunnels. In the case of an individual WLC tunnel, enter for the <IfcNum> the number of logical WLC tunnel interface, for example 10.
-groups	Shows the information for an individual or all available assignment/tag groups.

You can supplement the command `show capwap groups` with the parameters listed below, which control the scope of the displayed information:

Table 4: Overview of all CAPWAP group parameters with the show command

Parameters	Meaning
all	Shows the names configured in the setup menu and the device's internal names for all assignment/tag groups as well as the default groups that were set up. The default group represents an internal group which contains all APs.
<group1> <group2> <...>	Shows all APs of the respective assignment/tag groups.
-l <location>	Shows all APs of the respective location.
-c <country>	Shows all APs of the respective country.
-i <city>	Shows all APs of the respective city.
-s <street>	Shows all APs of the respective street.
-b <building>	Shows all APs of the respective building.
-f <floor>	Shows all APs of the respective floor.
-r <room>	Shows all APs of the respective room description.
-d <device>	Shows all APs that have the specified device name.
-a <antenna>	Shows all APs which have the specified antenna number.
-v <firmware>	Shows all APs which have the specified firmware. To do this, enter the version number for <firmware> followed by the build number, e.g., 9.00.0001.
-x <firmware>	Shows all APs with a firmware version lower than the one installed on the current device.
-y <firmware>	Shows all APs with a firmware version the same or lower than the one installed on the current device.
-z <firmware>	Shows all APs with a firmware version higher than the one installed on the current device.
-t <firmware>	Shows all APs with a firmware version the same or higher than the one installed on the current device.
-n <intranet>	Shows all APs with an IP belonging to the specified Intranet address.
-p <profile>	Shows all APs that have been assigned with the specified WLAN profile.
rmgrp <group1 intern_name> <group2 intern_name> ...	Deletes the group(s) with the specified internal names from the memory of the device. Use this command to free up the main memory if too large a number of groups is degrading the performance of the device. The entry in the setup menu is unaffected by this action.
resetgrps	Deletes all groups except the default group.

For location information the device evaluates the information entered under **Location** in the access point table. The following field names are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

For instance, the location entry `co=Germany, ci=Aachen` allows you to list all of the managed APs in Aachen from the console of the WLC with the command `+show capwap group -i Aachen`.

Example commands

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion ...
```

8.3 Automatic selection of the 2.4-/5-GHz mode

As of LCOS 9.00, the configuration of the WLAN physical parameters on WLCs and also on APs now includes the option of allowing the AP to select a suitable 2.4-/5-GHz mode.

■ 2.4-GHz mode / 5-GHz mode

Here you specify the wireless standard(s) that the physical WLAN interface provides to the WLAN clients.

In the 2.4-GHz and the 5-GHz frequency bands, there are several different wireless standards that an AP can use for transmission. In the 2.4-GHz frequency band, these were to date the standards IEEE 802.11b, IEEE 802.11g and IEEE 802.11n; in the 5-GHz frequency band, the standards are IEEE 802.11a, IEEE 802.11n and IEEE 802.11ac. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.




Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

For example, if there are only 802.11n-enabled devices in your WLAN, it is recommended to select greenfield mode (**802.11n only**): By doing this you prevent login of slower clients which would otherwise act as a brake on the network.

By selecting a compatibility mode, you are able to achieve the best possible data rates without excluding slower WLAN clients (e.g., for 2.4 GHz **802.11g/b/n (mixed)**; for 5 GHz **802.11a/n (mixed)**). In compatibility mode, a physical WLAN interface works according to the fastest standard, but reverts to a slower standard if a slower WLAN client logs on to the network. When using 802.11b, you can select whether the physical WLAN interface should exclusively support 11-Mbps mode or also the older 2-Mbps mode (... **(2-Mbps-compatible)**).

For APs operating according to the 802.11g standard you can optionally increase the data transfer speeds up to 108Mbps. In what is referred to as Turbo mode, an AP simultaneously uses two neighboring free channels for the radio transmission. With an AP in the 108Mbps Turbo mode, the only WLAN clients that can establish a connection to this AP are those also operating with the 108Mbps Turbo mode.

-  Turbo mode is associated with the 802.11g standard, although it was never officially adopted by the IEEE. The technology represents the proprietary extensions of various chipset manufacturers who also market this technology under the name "802.11g+" or "802.11g++". Turbo mode is therefore exclusively available on APs with pure 802.11g hardware.

If you leave the selection of the 2.5/5-GHz mode up to the device with the **Automatic** setting, the selection of the best mode depends on the frequency band in use and the capabilities of the device hardware:

- In the 2.4-GHz mode, the automatic setting results in either **802.11g/b/n (mixed)** or **802.11 g/b (mixed)**.
- In the 5-GHz mode, the automatic setting results in either **802.11a/n/c (mixed)**, **802.11 a/n (mixed)**, or **54Mbps mode**.

In principle, according to 802.11n APs in the 2.4-GHz frequency band are backwards compatible to the IEEE 802.11b and IEEE 802.11g standards. Only the 802.11n-specific functions are not available for 802.11n hardware operated in 802.11b or 802.11g mode. However, this backwards compatibility is not available in the 5-GHz frequency band: The affected 802.11n devices must explicitly support 802.11a.

8.3.1 Additions to the Status menu

2.4-GHz mode

This status value indicates the 2.4-GHz mode being operated by the WLAN module of the managed APs.

SNMP ID:

1.73.2.2.6

Telnet path:

Status > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:

11bg mixed

802.11g/b (mixed)

11b only

802.11b only (11Mbps)

11g only

802.11g only (54Mbps)

108Mbps

802.11g++ (108Mbps mode / turbo mode)

11bgn mixed

802.11g/b/n

11gn mixed

802.11g/n

Greenfield

802.11n only (greenfield mode)

Auto

Automatic

5GHz mode

This status value indicates the 5-GHz mode being operated by the WLAN module of the managed APs.

SNMP ID:

1.73.2.2.7

Telnet path:

Status > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:**Normal**

802.11 g (54Mbps mode)

108Mbps

802.11g++ (108Mbps mode / turbo mode)

11an mixed

802.11a/n (mixed)

Greenfield

802.11n only (greenfield mode)

11anac mixed

802.11a/n/ac (mixed)

11nac mixed

802.11n/ac (mixed)

11ac only

802.11ac only

Auto

Automatic

8.3.2 Additions to the Setup menu

2.4-GHz mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 2.4-GHz frequency band. Depending on the device type and frequency band, you have the choice of operating an AP exclusively in one specific mode, or you can set one of the compatibility modes.



Please observe that clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

SNMP ID:

2.37.1.2.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:**11bg mixed**

802.11g/b (mixed)

11b only

802.11b only (11Mbps)

11g only

802.11g only (54Mbps)

108Mbps

802.11g++ (108Mbps mode / turbo mode)

11bgn mixed

802.11g/b/n

11gn mixed

802.11g/n

Greenfield

802.11n only (greenfield mode)

AutoAutomatic. In the 2.4-GHz mode, automatic selection provides either **11bgn-mixed** or **11bg-mixed**.**Default:**

Auto

5GHz mode

Here you specify the radio standard(s) that the physical WLAN interface provides to the WLAN clients in the 5-GHz frequency band. Depending on the device type and frequency band, you have the choice of operating an AP exclusively in one specific mode, or you can set one of the compatibility modes.



Please observe that clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

SNMP ID:

2.37.1.2.7

Telnet path:**Setup > WLAN-Management > AP-Configuration > Radioprofiles****Possible values:****Normal**

802.11 g (54Mbps mode)

108Mbps

802.11g++ (108Mbps mode / turbo mode)

11an mixed

802.11a/n (mixed)

Greenfield

802.11n only (greenfield mode)

11anac mixed

802.11a/n/ac (mixed)

11nac mixed

802.11n/ac (mixed)

11ac only

802.11ac only

Auto

Automatic. In the 5-GHz mode, automatic selection provides either **11anac-mixed**, **11an-mixed**, or **Normal**.

Default:

Auto

8.4 WLC cluster

If you are operating multiple WLCs in your network, you can collect these devices into a cluster. The APs in a managed WLAN are no longer managed by a single, central WLC but by multiple, synchronized WLCs. For large networks in particular, a WLC cluster provides numerous advantages:

- Automatic network “load balancing” between the individual APs and WLCs;
- Increased failover reliability through the provision of backup WLCs (“hot standby”) and automatic redistribution of the APs in the case of a WLC failure;
- Setting up a certificate hierarchy: Management of certificates by a central certification authority (CA), represented either by a master WLC or an external station (such as a server).

As of LCOS 9.00, the cluster function received numerous enhancements described below.

8.4.1 WLC tunnel for internal communication

The use of WLC tunnels is essential for a WLC cluster. The WLCs in the WLC cluster use this tunnel to communicate with one another and keep their status information aligned. With the feature extensions as of LCOS 9.00, the way that LCOS deals with WLC tunnels is also improved:

- WLCs are able to find one another automatically.
- You have the option to statically configure WLC tunnels.
- WLCs disconnect a WLC tunnel only after a timeout.
- WLC tunnels can be switched on or off globally.

The settings for the WLC tunnels and other WLCs (remote WLCs) are located in the section **WLAN controller > General > WLC cluster**. The setting **WLC tunnel active** allows you to disable the usage of WLC tunnels, which in effect causes the clustering feature to be switched off.

Additions to the Setup menu

WLC cluster

This menu contains the settings for the data connections and status connections between multiple WLCs (WLC cluster).

SNMP ID:

2.37.34

Telnet path:**Setup > WLAN-Management****WLC-Tunnel-active**

Using this parameter, you can enable or disable the WLC tunnel used for WLC clustering. This indirectly switches the cluster functionality for the corresponding WLC on or off.

SNMP ID:

2.37.34.6

Telnet path:**Setup > WLAN-Management > WLC-Cluster****Possible values:****No**

WLC cluster tunnels on the device are disabled.

Yes

WLC cluster tunnels on the device are enabled.

Default:

No

WLC-Discovery

This table is used for each of your IPv4 networks to enable or disable the automatic search for WLCs in the same local network.



Enter the addresses of WLCs that are not on the local network (remote WLCs) into the static WLC list (SNMP ID [2.37.34.3](#)). The automatic search does not find remote WLCs.

SNMP ID:

2.37.34.4

Telnet path:**Setup > WLAN-Management > WLC-Cluster****Network**

Specify the name of the IPv4 network, in which the WLC automatically searches for remote WLCs.

SNMP ID:

2.37.34.4.1

Telnet path:**Setup > WLAN-Management > WLC-Cluster > WLC-Discovery****Possible values:****Network name** from **Setup > TCP-IP > Network-list**Max. 16 characters from `[A-Z][0-9]@{ }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`**Default:***empty***Enabled**

Using this option, you can enable or disable the automatic search for remote WLCs in the selected network.

The automatic search for remote WLCs is one way of establishing the connection between several WLCs. If you disable this option, the WLC cannot automatically connect to another WLC over the corresponding network, even if the use of WLC tunnels in general has been enabled. An alternative is to specify the remote sites in the static WLC list.

SNMP ID:

2.37.34.4.2

Telnet path:**Setup > WLAN-Management > WLC-Cluster > WLC-Discovery****Possible values:****Yes****No****Default:****No****Port**

Specify the port used for the automatic search for remote WLCs.

SNMP ID:

2.37.34.4.3

Telnet path:**Setup > WLAN-Management > WLC-Cluster > WLC-Discovery****Possible values:**

0 ... 65535

Special values:

0

The device uses default port 1027.

Default:

0

WLC-Data-Tunnel-active

This option activates or disables the use of data tunnels (L3 tunnels) between multiple WLCs. This allows you to extend a transparent layer-2 network as an overlay network across the remote WLCs.



Be sure never to bridge the corresponding WLC tunnels if the individual WLCs are located in the same broadcast domain. Otherwise you will create a switching loop that will overload your network.



In order to maximize data throughput and the network performance, you can forward the AP data traffic directly into the LAN. In this case there is no need for a layer-3 tunnel between the WLCs even when they are in different layer-2 networks.

SNMP ID:

2.37.34.2

Telnet path:**Setup > WLAN-Management > WLC-Cluster****Possible values:****Yes**

The WLC connects to remote WLCs via a layer-3 tunnel.

No

The WLC does not connect to remote WLCs via a layer-3 tunnel.

Default:

No

Static WLC list

In this table, you define the static IPv4 addresses of the remote WLCs which your WLC connects to. As an alternative, this table can also be used to bypass the search of the local network as performed by the **WLC Discovery** table.

If you connect to a remote WLC at a static IPv4 address, your WLC initially establishes a control tunnel to this remote site. If you have enabled the data tunnel option, your WLC automatically establishes a data tunnel to this remote site.



The WLCs can only interconnect if they have a certificate from the same certificate hierarchy.

SNMP ID:

2.37.34.3

Telnet path:**Setup > WLAN-Management > WLC-Cluster****IP address**

Here you specify the IPv4 address of the remote WLC to which your WLC establishes a connection.

SNMP ID:

2.37.34.3.1

Telnet path:**Setup > WLAN-Management > WLC-Cluster > Static-WLC-List****Possible values:**

0.0.0.0 ... 255,255,255,255

Default:*empty***Loopback-Addr.**

Here you can optionally specify another address (name or IP) used by your device to identify itself to the remote WLC 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 sender address set here is a loopback address, then even for masked remote stations, this address will be used **unmasked** !

SNMP ID:

2.37.34.3.2

Telnet path:**Setup > WLAN-Management > WLC-Cluster > Static-WLC-List****Possible values:**Max. 16 characters from `[A-Z][0-9]@{ | } ~ ! $ % & ' () + - , / : ; < = > ? [\] ^ _ .`**Special values:****Name of the IP network (ARF network), whose address should be used.****INT** for the address of the first Intranet**DMZ** for the address of the first DMZ

If the lists of IP networks or loopback addresses contains an interface named 'DMZ', then the device selects the associated IP address instead!

LB0...LB15 for one of the 16 loopback addresses or its name
Any IPv4 address

Default:

empty

Port

Specify the port used by your WLC to establish a data tunnel to the remote WLC.

SNMP ID:

2.37.34.3.3

Telnet path:

Setup > WLAN-Management > WLC-Cluster > Static-WLC-List

Possible values:

0 ... 65535

Special values:

0

The device uses default port 1027.

Default:

0

8.4.2 Setting up a CA hierarchy

In order to operate multiple WLAN controllers in a WLC cluster, they must all have identical configurations. This also includes the certificates used within the WLC cluster. The solution lies in establishing a certificate hierarchy, also known as a CA hierarchy: This involves defining the CA of a WLC as the root-CA. The other WLCs retrieve this certificate for their (sub-) CA.

The following scenario shows you the configuration steps which are necessary for setting up a CA hierarchy. As examples, the configuration is done using two WLCs:

- WLC-MAIN represents the device with the root-CA;
- WLC-SUB is the device which obtains a certificate from the root-CA in order to issue further certificates as a sub-CA.

Configuring the root-CA

The following section describes how to set up a root CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup > Certificates > SCEP-CA > CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

Example: /CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE

3. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Operating** to **Yes**.

You have now completed the configuration of the root CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly.

Configuring the sub-CA

The following section describes how to set up a sub-CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Root-CA** to **No**.
3. Navigate to the menu **Setup > Certificates > SCEP-CA > CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

Example: `/CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE`

4. Switch to the menu **Setup > Certificates > SCEP-CA > Sub-CA** and enter the distinguished name of the root-CA under the parameter **CADN**.

Example: `/CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE`

5. For the parameter **Challenge-Pwd**, enter the challenge password that is stored on WLC-MAIN under **Setup > Certificates > SCEP-CA**.
6. Enter the URL (address) to the root CA in the **CA-Url-address** parameter.
If another WLC with the LCOS operating system provides the root CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached. Example:
`http://192.168.1.1/cgi/bin/pkiclient.exe`.
7. Optional: Specify the **Ext-Key-Usage** and **Cert-Key Usage** to restrict the functions of the sub-CA. For more information, see the Menu Reference Guide.
8. Set the parameter **Auto-generated-request** to **Yes** to activate the sub-CA.
9. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Operating** to **Yes** to enable the CA server with SCEP.

You have now completed the configuration of the sub-CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly. The hierarchy of certificates must be visible here: The WLC first displays the certificate of the root CA and then the certificate of the sub-CA.

Additions to the Setup menu

Root CA

This parameter specifies whether or not the CA of the relevant WLC represents the root CA.

SNMP ID:

2.39.2.11

Telnet path:

Setup > Certificates > SCEP-CA

Possible values:

No
Yes

Default:

Yes

CA-Path-Length

Use this parameter to specify the maximum permitted length of the hierarchy of sub-CAs below the root CA (length of the "Chain of Trust").

A value of 1 means that only the root CA can issue certificates for sub-CAs. Sub-CAs themselves cannot issue certificates to other sub-CAs and so extend the "Chain of Trust". When set to 0, not even the root CA is capable of issuing certificates for sub-CAs. In this case, the root CA can only sign end-user certificates.

SNMP ID:

2.39.2.12

Telnet path:

Setup > Certificates > SCEP-CA

Possible values:

0 ... 65535

Default:

1

Sub-CA

This menu contains all of the settings you need for retrieving a certificate for the sub-CA.

SNMP ID:

2.39.2.13

Telnet path:

Setup > Certificates > SCEP-CA

Auto-generated-request

With this parameter you specify whether the WLC forwards the request for a certificate for the sub-CA automatically to the root CA.

SNMP ID:

2.39.2.13.1

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

No
Yes

Default:

No

CADN

Enter the certificate authority distinguished name (CADN) of the parent CA (e.g. the root CA) where the WLC obtains the certificate for the sub-CA.

SNMP ID:

2.39.2.13.2

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

Max. 100 characters from `#[A-Z][a-z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_`~`

Default:

empty

Challenge-Pwd

Set the challenge password used by the sub-CA to obtain the certificate from the parent CA (e.g., the root CA). You set the challenge password for the parent CA in LCOS in the menu **Setup > Certificates > SCEP-CA > Client-Certificates**.

SNMP ID:

2.39.2.13.3

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

Max. 100 characters from `#[A-Z][a-z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_`~`

Default:

empty

Ext-Key-Usage

With this item you specify additional designated purposes for the key usage. The extended key usage consists of a comma-separated list of key usages. These indicate the purposes for which the certificate's public key may be used.

The purposes are entered either as their abbreviations or the point-separated form of the OIDs. Although any OID can be used, only a few of them are meaningful (see below). Specifically the following PKIX, NS and MS values are significant and can be entered in any combination:

Table 5: Extended usage purposes: Meaningful abbreviations

Value	Meaning
serverAuth	SSL/TLS Web server authentication
clientAuth	SSL/TLS Web client authentication
codeSigning	Code signing
emailProtection	E-mail protection (S/MIME)
timeStamping	Trusted time stamping
msCodeInd	Microsoft personal code signing (Authenticode)
msCodeCom	Microsoft commercial code signing (Authenticode)
msCTLSign	Microsoft trust list signing
msSGC	Microsoft server gated crypto
msEFS	Microsoft encrypted file system
nsSGC	Netscape server gated crypto
critical	By setting this restriction, the key usage extension must always be observed. If the extension is not supported, the certificate is rejected as invalid.

Table 6: Extended usage purposes: Meaningful OIDs for WLAN switching

Device	OID
WLAN controller	1.3.6.1.5.5.7.3.18
Managed AP	1.3.6.1.5.5.7.3.19

Sample input: `critical,clientAuth,1.3.6.1.5.5.7.3.19`

SNMP ID:

2.39.2.13.4

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

Comma separated list of the abbreviations and/or OIDs listed above. Max. 100 characters from

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

Default:

empty

Cert-Key-Usage

Specify the intended application of the specified certificates (key usage). The WLC queries the certificates for the sub-CA only for the purpose indicated.

Table 7: Usage: Abbreviation

Value	Meaning
digitalSignature	
nonRepudiation	
keyEncipherment	
dataEncipherment	
keyAgreement	
keyCertSign	
cRLSign	
encipherOnly	
decipherOnly	
critical	By setting this restriction, the key usage extension must always be observed. If the extension is not supported, the certificate is rejected as invalid.

Sample input: digitalSignature, nonRepudiation

SNMP ID:

2.39.2.13.5

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

Comma separated list of the abbreviations listed above. Max. 100 characters from

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

Default:

empty

CA-Url-Address

Specify the URL (address) where the parent CA is to be found. If another WLC with the LCOS operating system provides the CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached.

SNMP ID:

2.39.2.13.8

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible values:

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

Default:

`http://127.0.0.1/cgi-bin/pkiclient.exe`

Restart

This action causes a restart of the sub-CA. Execute this action after performing configuration changes on the sub-CA.

SNMP ID:

`2.39.2.13.9`

Telnet path:

Setup > Certificates > SCEP-CA > Sub-CA

Possible arguments:

none

8.4.3 Enabling/disabling CAPWAP in the WLC

In order to operate multiple WLAN controllers in a cluster, they must all have identical configurations. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master controller's configuration.

Additions to the Setup menu

CAPWAP-enabled

Enables or disabled the CAPWAP service on your device.

In order to operate several WLAN controllers in the group (cluster), all involved devices must have an identical configuration. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master controller's configuration.

SNMP ID:

`2.37.36`

Telnet path:

Setup > WLAN-Management

Possible values:

No
Yes

Default:

Yes

8.4.4 Finding the ideal WLC

The algorithms implemented in LCOS ensure that the APs are intelligently distributed between the individual WLCs. This allows the APs to equally distribute the network load between all of the WLCs in a cluster, or to select an alternative WLC if one should fail. For this, an AP first sends out a discovery request on the network to identify all available WLCs. The WLCs then respond with a discovery response which an AP uses to create a prioritized list of WLCs. This AP prioritizes the list based on various criteria.

An AP works through the different criteria sequentially: If multiple WLCs appear to be ideal candidates after applying a criterion, the AP uses the next criteria to prioritize. This process ends when a WLC finally identifies just one WLC as being ideal after the prioritization described in the following.

Criteria for prioritization

- **Specificity of the AP configuration:** An AP evaluates whether a WLC can provide it with a configuration, and whether this contains a specific AP profile or a default profile. The AP prioritizes a specific AP profile as highest, followed by a default profile. If a profile is missing, it is given the lowest priority.
- **The preference value:** The AP evaluates the preference value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

If there still remain several WLCs which are considered to be ideal, the prioritization process continues by evaluating the connection status and the type of selection process (automatically vs. manually initiated):

- When the **calculation is triggered for the first time**, an AP calculates a weighted value for each of the remaining WLCs by taking the number of APs connected to each WLC and comparing this with the maximum possible number of APs (**license usage**). Ultimately, the ideal WLC is taken as that with the lowest license usage.



If a WLC has reached the maximum possible number of AP connections (license quota exhausted), an AP no longer considers the affected WLC for the current selection.

- In the case of **automatic checking** of the ideal AP distribution, an AP stays with the WLC it is connected to if this WLC is included in the list of the remaining WLCs. Otherwise, a **randomized algorithm** causes the AP to select an arbitrary AP.
- In the case of a **manually triggered check**, a **randomized algorithm** ensures that the APs distribute the available license quotas as evenly as possible across the network.

Additions to the Setup menu

Preference

This parameter specifies a priority value used by an AP to set the priority of a WLC within a WLC cluster. The AP evaluates the priority value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

SNMP ID:

2.37.37

Telnet path:

Setup > WLAN-Management

Possible values:

0 ... 255

Default:

0

8.4.5 Determining the ideal AP distribution

The identification of the ideal AP distribution in a WLC cluster and any redistribution that may be triggered by it occur automatically. Every AP automatically performs the *Finding the ideal WLC* process at irregular intervals between 30 and 60 minutes. If the result of the process is positive for the WLC which is already connected, no redistribution takes place. If a different WLC has a higher priority, the AP attempts to connect to this WLC.

However, as an administrator you can use LANmonitor to manually trigger a calculation of the ideal AP distribution and the resulting redistribution of the APs (see *Manually initiate ideal AP distribution* on page 254).

8.4.6 Manually initiate ideal AP distribution

The following steps show you how to start the recalculation of an ideal distribution, and if necessary to trigger a redistribution.

1. Start LANmonitor and select a WLC.
2. Navigate to the menu item **Wireless LAN > Active APs**.
3. Open the context menu on any AP and select **Start WLC search on APs**.

All APs then evaluate the ideal distribution for themselves and, if necessary, they associates with a better WLC.

Additions to the Setup menu

Trigger-WLC-rediscovery-on-WTPs

With this action, you command all of the managed APs to calculate the ideal distribution of the APs in the WLC cluster. The result of this calculation may cause the APs to be redistributed.

SNMP ID:

2.37.34.5

Telnet path:

Setup > WLAN-Management > WLC-Cluster

Possible arguments:

none

8.5 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.

These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in LCOS. If you cannot wait until the individual services request new certificates, a manual resolution requires deleting the SCEP files from the LCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, LCOS performs the necessary steps automatically.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup > Certificate > SCEP-CA > CA certificate**. This action generates a ZIP file within the LCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password,

unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **File management > Download certificate or file > SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **File management > Upload certificate or file > SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.



If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action *2.39.2.2.11 Restore-certificates-from-Backup* in order for the device to restore the certificate record.

8.6 Automatic restart of managed APs after firmware update

As of LCOS 9.00 you have the option in the WEBconfig menu **Extras > Load firmware in managed APs** to automatically start the APs after the manual upload of a new firmware version.

8.6.1 Load firmware in managed AP

This menu item is only available on WLAN controllers (WLCs).

On this page, you have the option of using remote access to manually update the firmware on an AP managed by the WLC. For example, this might make sense in order to test firmware on selected APs before using it productively. To do this, select an AP by its MAC address and select the appropriate firmware file. Next click on **Start upload** to load the firmware in the AP.



Please note that this process disables the firmware management in the AP table for the selected AP. This prevents the WLC from automatically uploading a different firmware version. Firmware management can be re-enabled at any time in the setup menu under **WLAN-Management > AP-Configuration > Manage-firmware**.

In order for the access point to use the loaded firmware, you must subsequently perform a restart. By enabling the setting **Restart AP after updating the firmware** you trigger an automatic restart as soon as the firmware upload is completed.

8.7 Automatic search for alternative WLCs

As of LCOS 9.00, an AP no longer attempts to reconnect to the last known WLC in case of a disconnection. Instead, the AP searches in the network for an available WLC which corresponds to the criteria for the [Finding the ideal WLC](#).

8.8 U-APSD configurable by WLC

As of LCOS 9.00 you have the additional option of enabling WLCs to configure the power-saving mechanism (U-)APSD for individual SSIDs.

8.8.1 Additions to the Status menu

APSD

Indicates whether the APSD power saving mode is enabled for the corresponding logical WLAN network.

SNMP ID:

1.73.2.1.42

Telnet path:**Status > WLAN-Management > AP-Configuration > Networkprofiles****Possible values:****Yes****No****APSD**

Indicates whether the APSD power saving mode is enabled for the corresponding logical WLAN network.

SNMP ID:

1.53.103.42

Telnet path:**Status > WLAN-Management > Network-profiles****Possible values:****Yes****No**

8.8.2 Additions to the Setup menu

APSD

Activates APSD power saving for the corresponding logical WLAN network.



Please note that in order for the APSD function to work in a logical WLAN, QoS must be activated on the device. APSD uses mechanisms in QoS to optimize power consumption for the application.

SNMP ID:

2.37.1.1.42

Telnet path:**Setup > WLAN-Management > AP-Configuration > Networkprofiles****Possible values:****Yes****No****Default:****Yes**

8.9 Group-related radio field optimization

The LANCOM WLAN controllers can form groups of access points based on location information, device properties or network structure. This grouping can also be used as a basis for radio field optimization. Instead of performing a radio field optimization either for all access points or just for one of them, you can address all of the access points within a building tract, with a particular name, or with a particular firmware version.

You can address the groups by using the appropriate group parameters in WEBconfig, LANmonitor and from the command line:

```
do /Setup/WLAN-Management/start optimization <Group>
```

The access points can be filtered with the following group-parameter options:

-g <Group name>

Access points belonging to the group. Multiple group names can be separated by commas.

-l <Location>

Access points with the matching setting for location.



The combination of -l and one of the location options -c to -r is not useful.

-c <Country>

Access points with the matching country.

-i <City>

Access points with the matching city.

-s <Street>

Access points with the matching street.

-b <Building>

Access points with the matching building.

-f <Floor>

Access points with the matching floor.

-r <Room>

Access points with the matching room.

-d <Device name>

Access points with the matching device name.

-a <Antenna>

Access points with the matching number of antennas.



A combination of the options -d and -a is not useful.

-v <Firmware>

Access points with this firmware version only.

-x <Firmware>

Access points with a firmware version lower than that specified here.

-y <Firmware>

Access points with a firmware version lower than or equal to that specified here.

-z <Firmware>

Access points with a firmware version higher than that specified here.

-t <Firmware>

Access points with a firmware version higher than or equal to that specified here.



Combinations are possible, e.g. to address access points with a firmware version between two versions.

-n <Intranet address>

Access points located on the intranet with the address specified here.

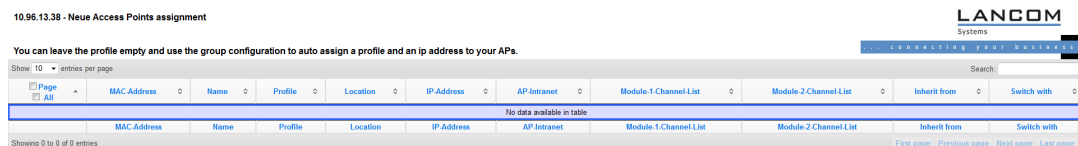
-p <Profile name>

Access points included in the WLAN profile specified here.

8.10 Adding new APs with the WEBconfig Setup Wizard

As of LCOS 9.00, WLCs have a revised Setup Wizard **Assign Access Points to Profiles**, which makes it easier to add new APs via WEBconfig. Just a few mouse clicks with the new Setup Wizard allows you to

- Make a targeted search for a new AP;
- Accept one or more new APs at the same time;
- Assign a WLAN profile or a channel list to a new AP;
- Allow a new AP to inherit the configuration from an accepted AP;
- To exchange the configuration in a new AP for that of an accepted missing AP. When exchanging a configuration, the new AP receives the complete configuration of the accepted missing AP (except for its MAC address). When the new AP has been integrated, the WLC then deletes the configuration of the accepted missing AP.



Click **Accept AP** to include the new AP with its new settings into the network.



If you have allowed an AP to be configured via assignment groups, there is no need for any further settings for this AP in the Setup Wizard. The WLC automatically assigns the settings for the appropriate groups to the AP.

8.10.1 Additions to the Status menu

Accept-AP

This action triggers the integration of a new AP. The action accepts different arguments depending on the firmware version of the device. A MAC address must be specified in any case; further arguments are optional.

Syntax used in versions before LCOS 9.00

```
[<-c>] <WTP-MAC> [<Profile>] [<Name>] [<IP>] [<Netmask>] [<Gateway>]
```

Syntax used in versions as of LCOS 9.00

```
<WTP-MAC> [ <WTP-MAC-2> ... <WTP-MAC-n> ] [-c] [-l <Location>] [-p <Profile>] [-i <IP>] [-n <Name>] [-m <Netmask>] [-g <Gateway>] [-1 <Wlan1Channels>] [-2 <Wlan2Channels>]
```



If you define multiple MAC addresses, the device ignores the arguments [-i <IP>] and [-n <Name>].

SNMP ID:

2.37.7

Telnet path:**Setup > WLAN-Management****Possible arguments:****-c**

The WLC generates a configuration entry for the AP.

-l <Location>

The WLC supplements the AP configuration with the specified location.

We recommend that you store each location in the device as a unique field value pair so that, for example, the filter function in LCOS can be used at the console. The following field identifiers are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

-p <Profile>

The WLC supplements the AP configuration with the specified WLAN profile.

-i <IP>

The WLC supplements the AP configuration with the specified IPv4 address.

-n <Name>

The WLC supplements the AP configuration with the specified device identifier.

-m <Netmask>

The WLC supplements the AP configuration with the specified netmask.

-g <Gateway>

The WLC supplements the AP configuration with the specified gateway address (IPv4).

-1 <Wlan1Channels>

The WLC supplements the AP configuration with the first channel list.

-2 <Wlan2Channels>

The WLC supplements the AP configuration with the second channel list.

8.11 Maximum bandwidth can be adjusted for each WLAN module

As of LCOS 9.00, you are able to set the maximum bandwidth for each WLAN module.

It is no longer possible to force 40MHz channel bundling.

Changes to WLCs

Max. channel bandwidth

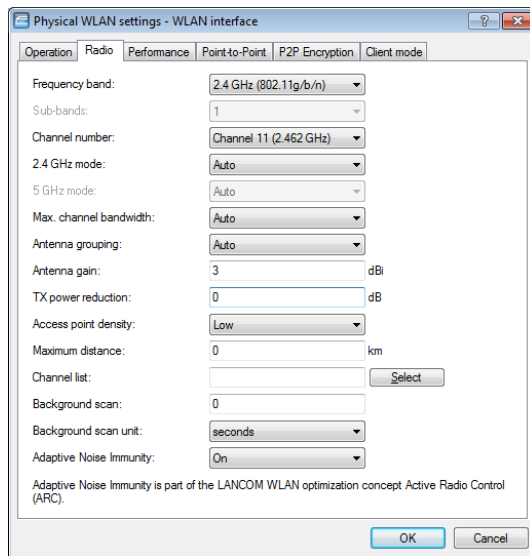
Enter how and to what extent the AP specifies the channel bandwidth for the physical WLAN interface(s). The following values are possible:

- **Automatic:** The access point automatically detects the maximum channel bandwidth (default).
- **20MHz:** The access point uses channels bundled at 20 MHz.
- **40MHz:** The access point uses channels bundled at 40MHz.
- **80MHz:** The access point uses channels bundled at 80MHz.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Changes to stand-alone APs



8.11.1 Additions to the Status menu

Channel bandwidths

Indicates which channel bandwidths are supported by the corresponding WLAN client.

SNMP ID:

1.3.32.66

Telnet path:

Status > WLAN > Station-table

Possible values:

20MHz

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidths

Indicates which channel bandwidths are supported by the corresponding remote station.

SNMP ID:

1.3.34.44

Telnet path:**Status > WLAN > Scan-Results****Possible values:****20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidth

Indicates which channel bandwidths are currently being used by the corresponding remote station.

SNMP ID:

1.3.34.45

Telnet path:**Status > WLAN > Scan-Results****Possible values:****20MHz**

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

Channel bandwidths

Displays the channel bandwidths that the AP supports for the P2P connection.

SNMP ID:

1.3.36.1.46

Telnet path:

Status > WLAN > Interpoints > Access-point-list

Possible values:

20MHz

Channels bundled at 20MHz.

40MHz

Channels bundled at 40MHz.

80MHz

Channels bundled at 80MHz.

160MHz

Channels bundled at 160MHz.

80+80MHz

160MHz channel bandwidth with two disjunct 80MHz channels (802.11ac devices only).

T-40MHz

Channels bundled at 40MHz in the 108Mbit Turbo mode (802.11g devices only)

8.11.2 Additions to the Setup menu

Max. channel bandwidth

Specify the maximum frequency range in which the physical WLAN interface is able to modulate the data to be transmitted onto the carrier signals (channel bandwidth).

In the setting **Auto**, the AP automatically adjusts the channel bandwidth to the optimum. You have also the option to disable the automation and deliberately limit the bandwidth. The available values depend on the WLAN standards supported by the device.

SNMP ID:

2.23.20.8.24

Telnet path:

Setup > Interfaces > WLAN > Radio-settings

Possible values:

Auto

The AP adjusts the channel bandwidth to the optimum. The AP allows the use of the maximum available bandwidth, assuming that the current operating conditions allow this. Otherwise, the AP limits channel bandwidth to 20MHz.

20MHz
40MHz
80MHz

Default:

Auto

Module-2-Max.-Channel-Bandwidth

Here you specify how and to what extent the AP sets the channel bandwidth for the second physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. Doubling the frequency range to 40 MHz allows 96 carrier signals to be used, resulting in a doubling of data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

SNMP ID:

2.37.1.4.25

Telnet path:

Setup > WLAN-Management > AP-Configuration > Base stations

Possible values:

Automatic

The AP automatically detects the maximum channel bandwidth.

20MHz

The AP uses channels bundled at 20 MHz.

40MHz

The AP uses channels bundled at 40MHz.

80MHz

The AP uses channels bundled at 80MHz.

Default:

Automatic

Module-1-Max.-Channel-Bandwidth

Here you specify how and to what extent the AP sets the channel bandwidth for the first physical WLAN interface.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. Doubling the frequency range to 40 MHz allows 96 carrier signals to be used, resulting in a doubling of data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

SNMP ID:

2.37.1.4.26

Telnet path:**Setup > WLAN-Management > AP-Configuration > Base stations****Possible values:****Automatic**

The AP automatically detects the maximum channel bandwidth.

20MHz

The AP uses channels bundled at 20 MHz.

40MHz

The AP uses channels bundled at 40MHz.

80MHz

The AP uses channels bundled at 80MHz.

Default:

Automatic

8.12 Client-steering by the WLC

With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLAN controller. Managed access points constantly report the current values to the WLAN controller, which uses these criteria to decide which access points may respond to requests from WLAN clients. For this reason, client steering is only possible with access points that are centrally managed by a WLAN controller.


In managed networks a WLC centralizes the client steering for all connected APs. In this case, client steering works as follows:

1. The WLC collects the data about the associated WLAN clients from the APs connected to it. These data are the basis for the WLC to control the client steering.
2. All APs are configured so that client steering is handled by the WLC.
3. An unassociated WLAN client sends a probe request to the APs within its range.
4. Using CAPWAP, the APs transmit the request and the signal strength of the WLAN client to the WLC.
5. For each AP within range of the WLAN client, the WLC calculates a value from three factors:
 - A value for signal strength
 - A value for the number of clients associated at the AP
 - A value for the frequency band

The WLC weights these factors and multiplies them together to derive the final value.

6. APs with the highest value, or a value that deviates from it within a specified tolerance level, receive a message from the WLC that they may accept the WLAN client at the next login attempt.
7. WLAN clients attempting to connect to an AP before it has received the response from the WLC are rejected.
8. If a WLAN client is acting "sticky", i.e. it does not attempt to connect to another AP with a good connection quality even though its current connection is of a lower quality, the WLC can prompt the current AP to log off the WLAN client. The WLAN client is then forced to connect with the AP offering the better connection.

 If an AP loses connection to the WLC which is responsible for client steering, the AP accepts all connections from authenticated WLAN clients.

 In order to optimize managed client steering, all APs require the installation of LCOS9.00 or later. If you have mixed operations with APs using earlier versions of LCOS, your WLAN will not be capable of optimizing the distribution of clients.

8.12.1 Configuration

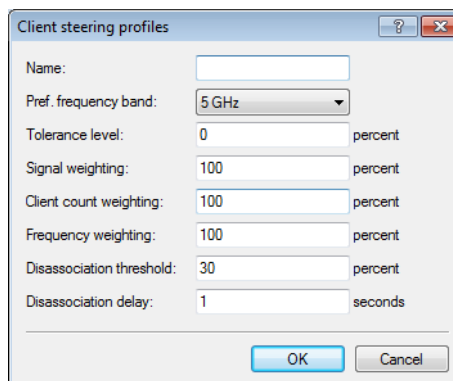
You configure client steering with LANconfig as follows:

1. First, in the WLC you activate client steering for an AP under **WLAN controller > Profiles > Physical WLAN parameters** using the selection list **Client steering**.

- **Off:** Client steering is disabled.
- **AP-based band steering:** The AP independently steers the WLAN client to a preferred frequency band.
- **On:** The AP lets the WLC handle the client steering.

2. Create a client-steering profile under **WLAN controller > AP configuration > Client steering profiles**.

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.



The items have the following meanings:

Name

Name of the client-steering profile.

Pref. Frequency band

Specifies the frequency band to which the WLC steers the AP.

- **2.4GHz:** The WLC steers the AP to the 2.4 GHz frequency band.
- **5GHz:** The WLC steers the AP to the 5 GHz frequency band.

Tolerance level

The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

Signal weighting

Specifies with how many percent the signal-strength value is entered into the final value.

Associated-Clients-Weighting

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Radio weighting

Specifies with how many percent the value for the frequency band is entered into the final value.

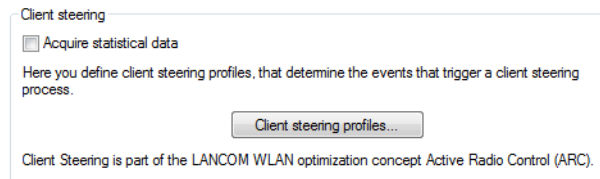
Disassociation threshold

Specifies the threshold value below which the connection to the client must drop before the AP disconnects from the client and initiates a new client-steering operation.

Disassociation delay

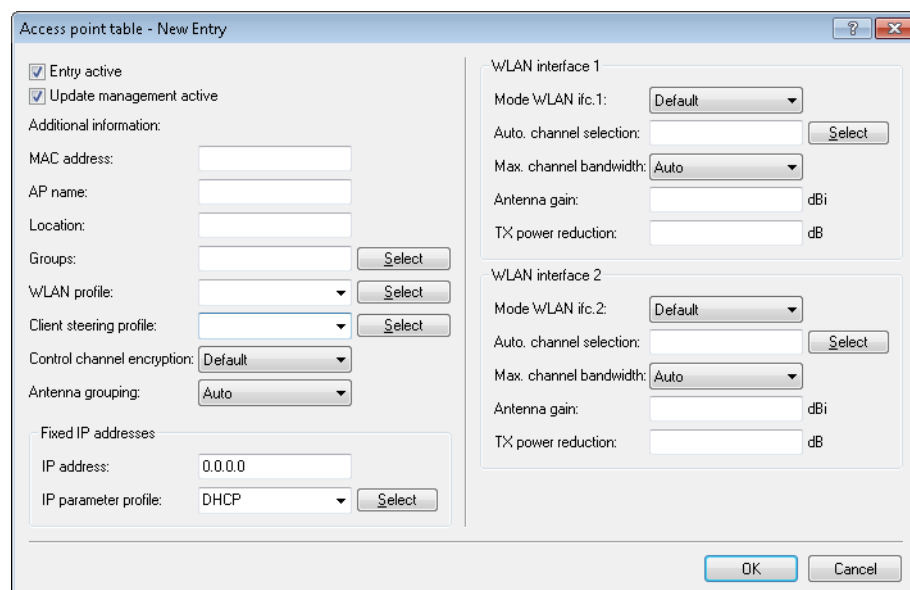
Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

- Optional: Enable the capture of client-steering statistics with the parameter **Acquire statistical data**. This statistical data is suitable for analysis by LANmonitor, for example.



Statistics capture increases the load on the WLC. LANCOM does not recommend the permanent recording of statistics.

- Now assign one of the client-steering profiles to the corresponding AP in the AP table under **WLAN controller > AP configuration > Access point table**.



5. Optional: If necessary, assign a suitable client-steering group to the defined assignment groups.

Assignment groups - New Entry

Name:

WLAN profile:

Client steering profile:

IP parameter profile: DHCP

Source IP range

A new access point must arrive with an IP address within the following range to be caught by this group.

First address:

Last address:

You have now completed the configuration of the client steering.

8.12.2 Additions to the Status menu

Client steering

The client-steering statistics are located in this directory.

SNMP ID:

1.73.123

Telnet path:

Status > WLAN-Management

Active

Indicates whether client steering by WLC controller is enabled.

SNMP ID:

1.73.123.1

Telnet path:

Status > WLAN-Management > Client-Steering

Client-steering-success-rate

The value indicates the ratio of successfully steered clients to all associated clients. In this case, success means that the client has associated with an AP after receiving permission to do so from the WLC.

SNMP ID:

1.73.123.3

Telnet path:**Status > WLAN-Management > Client-Steering****Client info**

This table contains the data of all WLAN clients that have successfully associated to the connected APs.

SNMP ID:

1.73.123.4

Telnet path:**Status > WLAN-Management > Client-Steering****Client-MAC**

This column shows the MAC address of the associated WLAN client.

SNMP ID:

1.73.123.4.1

Telnet path:**Status > WLAN-Management > Client-Steering > Client-Steering****APs-got-OK**

Displays the number of APs that have currently received permission from the WLC to accept this client.

SNMP ID:

1.73.123.4.2

Telnet path:**Status > WLAN-Management > Client-Steering > Client-Steering****State**

This column displays the status of the WLAN client.

SNMP ID:

1.73.123.4.3

Telnet path:**Status > WLAN-Management > Client-Steering > Client-Steering**

Possible values:**Steering OK**

Shows whether the client has associated with an AP after receiving permission to do so from the WLC.

Steering NOK

Shows whether the client has associated with an AP without receiving permission to do so from the WLC.

Pending

The controller has sent a message with "OK" or "NOK" for this client. This state is maintained until the controller receives information from an AP that the client has associated with it. The controller checks whether the AP had previously received an "OK". If this is the case, then it sets the status to "OK", otherwise it sets it to "NOK".

8.12.3 Additions to the Setup menu

Client-Steering-Profile

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.

SNMP ID:

2.37.1.4.27

Telnet path:

Setup > WLAN-Management > AP-Configuration > Base stations

Possible values:

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

Default:

empty

Client-Steering-Profile

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.

SNMP ID:

2.37.1.18.6

Telnet path:

Setup > WLAN-Management > AP-Configuration > Config-Assignment-Groups

Possible values:

Name from **Setup > WLAN-Management > Client-Steering > Profiles**

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

Default:

empty

Client steering

This directory is used to configure the client steering by the WLC.

SNMP ID:

2.37.40

Telnet path:

Setup > WLAN-Management

Trace-Mac

An aid to troubleshooting, only the MAC address you entered is shown when the trace is enabled (`trace # wlc-steering`).

SNMP ID:

2.37.40.11

Telnet path:

Setup > WLAN-Management > Client-Steering

Possible values:

16 characters from 0123456789abcdef

Default:

0000000000000000

Show statistics

Using this parameter, you enable or disable the recording of client-steering statistics. This statistical data is suitable for analysis by LANmonitor, for example. Another option for viewing the statistics is available under **Status > WLAN-Management > Client-Steering**.



Recording the statistics increases the load on the WLC. LANCOM does not recommend the permanent recording of statistics.

SNMP ID:

2.37.40.17

Telnet path:

Setup > WLAN-Management > Client-Steering

Possible values:

Yes

Enables the recording of client-steering statistics.

No

Disables the recording of client-steering statistics.

Default:

No

Profiles

This table is used to manage the profiles for the client steering. A client-steering profile specifies the conditions under which the WLC triggers a client-steering operation.

SNMP ID:

2.37.40.19

Telnet path:**Setup > WLAN-Management > Client-Steering****Name**

Name of the client-steering profile.

SNMP ID:

2.37.40.19.1

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:**Max. 31 characters from `[A-Z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_.`**Default:***empty***Tolerance level**

The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

SNMP ID:

2.37.40.19.2

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:**

0 ... 100 Percent

Default:

0

Signal weighting

Specifies with how many percent the signal-strength value is entered into the final value.

SNMP ID:

2.37.40.19.4

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:**

0 ... 100 Percent

Default:

100

Associated-Clients-Weighting

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

SNMP ID:

2.37.40.19.5

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:**

0 ... 100 Percent

Default:

100

Radio weighting

Specifies with how many percent the value for the frequency band is entered into the final value.

SNMP ID:

2.37.40.19.6

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles**

Possible values:

0 ... 100 Percent

Default:

100

Preferred band

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

SNMP ID:

2.37.40.19.9

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:****2.4GHz**

The WLC steers the AP to the 2.4 GHz frequency band.

5GHz

The WLC steers the AP to the 5 GHz frequency band.

Default:

5GHz

Disassociation-Threshold

Specifies the threshold value below which the connection to the client must drop before the AP disconnects from the client and initiates a new client-steering operation.

SNMP ID:

2.37.40.19.10

Telnet path:**Setup > WLAN-Management > Client-Steering > Profiles****Possible values:**

0 ... 100 Percent

Default:

30

Time-to-Disassociation

Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

SNMP ID:

2.37.40.19.11

Telnet path:

Setup > WLAN-Management > Client-Steering > Profiles

Possible values:

0 ... 10 Seconds

Default:

1

Client-MAC-Statistic-Filter

This parameter specifies a list of MAC addresses, for which the WLC explicitly records statistical data. The WLC writes statistics for the listed MAC addresses to the **Event-Table** under **Status > WLAN-Management > Client-Steering**. Enter multiple MAC addresses into a comma-separated list.



The recording of statistical is enabled elsewhere using the parameter [2.37.40.17 Show statistics](#) on page 271.

SNMP ID:

2.37.40.20

Telnet path:

Setup > WLAN-Management > Client-Steering

Possible values:

Max. 251 characters from `[0-9][a-f]:-,`

Special values:

empty

The device collects statistical data on all MAC addresses (filtering disabled).

Default:

empty

8.13 Automatic frequency-band selection

As of LCOS9.00 you have the option to allow a managed AP to choose the preferred frequency band for the physical WLAN interface by itself. In LANconfig the configuration is carried out in the dialog **WLAN Controller > AP configuration > Access point table**:

Mode WLAN ifc. 1

This setting allows you to configure the frequency band in which the AP operates the 1st physical WLAN interface. When set to **Default**, the AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 2.4GHz band, if available.

Mode WLAN ifc. 2

This setting allows you to configure the frequency band in which the AP operates the 2nd physical WLAN interface. When set to **Default**, the AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 5GHz band, if available.



If a managed AP only has one physical WLAN interface, the AP ignores the settings for the 2nd physical WLAN interface.

8.13.1 Additions to the Setup menu

WLAN module 1 default

This setting allows you to configure the frequency band in which the AP operates the 1st physical WLAN interface.

SNMP ID:

2.37.1.5

Telnet path:

Setup > WLAN-Management > AP-Configuration

Possible values:**Auto**

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 2.4GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4Ghz band.

5GHz

The AP operates the physical WLAN interface in the 5Ghz band.

Off

The AP disables the physical WLAN interface.

Default:

Auto

WLAN module 2 default

This setting allows you to configure the frequency band in which the AP operates the 2nd physical WLAN interface.



If a managed AP only has one physical WLAN interface, the AP ignores the settings for the 2nd physical WLAN interface.

SNMP ID:

2.37.1.6

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

The AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 5GHz band, if available.

2.4GHz

The AP operates the physical WLAN interface in the 2.4Ghz band.

5GHz

The AP operates the physical WLAN interface in the 5Ghz band.

Off

The AP disables the physical WLAN interface.

Default:

Auto

9 VPN

9.1 VPN remote access wizard in WEBconfig:

As of LCOS 9.00 you have the option of using WEBconfig to create VPN-client dial-in accounts using the LANCOM Advanced VPN Client or an alternative VPN client. This is possible as the existing Setup-Wizard **Provide remote access** has been extended with the VPN option. The setup steps are the same as those for LANconfig.



The 1-Click VPN configuration is not available in WEBconfig due to restrictions on browser access.

9.2 L2TPv2 (Layer-2 Tunneling Protocol version 2)

An L2TP access concentrator (LAC) tunnels the PPP request from a client via a public connection (Internet, ATM, frame relay) to an L2TP network server (LNS). The LNS serves as a gateway to the remote network. There, a connected RADIUS server initially authenticates the client, if necessary. The LNS then sends the IP address to the LAC and starts the L2TP tunnel. The LAC communicates the IP address to the client. As of this moment, the client has joined the remote network via an L2TP connection.

L2TP uses two types of data:

Control data

The control data are used to establish, maintain and tear down the tunnel connections.

The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

Payload data

The payload data are encapsulated in PPP frames, which are exchanged between the LAC and the LNS via the tunnel.

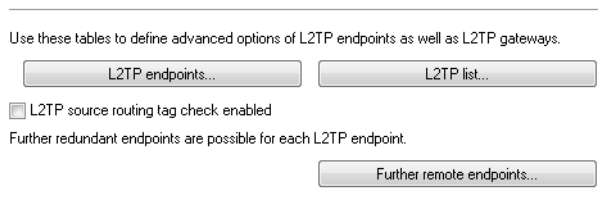
In contrast to the control data, payload data contains no data flow control. Thus there is no guarantee that the sender and receiver are exchanging data correctly.

Unlike PPTP, which transfers control and payload data via different protocols (TCP and GRE), L2TP only uses UDP for both data types. It is also possible to operate several logical payload-data channels on each control-data channel.

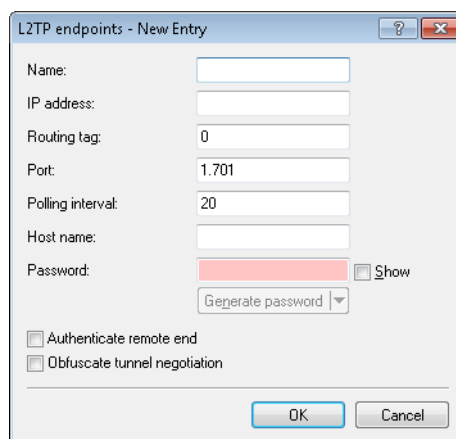
The LANCOM is able to operate as a LAC and also as a LNS.

9.2.1 Configuring the L2TP tunnel

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



The tunnel configuration for the control data of an L2TP tunnel to a tunnel endpoint is located under **L2TP endpoints**.



Name

Name of the tunnel endpoint

IP address

IP address of the tunnel endpoint (IPv4, IPv6, FQDN).

Routing tag

The routing tag of the route to the tunnel endpoint

Port

UDP Port

Polling interval

Polling interval in seconds

Host name

Name used by the device to authenticate at the tunnel endpoint

Password

Password used by the device to authenticate at the tunnel endpoint

Authenticate remote end

Enable this option if two tunnel endpoints (LAC and LNS) are required to mutually authenticate one another before establishing a tunnel. In this case, the tunnel endpoint name and password for this device are configured as the tunnel endpoint and the option to **Authenticate remote end** is similarly enabled.

Obfuscate tunnel negotiation

If the tunnel negotiations between the LAC and the LNS are to be encrypted, you enable this option. The two L2TP partners encrypt and decrypt the L2TP messages with the help certain AVPs (attribute value pairs) of a common preshared secret.

Under **L2TP list**, you make the link between the L2TP remote sites and a previously configured tunnel endpoint.

An entry in this table is necessary only under the following conditions:

- Outgoing connections
- Incoming connections with an idle timeout not equal to "20" or
- If incoming links specify the use of a specific tunnel only.

Remote site

Name of the L2TP remote device

L2TP endpoint

Name of the tunnel endpoint used by this remote site.

Short hold time

Determines how long the L2TP tunnel endpoint keeps the tunnel open when inactive.

In the case of incoming tunnel requests, a check is performed either by RADIUS or by means of an entry for the requesting host in the L2TP endpoints table. If the table contains an entry with the same IP address (or no IP address is specified for this entry), the device permits tunnel establishment to this host.

For additional protection, for example to enable encryption of the L2TP sessions via IPSec, the device can additionally check the routing tag of the remote site from which it received the data. This option is enabled with **L2TP source routing tag check enabled**.

You have the option to configure up to 32 additional gateways per tunnel endpoint by clicking on **Further remote endpoints**.

! Ensure that all additionally specified L2TP endpoints are configured identically to the referenced tunnel endpoint.

Remote site

Name of the tunnel endpoint, as configured in the table of **L2TP endpoints**.

Begin with L2TP endpoint

Option for selecting the next gateway. The following options are available:

- **Last used:** Select the last successful address
- **First:** Select the first gateway in the list
- **Random:** Random selection from the gateways in the list

On the following tabs you configure the names and the respective routing tags of the alternative gateways.

9.2.2 Authentication via RADIUS

RADIUS authentication for L2TP is possible in two cases:

- Tunnel authentication: The RADIUS server checks to see whether a LAC is allowed to establish a L2TP connection.
- PPP session: The RADIUS server checks the user data of the corresponding PPP session.

For this reason, the configuration of the RADIUS server for L2TP-tunnel authentication and the PPP user data are carried out independently of one another.

In the case of tunnel authentication by RADIUS, the settings in LANconfig are configured under **Communication > RADIUS** in the section **Tunnel authentication via RADIUS for L2TP**.

RADIUS server

Enables or disables the RADIUS server for the authentication of the tunnel endpoint, regardless of a PPP-session authentication. The following options are possible:

- **Deactivated:** The RADIUS server is not enabled for the authentication of tunnel endpoints.
- **Activated:** The RADIUS server handles the authentication of tunnel endpoints.
- **Exclusive:** Enables the use of the external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Protocols

Protocol for communication between the internal RADIUS server and the tunnel endpoint.

Address

IP address or DNS name of the RADIUS server.

Port

The port the RADIUS server

Source address

Optional sender address of the device. If you have configured loopback addresses, these can also be specified here. Following input formats are allowed:

- Name of the IP network (ARF network) whose address is to be used instead
- "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

Secret

Shared secret between the RADIUS server and the LANCOM

Password

Dummy password for tunnel authentication

If an L2TP tunnel request arrives from a remote host (Start Control Connection Request), the LANCOM sends a request to the RADIUS server that has been enabled for L2TP. This request contains among other things the name of the host, the dummy password, the IP address of the device, and also the service type "Outbound User". The RADIUS server authenticates the host and sends a "RADIUS accept" to the LANCOM together with; the tunnel password to be used; the tunnel type "L2TP" with the tag "0"; and also the Tunnel-Client-Auth-ID, which must match with the host name transmitted earlier by the LANCOM. The LANCOM checks this data and, if the result is positive, it takes the tunnel password to authenticate the dial-in client and, if applicable, to obfuscate the L2TP tunnel negotiations.



Configuring the RADIUS server to authenticate PPP sessions is conducted as described in the section **Other services > RADIUS > Configuration of RADIUS as authenticator or NAS > Dial-in using PPP and RADIUS**.

9.2.3 Operation as an L2TP access concentrator (LAC)

In the following example, the LANCOM operating as a L2TP access concentrator (LAC) establishes an L2TP tunnel to an L2TP network server (LNS) with the IP address 192.168.1.66.

Proceed as follows to configure the LANCOM as a LAC:

1. Under **Communication > Remote sites** in the table **L2TP endpoints** create an entry for an LNS as the remote L2TP gateway.

2. Enter a name for this site under **Communication > Protocols** in the table **L2TP list** and connect it with the L2TP endpoint you created previously.

It is possible to connect several remote sites with an L2TP tunnel. This allows multiple PPP sessions to be transported through an L2TP tunnel. For this purpose, configure in this table several remote sites with the same L2TP endpoint.

3. Under **Communication > Protocols** in the table **PPP list** create an entry for the L2TP tunnel.

- For this site, go to **Configuration > IP router > Routing** and create an entry in the corresponding IPv4 or IPv6 routing table.

9.2.4 Operation as the L2TP network server (LNS) for RAS clients

In order to configure the LANCOM as the L2TP network server (LNS) for authenticating RAS clients without configuring a RADIUS server in the LANCOM, you have two options:

- Under **Communication > Remote sites** in the table **L2TP endpoints**, create an entry "DEFAULT".

The entry for the IP address is "0.0.0.0", because the IP address of the L2TP-LAC is unknown to the LANCOM.

- Then, under **Communication > Remote sites** in the table **L2TP list**, configure a "DEFAULT" entry.

If the L2TP tunnel is to be connected permanently, set the short hold time to "9999".

- Alternatively, you make a separate entry for the RAS client (e.g., "CLIENT") under **Communication > Remote sites** in the **L2TP endpoints** table.

- You then configure a new entry for the client under **Communication > Protocols** in the **PPP list**.

9.2.5 Operation as an L2TP network server (LNS) with authentication via RADIUS

In the following example, the LANCOM functions as an L2TP network server (LNS). RADIUS is used to authenticate the incoming L2TP tunnel and the PPP sessions.

Proceed as follows to configure the LANCOM as a LNS:

1. Under **Communication > Remote sites** in the table **L2TP endpoints**, create an entry "DEFAULT".

2. Then, under **Communication > Remote sites** in the table **L2TP list**, configure a "DEFAULT" entry.

3. Configure the RADIUS server under **Communication > RADIUS**.

i You only configure the lower section **Tunnel authentication via RADIUS for L2TP** if L2TP tunnel authentication should be done via the RADIUS server.

4. Configure the RADIUS server in order for it to be able to authenticate the L2TP tunnel and the PPP sessions.

If a LAC needs to authenticate itself at the L2TP tunnel with the station name "router1" and the password "abcde", you configure the appropriate entry in the RADIUS server (e.g. FreeRADIUS) as follows:

```
router1 Cleartext-Password := "lancom"
      Service-Type = Outbound-User,
      Tunnel-Type = L2TP,
      Tunnel-Password = "abcde",
      Tunnel-Client-Auth-ID = "router1"
```

For the authentication of the PPP session of a user with the username "test" and the password "test", you configure the appropriate entry in the RADIUS server as follows:

```
test Cleartext-Password := "1234"
      Service-Type = Framed-User,
      Framed-Protocol = PPP
```

9.2.6 Additions to the Status menu

L2TP

Layer-2 tunneling protocol

SNMP ID:

1.84

Telnet path:

State

Rx-Packets

The number of received packets.

SNMP ID:

1.84.1

Telnet path:

Status > L2TP

Tx-Packets

The number of sent packets.

SNMP ID:

1.84.2

Telnet path:

Status > L2TP

TX retries

Retries on the control channel.

SNMP ID:

1.84.3

Telnet path:

Status > L2TP

Call errors

Number of failed attempts to establish a session.

SNMP ID:

1.84.4

Telnet path:

Status > L2TP

Endpoints

This table contains Information about the currently active tunnels. Once a tunnel has been established it is immediately deleted from the table, if no error occurred. The error is automatically deleted when the tunnel is established again, or it can be deleted manually. The syntax for this is: set <Peer> {last error} (none)

SNMP ID:

1.84.5

Telnet path:

Status > L2TP

L2TP endpoint

Name of the tunnel endpoint

SNMP ID:

1.84.5.1

Telnet path:

Status > L2TP > Endpoints

State

Current state of the tunnel endpoint.

SNMP ID:

1.84.5.2

Telnet path:**Status > L2TP > Endpoints****Last error**

The last detected error.

SNMP ID:

1.84.5.3

Telnet path:**Status > L2TP > Endpoints****Possible values:****(none)**

No error

DNS resolution failed

DNS resolution failed

No route to gateway

There is no route to the gateway

Invalid gateway address

The gateway IP address is not valid

No response

No response was received from the gateway

Message timeout

A control message was not answered

Tunnel already exists

A tunnel to this gateway already exists

Authorization failed

The authentication failed

Bad protocol version

An incorrect version of L2TP is being used

Shutting down

The device is booting at the moment

State machine error

Generic Error

No tunnel exists

Unknown tunnel ID

Invalid length

Invalid length of a parameter

Invalid value

Invalid value of a parameter

No resources

No resources available

Invalid session ID

Invalid session ID

Vendor-specific error

Vendor-specific error

Try another

Try a different gateway

Unknown mandatory attribute

Unknown mandatory attribute

Unknown

An unknown error occurred

Mode

Active (LAC) or passive (LNS) establishment.

SNMP ID:

1.84.5.4

Telnet path:

Status > L2TP > Endpoints

Phys. connection

Name of the physical connection used.

SNMP ID:

1.84.5.5

Telnet path:

Status > L2TP > Endpoints

Gateway

Resolved IP address of the current gateway.

SNMP ID:

1.84.5.6

Telnet path:

Status > L2TP > Endpoints

Sessions

Number of connections using the tunnel.

SNMP ID:

1.84.5.7

Telnet path:

Status > L2TP > Endpoints

Conn. time:

Duration of the connection in seconds.

SNMP ID:

1.84.5.8

Telnet path:

Status > L2TP > Endpoints

Embedded error message

Error messages in plain text

SNMP ID:

1.84.5.9

Telnet path:

Status > L2TP > Endpoints

Number of endpoints

Number of existing tunnels.

SNMP ID:

1.84.6

Telnet path:

Status > L2TP

Sessions

This table contains Information about the currently active sessions. IPv6 parameters do not appear in the table, they can be found in the IPv6 statistics for the various interfaces. Once a session has been established it is immediately deleted

from the table, if no error occurred. The error is automatically deleted when the session is established again, or it can be deleted manually. The syntax for this is: set <Peer> {last error} (none)

SNMP ID:

1.84.7

Telnet path:

Status > L2TP

Remote site

Name of the remote device/session.

SNMP ID:

1.84.7.1

Telnet path:

Status > L2TP > Connections

State

Current connection state of the session.

SNMP ID:

1.84.7.2

Telnet path:

Status > L2TP > Connections

Last error

The last recorded error.

SNMP ID:

1.84.7.3

Telnet path:

Status > L2TP > Connections

Mode

Indication of whether session establishment was active or passive.

SNMP ID:

1.84.7.4

Telnet path:**Status > L2TP > Connections****SH-Time**

Session idle timeout.

SNMP ID:

1.84.7.5

Telnet path:**Status > L2TP > Connections****L2TP endpoint**

Name of the tunnel being used.

SNMP ID:

1.84.7.6

Telnet path:**Status > L2TP > Connections****Peer address**

IPv4 address of remote device.

SNMP ID:

1.84.7.7

Telnet path:**Status > L2TP > Connections****IP address**

Own IPv4 address.

SNMP ID:

1.84.7.8

Telnet path:

Status > L2TP > Connections

DNS default

IPv4 address of the primary DNS server.

SNMP ID:

1.84.7.9

Telnet path:

Status > L2TP > Connections

DNS backup

IPv4 address of the secondary DNS server.

SNMP ID:

1.84.7.10

Telnet path:

Status > L2TP > Connections

NBNS default

IPv6 address of the primary NBNS server.

SNMP ID:

1.84.7.11

Telnet path:

Status > L2TP > Connections

NBNS backup

IPv4 address of the secondary NBNS server.

SNMP ID:

1.84.7.12

Telnet path:

Status > L2TP > Connections

Conn. time:

Duration of the session in seconds.

SNMP ID:

1.84.7.13

Telnet path:

Status > L2TP > Connections

Number of connections

Number of existing connections.

SNMP ID:

1.84.8

Telnet path:

Status > L2TP

Delete values

Action to reset the counter. Syntax: Do delete-values

SNMP ID:

1.84.9

Telnet path:

Status > L2TP

9.2.7 Additions to the Setup menu

L2TP-operating

This item determines whether RADIUS should be used to authenticate the tunnel endpoint.

SNMP ID:

2.2.22.20

Telnet path:

Setup > WAN > RADIUS

Possible values:

No

There is no RADIUS authentication.

Yes

RADIUS authentication occurs if, in the table 'L2TP Endpoints', the field 'Auth-Peer' is set to 'Yes', but no password was entered.

Exclusive

RADIUS authentication always occurs if, in the table 'L2TP Endpoints', the field 'Auth-Peer' is set to 'Yes', irrespective of whether a password was entered.

Default:

No

L2TP server host name

IP address of the RADIUS server.



The internal RADIUS server of the device does not support tunnel authentication. An external RADIUS server is required for this purpose.

SNMP ID:

2.2.22.21

Telnet path:

Setup > WAN > RADIUS

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

L2TP-Auth.-Port

The UDP port of the RADIUS server.

SNMP ID:

2.2.22.22

Telnet path:

Setup > WAN > RADIUS

Possible values:

0 ... 65535

L2TP-loopback address

The sender address used for RADIUS requests.

SNMP ID:

2.2.22.23

Telnet path:**Setup > WAN > RADIUS****Possible values:**Max. 16 characters from `[A-Z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ .`**L2TP protocol**

The protocol to be used.

SNMP ID:

2.2.22.24

Telnet path:**Setup > WAN > RADIUS****Possible values:****RADIUS****RADSEC****Default:**

RADIUS

L2TP secret

The shared secret between the router and the RADIUS server.

SNMP ID:

2.2.22.25

Telnet path:**Setup > WAN > RADIUS****Possible values:**Max. 64 characters from `#[A-Z][a-z][0-9]@{ | }~!$%&'()+- , / : ; < = > ? [\] ^ _ . ~`**L2TP-Password**

The password stored together with the host in the RADIUS server. After authentication, the password for the tunnel is sent by the RADIUS server.

SNMP ID:

2.2.22.26

Telnet path:**Setup > WAN > RADIUS****Possible values:**Max. 64 characters from `#[A-Z][a-z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_``**L2TP endpoints**

The table contains the basic settings for the configuration of an L2TP tunnel.



To authenticate RAS connections by RADIUS and without configuring a router, this table needs a default entry with the following values:

Identifier: DEFAULT

Poll: 20

Auth-peer: Yes

Hide: No

All other fields must be left empty. With 'Auth-Peer' set to 'No' in the DEFAULT entry, all hosts will be accepted unchecked and only the PPP sessions are authenticated.

SNMP ID:

2.2.35

Telnet path:**Setup > WAN****Identifier**

The name of the tunnel endpoint. If an authenticated L2TP tunnel is to be established between two devices, the entries 'Identifier' and 'Hostname' need to cross match.

SNMP ID:

2.2.35.1

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**Max. 16 characters from `[A-Z][0-9]@{ }~!$%&'()+-./:;<=>?[\]^_``**IP address**

The IP address of the tunnel endpoint. An FQDN can be specified instead of an IP address (IPv4 or IPv6).

SNMP ID:

2.2.35.2

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg tag**

The tag assigned to the route to the tunnel endpoint is specified here.

SNMP ID:

2.2.35.3

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**

0 ... 65535

Port

UDP port to be used.

SNMP ID:

2.2.35.4

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**

0 ... 65535

Default:

1701

Poll

The polling interval in seconds.

SNMP ID:

2.2.35.5

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**

0 ... 65535

Default:

20

Host name

User name for the authentication If an authenticated L2TP tunnel is to be established between two devices, the entries 'Identifier' and 'Hostname' need to cross match.

SNMP ID:

2.2.35.6

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**Max. 64 characters from `#[A-Z][a-z][0-9]@{ | } ~ ! $ % & ' () + - , / : ; < = > ? [\] ^ _ . ``**Password**

The password for the authentication This is also used to hide the tunnel negotiations, if the function is activated.

SNMP ID:

2.2.35.7

Telnet path:**Setup > WAN > L2TP-Endpoints****Possible values:**Max. 32 characters from `#[A-Z][a-z][0-9]@{ | } ~ ! $ % & ' () + - , / : ; < = > ? [\] ^ _ . ``**Auth-Peer**

Specifies whether the remote station should be authenticated.

SNMP ID:

2.2.35.8

Telnet path:**Setup > WAN > L2TP-Endpoints**

Possible values:

No
Yes

Default:

No

Hide

Specifies whether tunnel negotiations should be hidden by using the specified password.

SNMP ID:

2.2.35.9

Telnet path:

Setup > WAN > L2TP-Endpoints

Possible values:

No
Yes

Default:

No

L2TP additional gateways

This table allows you to specify up to 32 redundant gateways for each L2TP tunnel.

SNMP ID:

2.2.36

Telnet path:

Setup > WAN

Identifier

The name of the tunnel endpoint as also used in the table of L2TP endpoints.

SNMP ID:

2.2.36.1

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 16 characters from `[A-Z][0-9]@{ | }~!$%&'()+-./:;<=>?[\]^_.`**Begin with**

This setting specifies which redundant gateway is used first.

SNMP ID:

2.2.36.2

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:****Last used**

This selects the last successfully used gateway.

first

This always selects the first gateway.

random

A random gateway is selected at each attempt.

Default:

Last used

Gateway-1

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.3

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-1**

The routing tag of the route where Gateway-1 can be reached.

SNMP ID:

2.2.36.4

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-2

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.5

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-2**

The routing tag of the route where Gateway-29 can be reached.

SNMP ID:

2.2.36.6

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-3

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.7

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-3

The routing tag of the route where Gateway-3 can be reached.

SNMP ID:

2.2.36.8

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-4

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.9

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-4

The routing tag of the route where Gateway-4 can be reached.

SNMP ID:

2.2.36.10

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-5

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.11

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-5**

The routing tag of the route where Gateway-5 can be reached.

SNMP ID:

2.2.36.12

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-6

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.13

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-6**

The routing tag of the route where Gateway-6 can be reached.

SNMP ID:

2.2.36.14

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

0 ... 65535

Gateway-7

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.15

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-7

The routing tag of the route where Gateway-7 can be reached.

SNMP ID:

2.2.36.16

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-8

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.17

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-8

The routing tag of the route where Gateway-8 can be reached.

SNMP ID:

2.2.36.18

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-9

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.19

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-9**

The routing tag of the route where Gateway-9 can be reached.

SNMP ID:

2.2.36.20

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-10

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.21

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-10

The routing tag of the route where Gateway-10 can be reached.

SNMP ID:

2.2.36.22

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-11

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.23

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-11

The routing tag of the route where Gateway-11 can be reached.

SNMP ID:

2.2.36.24

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-12

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.25

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-12**

The routing tag of the route where Gateway-12 can be reached.

SNMP ID:

2.2.36.26

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-13

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.27

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-13**

The routing tag of the route where Gateway-13 can be reached.

SNMP ID:

2.2.36.28

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

0 ... 65535

Gateway-14

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.29

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-14

The routing tag of the route where Gateway-14 can be reached.

SNMP ID:

2.2.36.30

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-15

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.31

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-15

The routing tag of the route where Gateway-15 can be reached.

SNMP ID:

2.2.36.32

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-16

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.33

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-16**

The routing tag of the route where Gateway-16 can be reached.

SNMP ID:

2.2.36.34

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-17

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.35

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-17

The routing tag of the route where Gateway-17 can be reached.

SNMP ID:

2.2.36.36

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-18

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.37

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-18

The routing tag of the route where Gateway-18 can be reached.

SNMP ID:

2.2.36.38

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-19

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.39

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-19**

The routing tag of the route where Gateway-19 can be reached.

SNMP ID:

2.2.36.40

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-20

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.41

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-20**

The routing tag of the route where Gateway 20 can be reached.

SNMP ID:

2.2.36.42

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

0 ... 65535

Gateway-21

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.43

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-21

The routing tag of the route where Gateway-21 can be reached.

SNMP ID:

2.2.36.44

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-22

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.45

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-22

The routing tag of the route where Gateway-22 can be reached.

SNMP ID:

2.2.36.46

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-23

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.47

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-23**

The routing tag of the route where Gateway-23 can be reached.

SNMP ID:

2.2.36.48

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-24

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.49

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-24

The routing tag of the route where Gateway-24 can be reached.

SNMP ID:

2.2.36.50

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-25

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.51

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-25

The routing tag of the route where Gateway-25 can be reached.

SNMP ID:

2.2.36.52

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-26

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.53

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-26

The routing tag of the route where Gateway-26 can be reached.

SNMP ID:

2.2.36.54

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-27

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.55

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-27

The routing tag of the route where Gateway-27 can be reached.

SNMP ID:

2.2.36.56

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

0 ... 65535

Gateway-28

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.57

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-28

The routing tag of the route where Gateway-28 can be reached.

SNMP ID:

2.2.36.58

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-29

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.59

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

Max. 64 characters from [A-Z][a-z][0-9].-: %

Rtg-Tag-29

The routing tag of the route where Gateway-29 can be reached.

SNMP ID:

2.2.36.60

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-30

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.61

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`**Rtg-Tag-30**

The routing tag of the route where Gateway-30 can be reached.

SNMP ID:

2.2.36.62

Telnet path:**Setup > WAN > L2TP-Additional-Gateways****Possible values:**

0 ... 65535

Gateway-31

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.63

Telnet path:**Setup > WAN > L2TP-Additional-Gateways**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-31

The routing tag of the route where Gateway-31 can be reached.

SNMP ID:

2.2.36.64

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

Gateway-32

The first alternative IP address (IPv4 or IPv6) or FQDN of the tunnel endpoint.

SNMP ID:

2.2.36.65

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Rtg-Tag-32

The routing tag of the route where Gateway-32 can be reached.

SNMP ID:

2.2.36.66

Telnet path:

Setup > WAN > L2TP-Additional-Gateways

Possible values:

0 ... 65535

L2TP-Peers

In this table, the tunnel endpoints are linked with the L2TP remote stations that are used in the routing table. An entry in this table is required for outgoing connections if an incoming session should be assigned an idle timeout not equal to zero, or if the use of a particular tunnel is to be forced.

SNMP ID:

2.2.37

Telnet path:

Setup > WAN

Remote site

Name of the L2TP remote station.

SNMP ID:

2.2.37.1

Telnet path:

Setup > WAN > L2TP-Peers

Possible values:

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

L2TP endpoint

Name of the tunnel endpoint

SNMP ID:

2.2.37.2

Telnet path:

Setup > WAN > L2TP-Peers

Possible values:

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

SH-Time

Idle timeout in seconds.

SNMP ID:

2.2.37.3

Telnet path:**Setup > WAN > L2TP-Peers****Possible values:**

0 ... 9999

L2TP-Source-Check

The default setting checks the sender address of an incoming tunnel. The tunnel is established if the address is part of the configured gateway for the tunnel or if no gateways have been configured at all. It is also possible to check the routing tag of incoming packets. Note that only routing tags not equal to zero will be checked.

SNMP ID:

2.2.38

Telnet path:**Setup > WAN****Possible values:****Address****Tag+address****Default:**

Address

9.3 Support of the DH groups 15 and 16

As of version 9.00, for the encryption of VPN connections LANconfig offers you improved options for key exchange according to the Diffie-Hellmann algorithm. The DH groups 15 and 16 can be used for this on compatible devices. The relevant settings are located in the configuration menu under **VPN > General > Connection parameters > Add** and also under **VPN > Defaults**.

9.3.1 Additions to the Setup menu

IKE-Auth-Alg

Hash algorithm for the encryption. The available values depend on the device you want to configure.

SNMP ID:

2.19.4.11.4

Telnet path:**Setup > VPN > Proposals > IKE**

Possible values:

MD5
SHA1
SHA2-256
SHA2-384
SHA2-512

Default:

MD5

DH group

This value displays the corresponding DH group.

SNMP ID:

2.19.3.29.2.1

Telnet path:

Setup > VPN > Isakmp > DH-Groups > Group-config

Possible values:

Selection from the list of predefined DH groups

PFS-Grp

Perfect Forward Secrecy (PFS) is a security feature of encryption algorithms. The PFS group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID:

2.19.7.3

Telnet path:

Setup > VPN > Layer

Possible values:

0
No PFS
1
MODP-768
2
MODP-1024
5
MODP-1536

- 14 MODP-2048
- 15 MODP-3072
- 16 MODP-4096

Default:

14

IKE-Grp

The IKE group specifies the length of the Diffie-Hellman key used to encrypt the IKE negotiation.

SNMP ID:

2.19.7.4

Telnet path:

Setup > VPN > Layer

Possible values:

- 1 MODP-768
- 2 MODP-1024
- 5 MODP-1536
- 14 MODP-2048
- 15 MODP-3072
- 16 MODP-4096

Default:

2

AggrMode-IKE-Group-Default

This IKE group is used for aggressive-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID:

2.19.11

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

- 1**
MODP-768
- 2**
MODP-1024
- 5**
MODP-1536
- 14**
MODP-2048
- 15**
MODP-3072
- 16**
MODP-4096

Default:

2

MainMode-IKE-Group-Default

This IKE group is used for main-mode connections when the remote address cannot be identified by its IP address but by a subsequently transmitted ID.

SNMP ID:

2.19.14

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

- 1**
MODP-768
- 2**
MODP-1024
- 5**
MODP-1536
- 14**
MODP-2048
- 15**
MODP-3072

16

MODP-4096

Default:

2

QuickMode-PFS-Group-Default

This IPSec group is used for simplified dial-in with certificates.

SNMP ID:

2.19.20

Telnet path:**Setup > VPN****Possible values:****0**

No PFS

1

MODP-768

2

MODP-1024

5

MODP-1536

14

MODP-2048

15

MODP-3072

16

MODP-4096

Default:

2

10 Routing and WAN connections

10.1 Revised flow control

Until now, it was only possible to view the flow-control status for two network partners. As of LCOS 9.00, flow control can be viewed in the Status section of the mode (symmetrical, asymmetrical).

10.1.1 Additions to the Status menu

Flow control

Displays the current flow-control status. Possible values are:

SNMP ID:

1.5.51.6

Telnet path:

Status > LAN > Interfaces

Possible values:

No

Flow control is disabled.

Yes

Flow control is enabled (symmetrical operation).

TX only

Flow control is enabled (asymmetrical operation, send only).

RX only

Flow control is enabled (asymmetrical operation, receive only).

Flow control

Displays the current flow-control status. Possible values are:

SNMP ID:

1.51.1.8

Telnet path:

Status > Ethernet-Ports > Ports

Possible values:**No**

Flow control is disabled.

Yes

Flow control is enabled (symmetrical operation).

TX only

Flow control is enabled (asymmetrical operation, send only).

RX only

Flow control is enabled (asymmetrical operation, receive only).

10.1.2 Additions to the Setup menu

Flow control

Using flow control, you can prevent the loss of data packets if a partner network cannot process incoming data packets, for example due to a memory overflow. In this case, the receiver signals the sender to pause the data transmission for a certain period of time.

SNMP ID:

2.23.21.11

Telnet path:

Setup > Interfaces > Ethernet-ports

Possible values:**Auto**

If auto-negotiation is enabled, the flow control is performed automatically according to the capabilities of the partner (symmetric, asymmetric).



If auto-negotiation is disabled, no flow control takes place.

On

Enables symmetrical flow control when auto-negotiation is disabled.

Off

Disables the flow control when auto-negotiation is enabled.

Flow control

Using flow control, you can prevent the loss of data packets if a partner network cannot process incoming data packets, for example due to a memory overflow. In this case, the receiver signals the sender to pause the data transmission for a certain period of time.

SNMP ID:

2.23.30.9

Telnet path:

Setup > Interfaces > LAN-Interfaces

Possible values:**Auto**

If auto-negotiation is enabled, the flow control is performed automatically according to the capabilities of the partner (symmetric, asymmetric).



If auto-negotiation is disabled, no flow control takes place.

On

Enables symmetrical flow control when auto-negotiation is disabled.

Off

Disables the flow control when auto-negotiation is enabled.

10.2 AC name configurable for PPPoE server

As of LCOS 9.00, you have the option of assigning an AC name to a PPPoE server (Access Concentrator Name).

☐ PPPoE server enabled

Port table

Server name:

Service name:

Session limit:

Define in the remote site list the clients, that will be granted access from the PPPoE server. These clients can also be assigned further properties and rights in the PPP list or firewall.

Remote sites (PPPoE)...

Server name

This input field provides the option to give the PPPoE server a name that is independent of the device name (AC-Name = access concentrator name). If you leave this field blank, the PPPoE server uses the device name as the server name.

10.2.1 Additions to the Setup menu

AC name

This input field provides the option to give the PPPoE server a name that is independent of the device name (AC-Name = access concentrator name).

SNMP ID:

2.31.6

Telnet path:

Setup > PPPoE-Server

Possible values:

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

Special values:

empty

If you leave this field blank, the PPPoE server uses the device name as the server name.

Default:*empty*

10.3 Dual-SIM support for mobile devices

As of LCOS 9.00 you have the option to assign each of the mobile profiles created on the device directly to a SIM card. LANmonitor is used to switch between these profiles or SIM cards.

10.3.1 Configuring WWAN access

The following tutorial shows you how devices with an internal cellular modem are configured to use access via cellular networks (WWAN). First you either create a mobile profile for your provider or edit an existing profile, and then you assign this profile to the WAN interface of the device.

1. In LANconfig, open the configuration dialog for your device and navigate to the section **Interfaces > WAN**.
2. Select an existing profile to be edited or add a new profile for your provider in the **Mobile profiles** table.

In the interests of completeness this tutorial explains the creation of a new profile.

3. Under **Name** type in a unique label for the mobile profile.
4. Under **PIN** enter the 4-digit PIN of the mobile phone SIM card. The device needs this information to operate the mobile modem.



The SIM card logs every failed attempt with an incorrect PIN. The number of failed attempts remains stored even when the device is temporarily disconnected from the mains. After 3 failed attempts, the SIM card is locked from further access attempts. If this occurs, you usually need the 8-digit PUK or SuperPIN to unlock it.

5. If your device accommodates several SIM cards, use **SIM slot** to select the SIM card that you want to associate with this profile.

The item **Profile disabled** switches this mobile profile off. This option is useful if you wish to create a profile template only and complete the mobile setup at a later time.

 Only enabled profiles are visible for selection in LANmonitor.


6. Under **APN**, enter the name of the access server for the data services of your mobile provider.
The APN (access point name) is specific to each mobile phone provider. You will usually find this information in the documentation provided with your mobile phone contract.
7. Under **PDP type** you specify the type of the PDP context for the mobile profile.
The PDP context describes the support of the address spaces which the backbone of the corresponding cellular network provider offers for connections from the cellular network to the Internet. This can be either IPv4 or IPv6 alone, or can include support for both address spaces (dual stack). Clients that want to use the corresponding cellular network provider must support at least one of the specified address spaces.
8. Set the preferred **Network selection** mode:

Automatic

The mobile modem automatically connects to one of the available and permitted mobile phone networks.

Manual

The mobile modem connects to the specified mobile phone network only.

 Manual mobile network selection is especially suitable when the device is in stationary operation and you wish to prevent it from connecting to another undesirable or more expensive mobile phone network.

9. If you have selected manual network selection, enter the exact name of your desired network under **Network name**.
10. Specify the preferred transfer mode within the mobile network under **Transmission mode**:

Automatic

Automatic selection of transmission mode

LTE

LTE/4G mode only

UMTS + GPRS

Combined UMTS/3G & GPRS mode

UMTS

UMTS/3G mode only

GPRS

GPRS mode only

11. Under **Downstream rate** and **Upstream rate** you specify the transfer rates for the mobile phone connection. This is important for the QoS (quality-of-service) feature and the functioning of the firewall.
If the value is set to 0, the mobile interface in the corresponding direction is considered to be unlimited and the QoS mechanisms will not take effect.
12. If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result. The selection under **LTE bands** allows you to control which frequency bands are used by the mobile modem.

All

All frequency bands are enabled.

2100 MHz (B1)

2.1GHz band is enabled.

1800 MHz (B3)

1.8GHz band is enabled.

2600 MHz (B7)

2.6GHz band is enabled.

900 MHz (B8)

900MHz band is enabled.

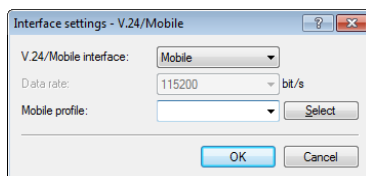
800 MHz (B20)

800MHz band is enabled.

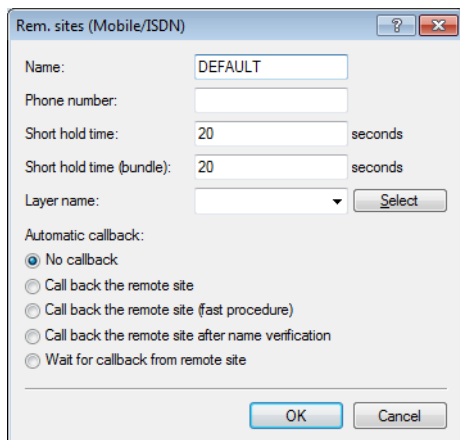


This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

13. Click **OK** to save the settings.
14. In the dialog **Interfaces > WAN**, click **Interface settings** and select **V.24/Mobile**.
15. Set the **V.24/Mobile interface** to **Mobile**.
16. Under **Mobile profiles**, select the profile you created earlier for your mobile phone provider.



17. Click **OK** to save the settings.
18. In the view **Communication > Remote sites**, click **Rem. sites (Mobile /...)** and edit the **DEFAULT** profile.



19. Under **Phone number**, enter the dial-in number of your mobile phone provider. If your provider has not given you a dial-in phone number, enter *99#.
20. Under **Short hold time**, enter the time after which the device disconnects from the remote site if no packets are transmitted

Enter a value in seconds to find a balance between the costs arising from idle time those of connection establishment, for example 300. A value of 0 causes the device to stay connected until it is broken and terminated. With a value of 9999 the device automatically reconnects every time.
21. For **Layer name** select the presetting UMTS.
22. Click **OK** to save the settings.

23. In the view **Communication > Protocols**, open the **PPP list** and edit the **DEFAULT** site.

24. Enable the check box for **Enable IPv4 routing**.
25. Deselect any settings under **Authentication of the remote site (request)**.
26. Click **OK** to save the settings.
27. In the view **IP Router > Routing**, click **IPv4 routing table** and add the **Default route** (255 . 255 . 255 . 255).

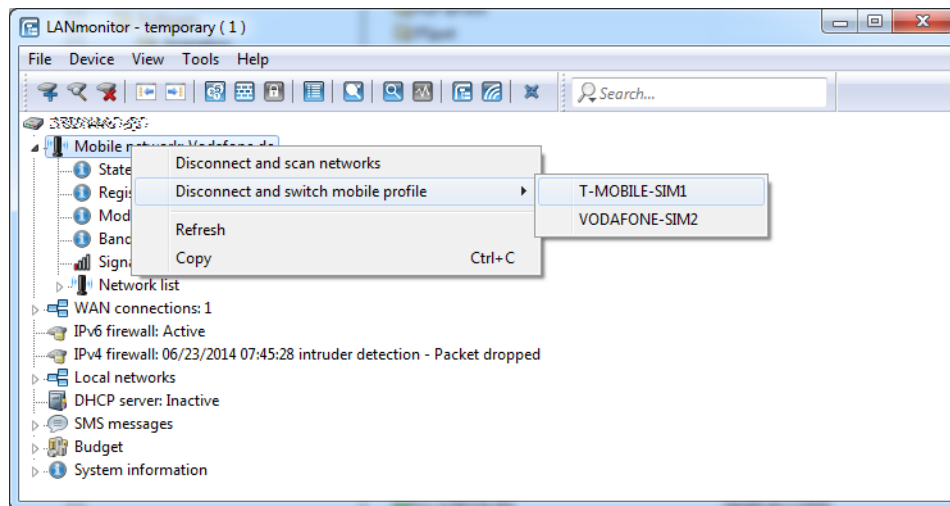
28. Under **Router**, select the profile created earlier under **Rem. sites (Mobile /...)**.
29. Set the **IP masquerading** to **Masking intranet and DMZ (default)**.
30. Click **OK** to save the settings.
31. Write the changes back to the device.

This concludes the configuration of the WWLAN access.

10.3.2 Switching between mobile profiles or SIM cards

If you have created different mobile profiles for a SIM card or one mobile profile for several SIM cards, LANmonitor allows you to toggle between these profiles or SIM cards. The following steps show you how to select an alternate profile or an alternate SIM card.

1. Select your device in LANmonitor.
2. On the entry **Mobile network**, open the context menu and select the option **Disconnect and switch mobile profile**.



3. Select the mobile profile that you want to switch to.

The device then disconnects from the mobile network and reconnects using the selected mobile profile.

10.3.3 Additions to the Status menu

Simstatus-Refresh

Using this action, you manually trigger the update of the SIM card status in the Simstatus table.

SNMP ID:

1.49.44

Telnet path:

Status > Modem-Mobile

Possible arguments:

none

10.3.4 Additions to the Setup menu

SIM-Slot

This parameter selects the SIM card slot that you want to link with the mobile profile.

SNMP ID:

2.23.41.1.12

Telnet path:

Setup > Interfaces > Mobile > Profiles

Possible values:

0 ... 2

10.4 Combined UMTS-GPRS operation for LTE devices

LCOS9.00 allows LTE/4G devices operating in areas without LTE/4G coverage to use a combined mode with both UMTS/3G and GPRS. Thus it is no longer necessary to manually set either UMTS/3G or GPRS.

10.4.1 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

UMTS

UMTS/3G mode only

GPRS

GPRS mode only

UMTS-GPRS

Combined UMTS/3G & GPRS mode

LTE

LTE/4G mode only

Default:

Auto

11 Other services

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

11.1 Deactivating device LEDs – boot-persistent

To operate an access point as unobtrusively as possible, you can disable the operating and status LEDs on the device. Even after restarting the device, the LEDs stay switched off. You can set up the device so that the LEDs light up briefly for a certain time after a restart, before the device disables them. This is useful for access points that are managed by WLAN controllers, for example to monitor the establishment of the connection to a WLAN controller.

You can set the operating mode of the LEDs in the **Display** section under **Management > Advanced**.

Display

CPU load averaging interval: 60s

LED mode: Normal

LED switch-off delay: 300 seconds

The selection list **LED mode** has three options to choose from:

Normal

The LEDs are always enabled, also after rebooting the device.

All off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

The "LED-Test" function is available despite the LEDs being disabled.



If you change this value and save it within the previously set time, you should restart the timer.

11.1.1 Additions to the Setup menu

LED mode

This sets the operating mode of the device LEDs.

The "LED test" function can still be run even if the LEDs are disabled.

SNMP ID:

2.11.90

Telnet path:

Setup > Config

Possible values:

On

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

Default:

On

LED-Off-Seconds

Here you set the time in seconds after which the device disables the LEDs following a restart.



If you change this to a value less than the previously set time, you have to save it and restart the timer.

SNMP ID:

2.11.91

Telnet path:

Setup > Config

Possible values:

Max. 4 characters 0123456789

Default:

300

11.2 Comment box for CRON jobs

As of LCOS9.00 you can add comments to CRON job entries.

11.2.1 Configuring the scheduler

The following tutorial shows you how to create a new CRON job and which parameters are available to you.

1. In LANconfig, open the configuration for your device.
2. Open the **Cron table** in the dialog **Date & Time > General** and click **Add...** to create a new CRON job.

3. Enter a time base.
The time base determines whether LCOS performs the timing of future actions based on the real time or the uptime of the device. With the setting **Real time**, the system evaluates time and dates. With the setting **Operating time**, the system evaluates only the minutes and hours since the device was last started.
4. The value for **Variation** specifies the maximum delay in minutes for the start of the CRON job after the specified start time.
The device determines the actual delay time at random. It lies between 0 and the time entered here. With the variation set to zero the CRON job will be executed at the specified time.

! Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.

5. Enter the minute(s), hour(s), day(s) of the week, day(s) of the month and the month(s) when your device should execute the specified command.
If you do not enter a value, your device ignores the corresponding value. For each parameter you can optionally specify a comma-separated list of values or a range of values (in the form of <Min . > - <Max . >).

The syntax of the field **Days of week** corresponds to the usual CRON interpretation:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0	1	2	3	4	5	6

i The day-of-the-week field is also significant for rules relating to the operating time. This is useful for actions that you perform only once when you start the device (i.e., with zero days uptime). In this way you can match the day of the week to the days of operating time, for example.

6. Under **Commands** you enter the command or a comma-separated list of commands.
Any command-line function can be executed.
7. Specify the **Owner** of the CRON job.

An owner is able to select an administrator defined in the device. If an owner is specified, then the CRON job commands will be executed with the rights of the owner.

8. A brief description of the CRON job can be entered in the **Comment** field.
9. Click **OK** to save the entry. You then write the configuration back to the device.

Other configuration examples:

Time base	At least	Hr.	W. days	M. days	Months	Command
Real time	0	4	0-6	1-31	1-12	do /so/man/disconnect internet
Real time	59	3	0-6	1-31	1-12	mailto:admin@mylancom.de?subject=Forced-disconnect?body=Manual Internet disconnect
Real time	0	0		1		do /setup/accounting/delete
Real time	0	18	1,2,3,4,5			do /so/man/connect MAINOFFICE

- The first entry disconnects from the ISP every morning at 04:00h (forced disconnect).
- The second entry sends a brief e-mail to the admin each morning at 03:59h, just before the forced disconnect.
- The third entry deletes the accounting table on the 1st day of each month.
- The fourth entry establishes a connection to the main office each weekday at 18:00h.



The device executes scheduled rules with an accuracy of one minute. Please ensure that the language you use to enter commands matches with that set for the console, otherwise scheduler commands will be ignored.

11.2.2 Additions to the Setup menu

Comment

This parameter is used to leave a comment about the entry in the CRON table.

SNMP ID:

2.11.20.12

Telnet path:

Setup > Config > Cron-Table

Possible values:

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

Default:

empty

11.3 LANCAPI disabled by default

As of LCOS9.00 LANCAPI is disabled for the individual interfaces by default.

11.3.1 Additions to the Setup menu

Active

You can specify if and how this interface is available for LANCAPi clients.

SNMP ID:

2.13.6.2

Telnet path:

Setup > LANCAPi > Interface-List

Possible values:**Yes**

The device allows all calls through this interface.

No

The device allows no calls through this interface.

Dial-only

The device only allows outgoing calls through this interface.

Dial-in only

The device only allows incoming calls through this interface.

Default:

No

11.4 DHCP snooping and DHCP option 82

In its original form, DHCP has no safeguards to protect from attacks on the assignment of the network configuration. For example, if a client sends a 'DHCP discover' packet on the network in order to retrieve a valid network configuration from a DHCP server, an attacker can send the client fake 'DHCP offer' packets and trick it into using a false default gateway (DHCP spoofing).

With DHCP snooping, the devices that receive and redirect DHCP packets are able to analyze and change these data packets, and to filter them by certain criteria. Additionally inserted information about the origin of the DHCP packets improves a DHCP server's capacity to manage extensive networks. Further, as this additional information is missing from the attacker's DHCP packets, they can no longer be used to interfere with the DHCP negotiations between DHCP servers, DHCP relay agents and the DHCP clients.

The access point supports DHCP snooping on layer 2. This enables it, for example, to add information (such as the SSID) to the DHCP packets received from the client on the WLAN before forwarding them to the LAN. The access point then adds the DHCP relay agent information option (option 82) according to RFC 3046.

In LANconfig you can set up DHCP snooping for each interface under **Interfaces > Snooping** and a click on **DHCP snooping**.

After selecting the appropriate interface, you can set the following:

Add agent info

Here you decide whether the DHCP relay agent appends incoming DHCP packets with the DHCP option "relay agent info" (option 82), or modifies an existing entry, before forwarding the request to a DHCP server.

The "relay agent info" is composed of values for the **Remote ID** and the **Circuit ID**.

On present agent info

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets. The following settings are possible:

- **Keep content:** In this setting, the DHCP relay agent forwards a DHCP packet and any existing "relay agent info" unchanged to the DHCP server.
- **Replace content:** In this setting, the DHCP relay agent replaces any existing "relay agent info" with the values specified in the fields **Remote ID** and **Circuit ID**.
- **Drop packet:** In this setting, the DHCP relay agent deletes any DHCP packet containing "relay agent info".

Remote ID

The remote ID is a sub-option of the "Relay agent info" option. It uniquely identifies the client making a DHCP request.

Circuit ID

The circuit ID is a sub-option of the "Relay agent info" option. It uniquely identifies the interface used by the client to make a DHCP request.

You can use the following variables for **Remote ID** and **Circuit ID**:

- **%:** Inserts a percent sign.
- **%c:** Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%i:** Inserts the name of the interface where the relay agent received the DHCP request.
- **%n:** Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- **%v:** Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p:** Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s:** Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- **%e:** Inserts the serial number of the relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

11.4.1 Additions to the Setup menu

DHCP snooping

Here you can configure DHCP snooping for each interface.

SNMP ID:

2.20.40

Telnet path:

Setup > LAN-Bridge

Port

Indicates the physical or logical interface to which this DHCP-snooping configuration applies.

SNMP ID:

2.20.40.1

Telnet path:

Setup > LAN-Bridge > DHCP-Snooping

Possible values:

LAN-x

All physical LAN interfaces

WLAN-x

All physical WLAN interfaces

WLAN-x-x

All logical WLAN interfaces

P2P-x-x

All logical P2P interfaces

WLC-TUNNEL-x

All virtual WLC tunnels

Add-Agent-Info

Here you determine how the DHCP relay agent handles the incoming DHCP packets, i.e. whether it appends the DHCP option "relay agent info" (option 82) or edits any existing "relay agent info", before forwarding the request to a DHCP server.

This option allows the relay agent to deliver additional information to the DHCP server about the interface used by the client to make the request.

The "relay agent info" consists of the **Remote ID** and the **Circuit ID**.

If these two fields are empty, the DHCP relay agent does not add any "relay agent info" to the data packets.

SNMP ID:

2.20.40.2

Telnet path:

Setup > LAN-Bridge > DHCP-Snooping

Possible values:**Yes**

Adds "relay agent info" to the DHCP packets.

No

This setting disables DHCP snooping for this interface.

Default:

No

Treat-Existing-Agent-Info

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets.

SNMP ID:

2.20.40.3

Telnet path:

Setup > LAN-Bridge > DHCP-Snooping

Possible values:**Keep**

In this setting, the DHCP relay agent forwards a DHCP packet and any existing "relay agent info" unchanged to the DHCP server.

Replace

In this setting, the DHCP relay agent replaces any existing "relay agent info" with the values specified in the fields **Remote ID** and **Circuit ID**.

Discard

In this setting, the DHCP relay agent deletes any DHCP packet containing "relay agent info".

Default:

Keep

Remote ID

The remote ID is a sub-option of the "Relay Agent Info" option. It uniquely identifies the client making a DHCP request.

You can use the following variables:

- **%**: Inserts a percent sign.
- **%c**: Adds the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%i**: Inserts the name of the interface on which the relay agent received the DHCP request.
- **%n**: Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For others clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

2.20.40.4

Telnet path:

Setup > LAN-Bridge > DHCP-Snooping

Possible values:

Max. 30 characters [A-Z][a-z][0-9]#@{ }~!\$%&'()*+,-./:;<=>?[\]^_.

Default:

empty

Circuit ID

The circuit ID is a sub-option of the "Relay Agent Info" option. It uniquely identifies the interface used by the client to make a DHCP request.

You can use the following variables:

- `%`: Inserts a percent sign.
- `%c`: Adds the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- `%i`: Inserts the name of the interface on which the relay agent received the DHCP request.
- `%n`: Inserts the name of the DHCP relay agent as specified under **Setup > Name**.
- `%v`: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- `%p`: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.
- `%s`: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For others clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the relay agent, to be found for example under **Status > Hardware-Info > Serial number**.

SNMP ID:

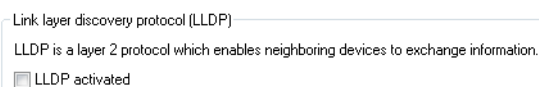
2.20.40.5

Telnet path:**Setup > LAN-Bridge > DHCP-Snooping****Possible values:**Max. 30 characters `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_.`**Default:***empty*

11.5 Enabling LLDP with LANconfig


As of LCOS 9.00, LLDP can also be enabled via LANconfig.

In LANconfig, LLDP is enabled under **Interfaces > LAN**.



11.6 Wildcard certificates in the LANCOM Content Filter

As of LCOS 9.00 you have the possibility of using wildcard certificates in the LANCOM Content Filter.

 To use the content filter properly a firewall rule must be applied that will check the HTTP traffic content.

☐ Activate Content Filter

Global Settings

In case of error: Forbidden

On license exceedance: Forbidden

On license expiration: Forbidden

Max. proxy connections: 1.000

Proxy processing timeout: 3.000 milliseconds

☐ Save content filter information at flash ROM activated

☐ Allow wildcard certificates

Allow wildcard certificates

With this feature enabled, Web sites with wildcard certificates (consisting of CN entries such as *.mydomain.com) are verified using the main domain (mydomain.com). Verification is evaluated in this sequence:

- Server name check in the "Client Hello" (depends on the browser used)
- Check of the CN in the SSL certificate that you received
- Entries with wildcards are ignored
- If the CN cannot be verified, the field "Alternative Name" is evaluated.
- DNS reverse lookup of the associated IP address and verification of the host name obtained
- If wildcards are included in the certificate, the main domain is checked instead (corresponds to the above function)
- Verification of the IP address

11.6.1 Additions to the Setup menu

Wildcard

With this feature enabled, Web sites with wildcard certificates (consisting of CN entries such as *.mydomain.com) are verified using the main domain (mydomain.com). The check takes place in this order:

- Verification of the server name in the "Client Hello" (depending on the browser used)
- Verification of the CN in the SSL certificate that you received
- Entries with wildcards are ignored
- If the CN cannot be verified, the field "Alternative Name" is evaluated
- DNS reverse lookup of the associated IP address and verification of the host name obtained
- If wildcards are included in the certificate, the main domain is checked instead (corresponds to the above function)
- Verification of the IP address

SNMP ID:

2.41.2.2.29

Telnet path:

Setup > UTM > Content-Filter > Global-Settings

Possible values:

No
Yes

Default:

No