LCOS LX 6.10

Addendum

02/2023

LANCOM
SYSTEMS

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under *gpl@lancom.de*.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

1 Addendum to LCOS LX version 6.10

This document describes the changes and enhancements in LCOS LX version 6.10 since the previous version.

2 Support for Wi-Fi 6E / 6 GHz band

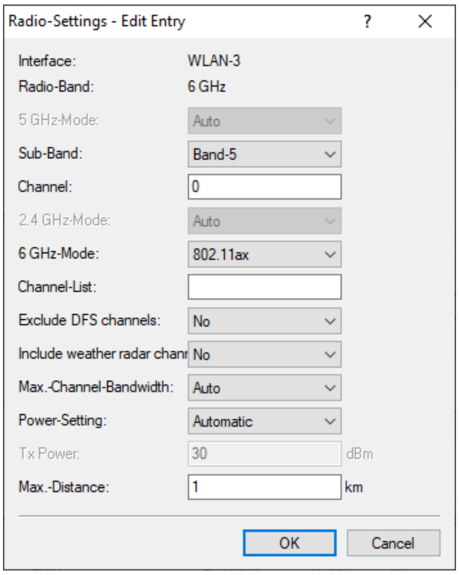
As of LCOS LX 6.10, the use of the 6 GHz frequency band for WLAN is supported.

The following settings have been modified or expanded if 6 GHz is to be operated:

Wireless-LAN > **WLAN-Networks** > **Radio-Settings**

For compatible access points, this table contains an additional entry "WLAN-3" for configuring the 6 GHz WLAN radio.

ⓘ As with the 2.4 GHz and 5 GHz radios, the frequency band cannot be changed. The radio WLAN-3 only supports the 6 GHz band.



Radio-Settings - Edit Entry

Interface:	WLAN-3	
Radio-Band:	6 GHz	
5 GHz-Mode:	Auto	
Sub-Band:	Band-5	
Channel:	0	
2.4 GHz-Mode:	Auto	
6 GHz-Mode:	802.11ax	
Channel-List:		
Exclude DFS channels:	No	
Include weather radar chanr	No	
Max.-Channel-Bandwidth:	Auto	
Power-Setting:	Automatic	
Tx Power:	30	dBm
Max.-Distance:	1	km

Sub-Band

The sub-band "Band-5" was added. The designation Band-5 is based on the FCC's U-NII nomenclature and corresponds to band U-NII-5. In the EU, only the 5925–6425 MHz frequency range is approved for WLAN in the 6 GHz band (which corresponds to band 5 or U-NII-5). For this reason, LCOS LX currently only offers the sub-band "Band-5" for selection.

Channel

In the 6 GHz band, the following channels can be configured in LCOS LX:

1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93

These channels are 20 MHz wide. If a channel width greater than 20 MHz is selected (default setting for the 6 GHz band: 160 MHz), the channel set here becomes the primary channel for the wider channel. In this way, the primary channel can also be freely selected within a >20 MHz-wide channel; all you have to do is enter the desired 20 MHz channel.

6 GHz-Mode

Only the latest 802.11ax standard is supported in the 6 GHz band. Consequently, this is the only one that can be selected.

Max. channel bandwidth

In Auto mode, a channel bandwidth of 160 MHz is always used for the 6 GHz band (2.4 GHz: 20Mhz; 5 GHz; 80 MHz). If desired, the channel bandwidth can be further restricted here.

Note on WLAN encryption in the 6 GHz band

Since the 6 GHz band is a completely new frequency band, backwards compatibility with older clients is not necessary. Similarly, outdated security methods are not supported. Specifically, this means

- that network encryption is exclusively based on WPA3. Accordingly, no transition mode or mixed mode such as WPA2/3 is available.
- Using Enhanced Open for ”open” networks (which thus offer encryption of the transmitted data). It is no longer possible to use open, unencrypted SSIDs.
- Protected Management Frames are mandatory

The conditions mentioned above can be set in the LCOS LX configuration. If an explicit configuration is not desired or possible (e.g. with mixed operation of the same SSID on several bands, which is a common application), the following adjustments are made dynamically by LCOS LX as soon as an SSID on the 6 GHz band is to be used:

- WPA versions <3 are automatically switched to WPA3
- Enhanced Open is enabled for open networks
- Protected Management Frames is activated

This makes it possible to continue using existing encryption profiles and to use a common configuration for an SSID that is also to be broadcast on 6 GHz. These settings are dynamically adjusted during operation, and there is no change to the configuration stored in the device.

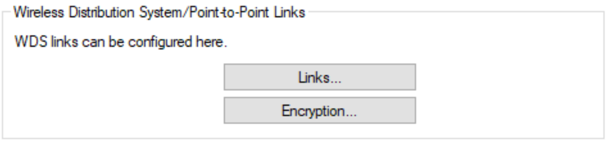
3 Wireless Distribution System (WDS) / point-to-point links

WDS can be used to set up point-to-point WLAN links between access points. These connections serve as a wireless backhaul, allowing remote access points to be connected to the rest of the network. This allows WLAN coverage to be provided even in areas where access points cannot be connected via Ethernet, for example.

These access points optionally offer SSIDs for connecting WLAN clients ("repeater" mode) or for connecting the wireless backhaul to its Ethernet port (wireless bridge).

With LCOS LX 6.10, WDS operation is validated over a maximum distance of 300 meters.

The WDS settings for your device are located under **Wireless-LAN** > **WDS**.



Wireless Distribution System/Point-to-Point Links

WDS links can be configured here.

Transmitting WLAN networks

One option of the WLAN configuration is to broadcast specific SSIDs over WDS links. You do this under **Wireless-LAN** > **WLAN-Networks** > **Network** in the selection field **WDS-Link**.

If you wish to implement the repeater mode, this configuration must also be duplicated on the remote access point that is connected via WDS.

Radio settings

The general radio settings made for the access point also apply to WDS links (in particular the setting of the WLAN channel). Configure this in the usual way under **Wireless-LAN** > **WLAN-Networks** > **Radio-Settings**.

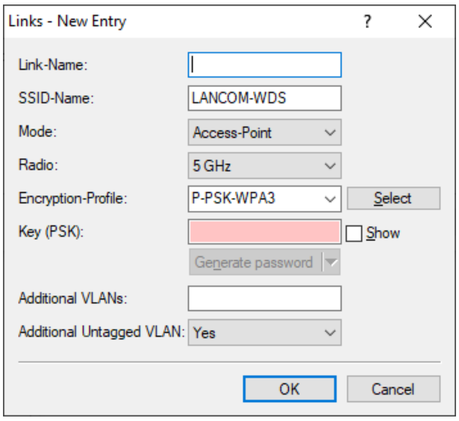
In particular, make sure that any specified channels or limitations to certain sub-bands match at both ends of the WDS link, otherwise the connection will not be established. Alternatively, automatic channel selection can be operated at both ends. In this case, the device searches through all permitted channels until the WDS partner is found.

Supported LANCOM devices

- LX-6500(E)
- LX-6400
- LX-6402
- LW-600
- OX-6400
- OX-6402
- OW-602
- LX-6200(E)

3.1 Connections

General settings relating to the WDS connection are configured under **Wireless-LAN** > **WDS** > **Links**. Add a line to the table for each WDS connection. By default, the table is empty.



Link-Name:
SSID-Name: LANCOM-WDS
Mode: Access-Point
Radio: 5 GHz
Encryption-Profile: P-PSK-WPA3
Key (PSK):
□ Show
Additional VLANs:
Additional Untagged VLAN: Yes

Link-Name

The name of the link. Used for further referencing in the device configuration.

SSID-Name

The name of the special SSID used for the WDS link. This name must match at both ends of the connection.

Mode

There are two roles for a WDS link: Access point and station. The partner configured as a station searches for the partner configured as an access point using the SSID configured above and initiates the connection.

In a point-to-multipoint scenario, multiple stations can connect to an access point.

The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above. In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

Encryption-Profile

The encryption profile to be used for the WDS link. We recommend the exclusive use of the default setting, WPA3.

Key (PSK)

The WPA-PSK used for the WDS link.

Additional VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

Additional Untagged VLAN

Untagged packets are to be transmitted.

3.2 Encryption

The settings for encryption and authentication of the Wireless Distribution System are configured under **Wireless-LAN** > **WDS** > **Encryption**.

For WDS connections, we recommend using WPA3 to guarantee maximum security.

The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-PSK-WPA2

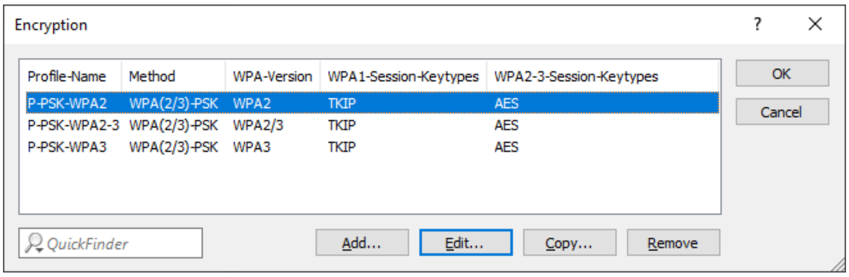
The authentication method used is WPA2 with pre-shared key (PSK), also known as WPA2-Personal. A key must be configured for the WLAN network.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.



Profile-Name	Method	WPA-Version	WPA1-Session-Keytypes	WPA2-3-Session-Keytypes
P-PSK-WPA2	WPA(2/3)-PSK	WPA2	TKIP	AES
P-PSK-WPA2-3	WPA(2/3)-PSK	WPA2/3	TKIP	AES
P-PSK-WPA3	WPA(2/3)-PSK	WPA3	TKIP	AES

Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

Method

Here you configure the encryption method. The following methods are available:

WPA

WPA(2/3)-PSK: WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal.

WPA-Version

Wi-Fi Protected Access (WPA) is an encryption method. Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA3: WPA version 3 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.
- WPA2/3: Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

ⓘ Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

WPA2/3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2 and 3. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

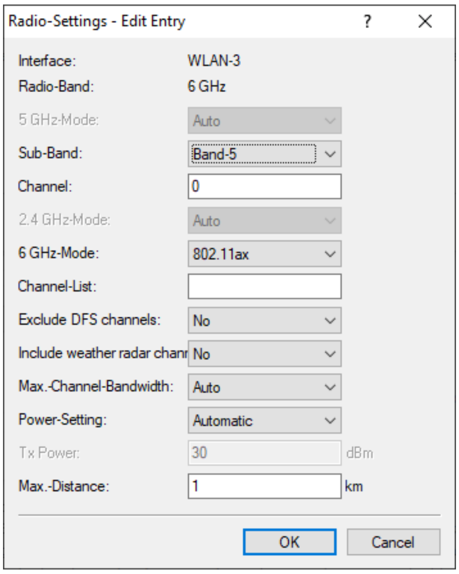
Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

ⓘ Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

3.3 Maximum distance

In addition, under **Wireless-LAN** > **WLAN-Networks** > **Radio-Settings** you have the option to specify the maximum distance to a WLAN station.



Interface:	WLAN-3
Radio-Band:	6 GHz
5 GHz-Mode:	Auto
Sub-Band:	Band-5
Channel:	0
2.4 GHz-Mode:	Auto
6 GHz-Mode:	802.11ax
Channel-List:	
Exclude DFS channels:	No
Include weather radar chanr	No
Max.-Channel-Bandwidth:	Auto
Power-Setting:	Automatic
Tx Power:	30 dBm
Max.-Distance:	1 km

Max.-Distance

Enter the distance to the most distant WLAN station here (e.g., to a WDS partner).

This setting is used to increase the internal timeout for WLAN ACK packets so that packets from a distant station can still be processed. Default is 1 kilometer.

3.4 Additions to the Setup menu

3.4.1 WDS link

Here you choose to broadcast specific SSIDs over WDS links. Also see *2.20.13.1.1 Link-Name* on page 12.

ⓘ If you wish to implement the repeater mode, this configuration must also be duplicated on the remote access point that is connected via WDS.

SNMP ID:

2.20.1.32

Console path:

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

Possible values:

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

3.4.2 WDS

The Wireless Distribution System (WDS) can be used to set up point-to-point WLAN links between access points. These connections serve as a wireless backhaul, allowing remote access points to be connected to the rest of the network. This allows WLAN coverage to be provided even in areas where access points cannot be connected via Ethernet, for example.

These access points optionally offer SSIDs for connecting WLAN clients (“repeater” mode) or for connecting the wireless backhaul to its Ethernet port (wireless bridge).

SNMP ID:

2.20.13

Console path:

Setup > **WLAN**

Links

In this table you configure the general settings for the WLAN networks (SSIDs) that are broadcast. Add a line to the table for each WLAN network. By default, the table is empty.

SNMP ID:

2.20.13.1

Console path:

Setup > **WLAN** > **WDS**

Link-Name

The name of the link. Used for further referencing in the device configuration.

SNMP ID:

2.20.13.1.1

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

SSID name

The name of the special SSID used for the WDS link. This name must match at both ends of the connection.

SNMP ID:

2.20.13.1.2

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

Mode

There are two roles for a WDS link: Access point and station. The partner configured as a station searches for the partner configured as an access point using the SSID configured above and initiates the connection.

In a point-to-multipoint scenario, multiple stations can connect to an access point.

> The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

> Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above. In station mode, however, only one WDS link can operate per device.
>
> Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

SNMP ID:

2.20.13.1.3

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

Access point
Station

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

SNMP ID:

2.20.13.1.4

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

2.4GHz

The SSID is only broadcast on the 2.4 GHz frequency.

5GHz
The SSID is only broadcast on the 5 GHz frequency.

6GHz
The SSID is only broadcast on the 6 GHz frequency.

Encryption-Profile

The encryption profile to be used for the WDS link. We recommend the exclusive use of the default setting, WPA3.

SNMP ID:

2.20.13.1.5

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

Max. 128 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Encryption-Key

The WPA-PSK used for the WDS link.

SNMP ID:

2.20.13.1.6

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

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

Additional-VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

SNMP ID:

2.20.13.1.8

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

Max. 128 characters from `[0-9],`

Additional-Untagged-VLAN

Non-VLAN tagged packets are transmitted via the WDS link.

SNMP ID:

2.20.13.1.10

Console path:

Setup > **WLAN** > **WDS** > **Links**

Possible values:

No

Non-VLAN tagged packets are not transmitted via the WDS link.

Yes

Non-VLAN tagged packets are transmitted via the WDS link.

Default:

Yes

Encryption

The settings for encryption and authentication of the Wireless Distribution System are configured in this table.

ⓘ For WDS connections, we recommend using WPA3 to guarantee maximum security.

SNMP ID:

2.20.13.2

Console path:

Setup > **WLAN** > **WDS**

Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

SNMP ID:

2.20.13.2.1

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

Max. 128 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Method

Here you configure the encryption method.

SNMP ID:

2.20.3.2.2

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

802.11i-WPA-PSK
WPA(2/3) with Pre-Shared-Key

WPA version

Here you configure the WPA version used for the encryption methods **802.11i WPA-PSK** and **802.11i WPA 802.1X**.

SNMP ID:

2.20.13.2.3

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

WPA1
WPA version 1 is used exclusively.

WPA2
WPA version 2 is used exclusively.

WPA3
WPA version 3 is used exclusively.

WPA1/2
Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.

WPA2/3
Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used.

ⓘ Operating TKIP is only recommended when using older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

SNMP ID:

2.20.13.2.4

Console path:

Setup > **WLAN** > **WDS** > **Encryption**

Possible values:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

WPA2 session keytypes

Here you configure the session key type to be used for WPA version 2 or 3. This also influences the encryption method used.

ⓘ Operating TKIP is only recommended when using older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

SNMP ID:

2.20.13.2.5

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

3.4.3 Max.-Distance

Enter the distance to the most distant WLAN station here (e.g., to a WDS partner).

This setting is used to increase the internal timeout for WLAN ACK packets so that packets from a distant station can still be processed. Default is 1 kilometer.

SNMP ID:

2.20.8.36

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Max. 2 characters from `[0-9]`

Default:

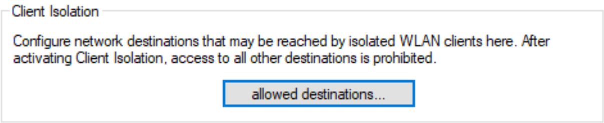
1

4 Client Isolation

From LCOS LX 6.10 you can prevent WLAN clients from communicating with one another or with unauthorized destinations on the network. Client isolation can be configured for this.

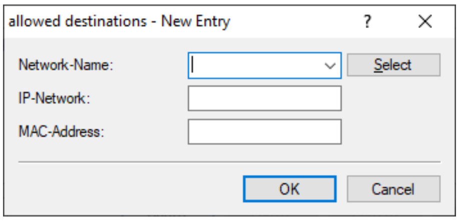
Data traffic from WLAN clients to destinations that are not explicitly whitelisted is prohibited.

Client isolation can be switched on per SSID. Configure this under **Wireless-LAN** > **WLAN-Networks** > **Network** > **Client Isolation**. Then configure the allowed destinations under **Wireless-LAN** > **WLAN-Networks** > **allowed destinations**.



Client Isolation

Configure network destinations that may be reached by isolated WLAN clients here. After activating Client Isolation, access to all other destinations is prohibited.



allowed destinations - New Entry

Network-Name:

IP-Network:

MAC-Address:

Network-Name

Select the network / SSID that the entry should apply for. Then enter either a destination IP address or destination MAC address.

In hotspot scenarios, the MAC address of the gateway should be entered here to ensure Internet access. It is not sufficient to specify its IP address because in this scenario the destination IP address is that of a destination on the Internet.

The feature automatically determines the appropriate gateway address from a DHCP negotiation between a WLAN client and a DHCP server. However, in roaming scenarios there is usually no renewed DHCP negotiation during roaming, so in this case the gateway must be explicitly whitelisted.

IP-Network

Allowed destination IP address for this network.

MAC-Address

Allowed destination MAC address for this network.

4.1 Additions to the Setup menu

4.1.1 Client-Isolation

Client isolation prevents WLAN clients from communicating with one another or with unauthorized destinations on the network.

Data traffic from WLAN clients to destinations that are not explicitly whitelisted is prohibited.

Client isolation can be switched on here for each SSID. Enter the allowed destinations under *2.20.5 Client-Isolation-Allowed* on page 20.

SNMP ID:

2.20.1.14

Console path:

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

Possible values:

No

No client isolation.

Yes

Client isolation is active for this network.

4.1.2 Client-Isolation-Allowed

Configure the allowed destinations for client isolation here. See also *2.20.1.14 Client-Isolation* on page 19.

SNMP ID:

2.20.5

Console path:

Setup > **WLAN**

Network-Name

Select the network / SSID that the entry should apply for. Then enter either a destination IP address (*2.20.5.2 IP network* on page 21) or destination MAC (*2.20.5.3 MAC-Address* on page 21) address.

In hotspot scenarios, the MAC address of the gateway should be entered here to ensure Internet access. It is not sufficient to specify its IP address because in this scenario the destination IP address is that of a destination on the Internet.

The feature automatically determines the appropriate gateway address from a DHCP negotiation between a WLAN client and a DHCP server. However, in roaming scenarios there is usually no renewed DHCP negotiation during roaming, so in this case the gateway must be explicitly whitelisted.

SNMP ID:

2.20.5.1

Console path:

Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

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

IP network

Allowed destination IP address for this network.

SNMP ID:

2.20.5.2

Console path:

Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

Max. 19 characters of an IPv4 address `a.b.c.d/xx`

MAC-Address

Allowed destination MAC address for this network.

SNMP ID:

2.20.5.3

Console path:

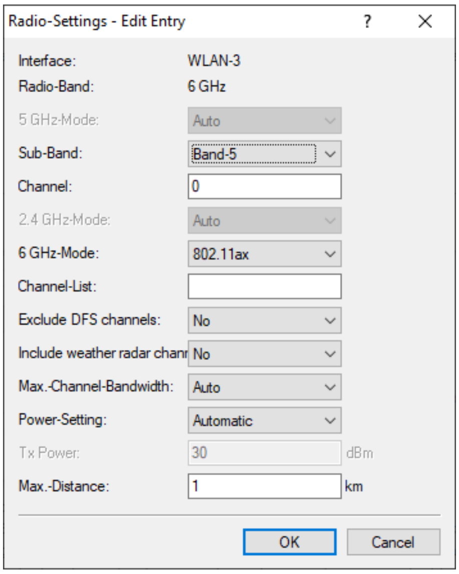
Setup > **WLAN** > **Client-Isolation-Allowed**

Possible values:

Max. 17 characters of a MAC address `xx:xx:xx:xx:xx:xx`

5 Include weather radar channels

From LCOS LX 6.10 you can use the 5 GHz channels which are otherwise reserved for weather radars. In LANconfig you configure this under **Wireless-LAN** > **WLAN-Networks** > **Radio-Settings** with the new setting **Include weather radar channels**.



Radio-Settings - Edit Entry

Interface:	WLAN-3
Radio-Band:	6 GHz
5 GHz-Mode:	Auto
Sub-Band:	Band-5
Channel:	0
2.4 GHz-Mode:	Auto
6 GHz-Mode:	802.11ax
Channel-List:	
Exclude DFS channels:	No
Include weather radar chann	No
Max.-Channel-Bandwidth:	Auto
Power-Setting:	Automatic
Tx Power:	30 dBm
Max.-Distance:	1 km

Include weather radar channels

The channels 120, 124 and 128 in the frequency range 5.6 to 5.65 MHz are used by weather radars. Although automatic channel selection does include these channels, they can also be selected specifically. If one of the channels is used, the DFS scan time (CAC time) increases from one to 10 minutes. During the scan, the 5 GHz radio cannot be reached by clients.

5.1 Additions to the Setup menu

5.1.1 Include-Weather-Radar-Channels

The channels 120, 124 and 128 in the frequency range 5.6 to 5.65 MHz are used by weather radars. Although automatic channel selection does include these channels, they can also be selected specifically. If one of the channels is used, the DFS scan time (CAC time) increases from one to 10 minutes. During the scan, the 5 GHz radio cannot be reached by clients.

SNMP ID:

2.20.8.35

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

No

Use channels reserved for weather radar.

Yes

Do not use channels reserved for weather radar.

6 Layer-3 Ethernet tunnel with L2TPv3

From LCOS LX 6.10 you can use L2TP to set up Ethernet tunnels. The configuration settings are described below for LANconfig, WEBconfig, and the CLI.

6.1 Layer-3 Ethernet tunnel with L2TPv3

LCOS LX supports the Layer 2 Tunneling Protocol (L2TP) in version 3. With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers, and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

L2TP uses two types of data:

Control data

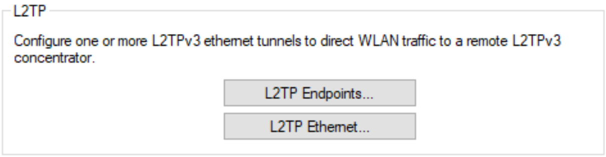
The control data are used to establish, maintain and tear down the tunnel connections. The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

Payload data

The payload data are encapsulated in Ethernet 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. You also have the option to operate multiple logical payload-data channels on each control-data channel.

LANconfig: **Miscellaneous Services** > **L2TP**

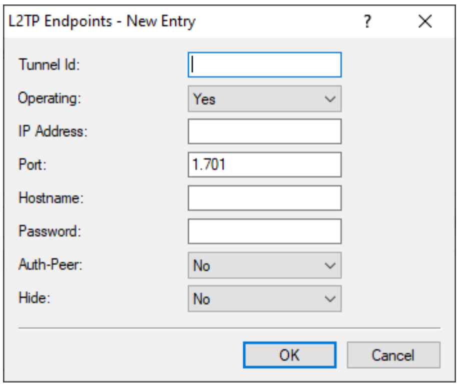


L2TP

Configure one or more L2TPv3 ethernet tunnels to direct WLAN traffic to a remote L2TPv3 concentrator.

6.1.1 L2TP Endpoints

Use **L2TP Endpoints** to configure the L2TP endpoints for the L2TPv3 tunnels. This configures the tunnel so that the control data makes an L2TP tunnel into a tunnel endpoint.



L2TP Endpoints - New Entry

Tunnel Id:	
Operating:	Yes
IP Address:	
Port:	1.701
Hostname:	
Password:	
Auth-Peer:	No
Hide:	No

Tunnel ID

The name of the tunnel endpoint. For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Operating

This L2TP endpoint is enabled or disabled.

IP Address

The IP address of the tunnel endpoint.

Port

UDP port to be used. Default: 1701

Hostname

User name for the authentication For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Password

The password for the authentication This is also used to hide the tunnel negotiations, if the function is activated.

Auth-Peer

Specifies whether the remote station should be authenticated.

Hide

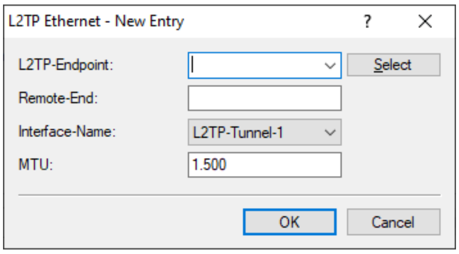
Specifies whether tunnel negotiations should be hidden by using the specified password.

Then connect a configured WLAN network to the virtual L2TP Ethernet interface.

To do this, go to **Wireless-LAN** > **WLAN-Networks** > **Network** and, for the desired entry, set the **Bridge** to the virtual L2TP Ethernet interface you just configured.

6.1.2 L2TP-Ethernet

The item **L2TP Ethernet** is used to configure the L2TPv3 tunnel between a WLAN network and an L2TP endpoint.



L2TP-Endpoint:
Remote-End:
Interface-Name: L2TP-Tunnel-1
MTU: 1.500

L2TP Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint.

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

Interface-Name

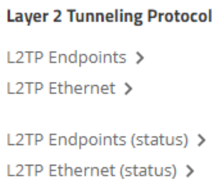
The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

MTU

This setting adjusts the MTU of an L2TP Ethernet tunnel to the specified value, e.g. when connecting the tunnel across networks with smaller MTUs. Possible values: 68-1500

6.2 Layer-3 Ethernet tunnel with L2TPv3

The settings for the Layer 3 Ethernet tunnel with L2TPv3 can be found in WEBconfig under **System configuration** > **Layer 2 Tunneling Protocol**.



LCOS LX supports the Layer 2 Tunneling Protocol (L2TP) in version 3. With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers, and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

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.

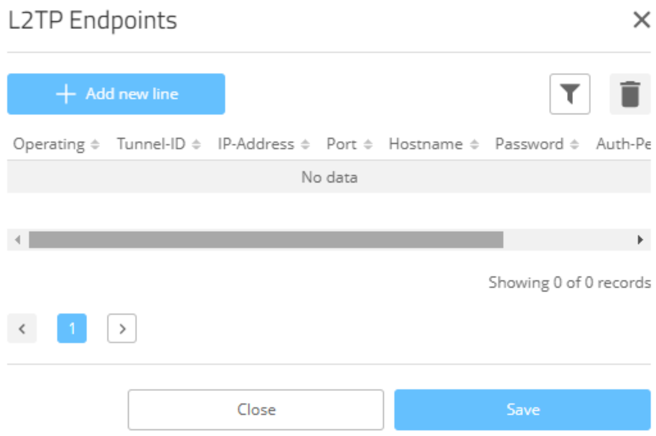
Payload data

The payload data are encapsulated in Ethernet 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. You also have the option to operate multiple logical payload-data channels on each control-data channel.

6.2.1 L2TP Endpoints

Use **L2TP Endpoints** to configure the L2TP endpoints for the L2TPv3 tunnels. This configures the tunnel so that the control data makes an L2TP tunnel into a tunnel endpoint.



Operating	Tunnel-ID	IP-Address	Port	Hostname	Password	Auth-Pe
No data						

Tunnel ID

The name of the tunnel endpoint. For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Operating

This L2TP endpoint is enabled or disabled.

IP Address

The IP address of the tunnel endpoint.

Port

UDP port to be used. Default: 1701

Hostname

User name for the authentication For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

Password

The password for the authentication This is also used to hide the tunnel negotiations, if the function is activated.

Auth-Peer

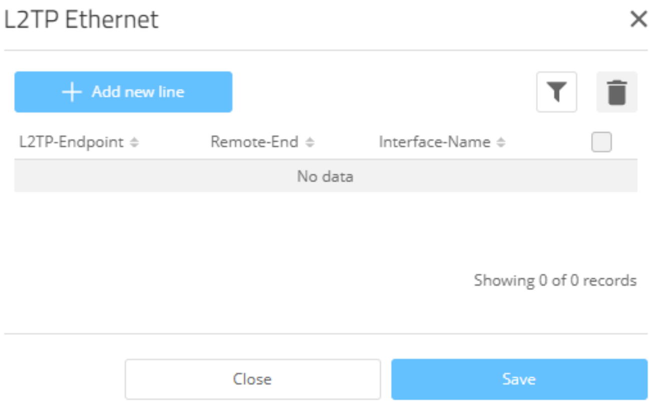
Specifies whether the remote station should be authenticated.

Hide

Specifies whether tunnel negotiations should be hidden by using the specified password.

6.2.2 L2TP Ethernet

The item **L2TP Ethernet** is used to configure the L2TPv3 tunnel between a WLAN network and an L2TP endpoint.


L2TP Ethernet

L2TP-Endpoint	Remote-End	Interface-Name	□
No data			

Showing 0 of 0 records

L2TP Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint.

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

Interface-Name

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

MTU

This setting adjusts the MTU of an L2TP Ethernet tunnel to the specified value, e.g. when connecting the tunnel across networks with smaller MTUs. Possible values: 68-1500

6.2.3 L2TP Status

Under **L2TP Endpoints (status)** and **L2TP Ethernet (status)**, you can see status information about the L2TP tunnels.

6.3 Additions to the Setup menu

6.3.1 L2TP

LCOS LX supports the Layer 2 Tunneling Protocol (L2TP) in version 3. With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers, and this allows WLAN traffic to be bridged through tunnels to the central site.

Data types

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 Ethernet 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. You also have the option to operate multiple logical payload-data channels on each control-data channel.

SNMP ID:

2.61

Console path:

Setup

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:

- **Tunnel-Id**: DEFAULT
- **Auth-Peer**: Yes
- **Hide**: No

All other values must remain 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:

2.61.1

Console path:

Setup > **L2TP**

Tunnel-Id

The name of the tunnel endpoint. For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

SNMP ID:

2.61.1.1

Console path:

Setup > **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:

2.61.1.2

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

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

Port

UDP port to be used.

SNMP ID:

2.61.1.3

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

0 … 65535

Default:

1701

Host name

User name for the authentication For an authenticated L2TP tunnel to be established between two devices, the entries for **Tunnel-Id** and **Hostname** need to match.

SNMP ID:

2.61.1.4

Console path:

Setup > **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:

2.61.1.5

Console path:

Setup > **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:

2.61.1.6

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

Peer does not have to be authenticated.

Yes

Peer must be authenticated.

Default:

No

Hide

Specifies whether tunnel negotiations should be hidden by using the specified password.

SNMP ID:

2.61.1.7

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

Tunnel negotiation is not obfuscated.

Yes

Tunnel negotiation is obfuscated.

Default:

No

Operating

This L2TP endpoint is enabled or disabled.

SNMP ID:

2.61.1.8

Console path:

Setup > **L2TP** > **Endpoints**

Possible values:

No

L2TP endpoint is disabled.

Yes

L2TP endpoint is enabled.

Default:

Yes

Ethernet

This table is used to link the L2TPv3 endpoints with a WLAN network.

SNMP ID:

2.61.2

Console path:

Setup > **L2TP**

L2TP-Endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table (<xref href="2_61_1_1.dita"/>). This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need "to run" via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

SNMP ID:

2.61.2.1

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

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

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

SNMP ID:

2.61.2.2

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

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

Interface name

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

SNMP ID:

2.61.2.3

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16
16 virtual L2TP Ethernet interfaces

MTU

This setting adjusts the MTU of an L2TP Ethernet tunnel to the specified value, e.g. when connecting the tunnel across networks with smaller MTUs.

SNMP ID:

2.61.2.4

Console path:

Setup > **L2TP** > **Ethernet**

Possible values:

68 … 1500

Default:

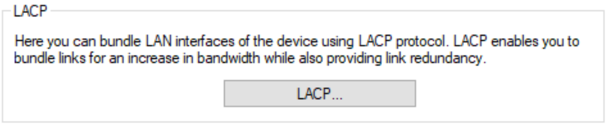
1500

7 Link Aggregation (LACP)

Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle LAN ports into a virtual link. Physical connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

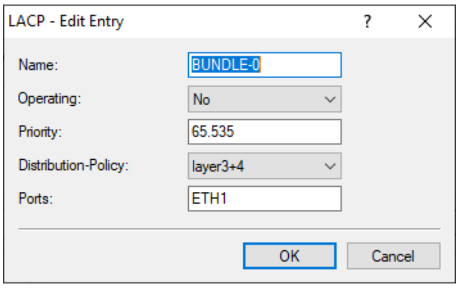
LANconfig: **Miscellaneous Services** > **Link Aggregation**


LACP

Here you can bundle LAN interfaces of the device using LACP protocol. LACP enables you to bundle links for an increase in bandwidth while also providing link redundancy.

7.1 LACP (Link Aggregation Control Protocol)

The **LACP** menu is used to configure the Link Aggregation Control Protocol.


LACP - Edit Entry

Name: BUNDLE-0

Operating: No

Priority: 65.535

Distribution-Policy: layer3+4

Ports: ETH1

Name

This is the logical interface used to bundle the selected physical interfaces.

Operating

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together into one common logical bundled interface. In the disabled state the interfaces that are selected in the corresponding table still operate as individual interfaces.

Priority

Enter the LACP system priority. The default value is 65,535.

Distribution-Policy

There are a number of options for distributing the network packets to the various bundled interfaces. The following characteristics are used for distribution:

layer2

MAC addresses

layer2+3

A combination of MAC addresses and IP addresses

layer3+4

IP addresses and TCP/UDP ports

encap2+3

Like layer2+3. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

encap3+4

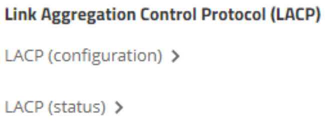
Like layer3+4. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

Ports

Use this parameter to select the physical interfaces as a comma-separated list that the device bundles via LACP. Default: ETH1,ETH2

7.2 Link Aggregation Control Protocol (LACP)

The settings for the Link Aggregation Control Protocol (LACP) can be found in WEBconfig under **System configuration** > **Link Aggregation Control Protocol (LACP)**.



Link Aggregation Control Protocol (LACP)

LACP (configuration) >

LACP (status) >

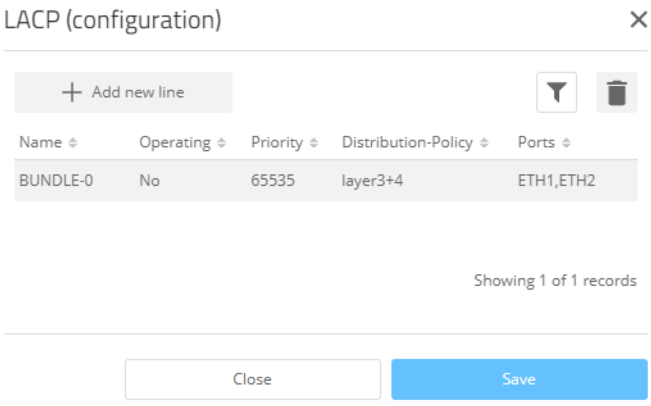
Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle LAN ports into a virtual link. Physical connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

LANconfig: **Miscellaneous Services** > **Link Aggregation**

7.2.1 L2TP Endpoints

The **LACP** menu is used to configure the Link Aggregation Control Protocol.



LACP (configuration)

Name	Operating	Priority	Distribution-Policy	Ports
BUNDLE-0	No	65535	layer3+4	ETH1,ETH2

Showing 1 of 1 records

Name

This is the logical interface used to bundle the selected physical interfaces.

Operating

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together into one common logical bundled interface. In the disabled state the interfaces that are selected in the corresponding table still operate as individual interfaces.

Priority

Enter the LACP system priority. The default value is 65,535.

Distribution-Policy

There are a number of options for distributing the network packets to the various bundled interfaces. The following characteristics are used for distribution:

layer2

MAC addresses

layer2+3

A combination of MAC addresses and IP addresses

layer3+4

IP addresses and TCP/UDP ports

encap2+3

Like layer2+3. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

encap3+4

Like layer3+4. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

Ports

Use this parameter to select the physical interfaces as a comma-separated list that the device bundles via LACP. Default: ETH1,ETH2

7.2.2 LACP (Status)

The item **LACP (Status)** displays status information on the LACP connections.

7.3 Additions to the Setup menu

7.3.1 LAN

This item contains the settings relating to the LAN connection of the access point.

SNMP ID:

2.62

Console path:

Setup

LACP

Significant improvements in terms of failover reliability and performance come with support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle LAN ports into a virtual link. Physical connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

SNMP ID:

2.62.1

Console path:

Setup > **LAN**

Name

This parameter shows the logical cluster interface used for bundling the selected physical interfaces of the devices.

SNMP ID:

2.62.1.1

Console path:

Setup > **LAN** > **LACP**

Possible values:

Max. 9 characters from `` [A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Default:

BUNDLE-0

Operating

Using this parameter, you enable or disable interface bundling.

With bundling enabled, the device groups the selected device interfaces together into one common logical bundled interface. In the disabled state the interfaces that are selected in the corresponding table still operate as individual interfaces.

SNMP ID:

2.62.1.2

Console path:

Setup > **LAN** > **LACP**

Possible values:

No
Yes

Priority

Enter the LACP system priority.

SNMP ID:

2.62.1.3

Console path:

Setup > **LAN** > **LACP**

Possible values:

Multiples of 4096 `Max. 6 characters from [0-9]`

Default:

65535

Distribution-Policy

There are a number of options for distributing the network packets to the various bundled interfaces. The following characteristics are used for distribution:

layer2

MAC addresses

layer2+3

A combination of MAC addresses and IP addresses

layer3+4

IP addresses and TCP/UDP ports

encap2+3

Like layer2+3. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

encap3+4

Like layer3+4. However, in the case of encapsulated protocols, an attempt is made to obtain this information from the inner protocol

SNMP ID:

2.62.1.4

Console path:

Setup > **LAN** > **LACP**

Possible values:

layer2
layer2+3
layer3+4
encap2+3
encap3+4

Default:

layer3+4

Ports

Use this parameter to select the physical interfaces as a comma-separated list that the device bundles via LACP.

SNMP ID:

2.62.1.5

Console path:

Setup > **LAN** > **LACP**

Possible values:

Max. 16 characters from `` [A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Default:

ETH1,ETH2