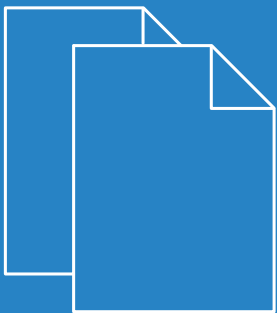


LCOS LX 5.36

Addendum



Contents

- 1 Addendum to LCOS LX version 5.36.....4**
- 2 Adjusting the admin password criteria.....5**
- 3 Delayed reboot.....6**
 - 3.1 Additions to the Setup menu.....6
 - 3.1.1 Delayed-Reboot.....6
 - 3.1.2 Cancel-Delayed-Reboot.....6
- 4 writeconfig command.....7**
- 5 Untagged VLAN for further Ethernet ports.....8**
 - 5.1 Additions to the Setup menu.....8
 - 5.1.1 Untagged-VLAN.....8
- 6 ARP handling.....10**
 - 6.1 Additions to the Setup menu.....12
 - 6.1.1 ARP handling.....12
- 7 Opportunistic Key Caching.....13**
 - 7.1 Additions to the Setup menu.....15
 - 7.1.1 OKC.....15
- 8 LANCOM Layer 2 Management protocol (LL2M).....16**
 - 8.1 LL2M configuration.....16
 - 8.2 Additions to the Setup menu.....19
 - 8.2.1 LL2M.....19

Copyright

© 2022 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

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 (ey@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 5.36

This document describes the changes and enhancements in LCOS LX version 5.36 since the previous version.

2 Adjusting the admin password criteria

From LCOS LX 5.36 an admin password that is set during the initial commissioning with WEBconfig must meet the following criteria:

- > At least 8 characters
- > At least one letter
- > At least one digit
- > At least one special character

3 Delayed reboot

The command `do /Other/Delayed-Reboot [<seconds>]` restarts the device after the specified number of seconds.

The command `do /Other/Cancel-Delayed-Reboot` cancels the reboot again if it is entered within the specified time.

This feature is used when operating with some management systems.

3.1 Additions to the Setup menu

3.1.1 Delayed-Reboot

This action is used to restart the device after a delay. The delay is specified in seconds.

Example: `do Delayed-Reboot 30`

SNMP ID:

—

Console path:

Other

3.1.2 Cancel-Delayed-Reboot

This action lets you interrupt a delayed restart initiated with `do Delayed reboot` within the delay time.

Example: `do Cancel-Delayed-Reboot`

SNMP ID:

—

Console path:

Other

4 writeconfig command

By executing the `writeconfig` command in a CLI session, a configuration in LCF format can be transferred to the device, which is then applied and made persistent.

Appending the parameter `noflash` means that the transferred configuration is not made persistent. This can be done subsequently by running the `flash` command. This feature is mainly relevant for operating with some management systems.

Command	Description
<code>writeconfig [noflash]</code>	<p>Writes a new configuration in the LCF file format to the device. The system interprets all of the following lines as configuration values until two empty lines are read. This is used by management systems, for example. Possible arguments are:</p> <ul style="list-style-type: none">➤ <code>noflash</code>: The transferred configuration is not persistent. This can be done subsequently by running the <code>flash</code> command.

5 Untagged VLAN for further Ethernet ports

If a device has more than one Ethernet port, the other Ethernet ports can optionally be configured with an untagged VLAN. The untagged VLAN is used without a VLAN tag on the other LAN port and is used, for example, to integrate network devices that are not VLAN-capable. The other Ethernet port thus acts as an access port.

The following access points with LCOS LX are equipped with more than one Ethernet port and thus support this feature:

- > LANCOM LW-500
- > LANCOM LX-6400
- > LANCOM LX-6402
- > LANCOM OW-602

5.1 Additions to the Setup menu

5.1.1 Untagged-VLAN

If a device has more than one Ethernet port, the other Ethernet ports can optionally be configured with an untagged VLAN. The untagged VLAN is used without a VLAN tag on the other LAN port and is used, for example, to integrate network devices that are not VLAN-capable. The other Ethernet port thus acts as an access port. The untagged ports and their VLAN tag are specified in this table.

SNMP ID:

2.70.8

Console path:

Setup > IP-Configuration

Port

Enter a port for the untagged VLAN.

SNMP ID:

2.70.8.1

Console path:

Setup > IP-Configuration > Untagged-VLAN

Possible values:

ETH1
ETH2
...

VLAN

Specify a VLAN ID for the untagged VLAN.

SNMP ID:

2.70.8.2

Console path:

Setup > IP-Configuration > Untagged-VLAN

Possible values:

0 ... 4095

Special values:

0

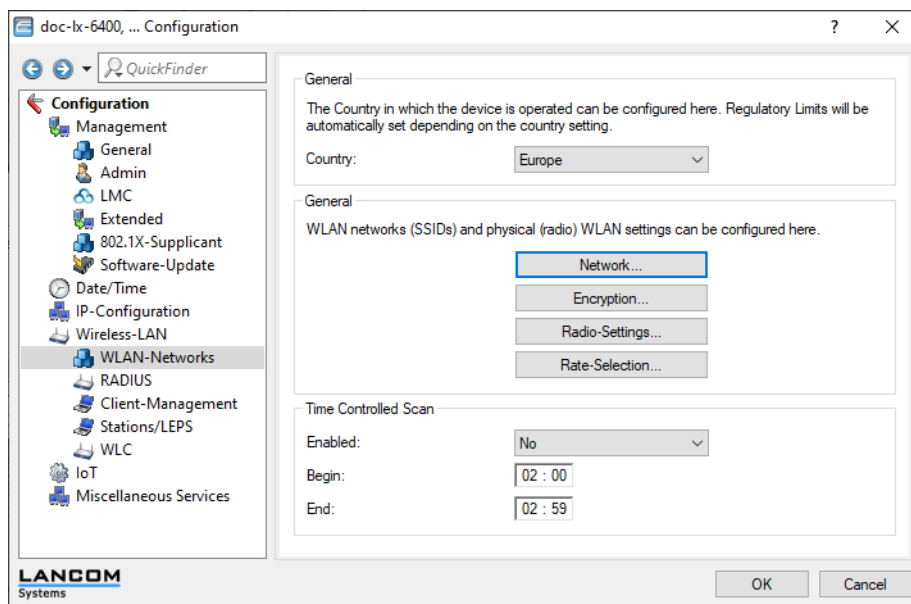
The default value 0 means that no VLAN is used.

6 ARP handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If "ARP handling" is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

Configuration by LANconfig

The ARP handling is configured under **Wireless-LAN > WLAN-Networks > Network**.



ARP handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If "ARP handling" is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point identifies the IP address / MAC address assignment from the DHCP messages that are exchanged between the WLAN client and the DHCP server. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

i If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to "On".

! If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to "Strict". This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

Off

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. ARP requests are only forwarded to the WLAN if the IP address/MAC address assignment could not be determined.

Strict

ARP handling enabled. ARP requests are not routed to the WLAN.

Configuration by WEBconfig

The ARP handling is configured under **Wi-Fi configuration > SSID**.

Networks	Communication between clients on this SSID	Bandwidth limits (Mbps)	Timing	VLAN	Miscellaneous
Names: NETWORK SSID: LANCOM	<input checked="" type="radio"/> allow <input type="radio"/> disallow	per SSID <input type="text" value="0"/>	Timeframe ALWAYS	VLAN-ID <input type="text" value="0"/>	Multicast-to-Unicast No
		per client <input type="text" value="0"/>	<input type="button" value="Edit Timeframes"/>		ARP-Handling Off

Other

ARP handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If "ARP handling" is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point identifies the IP address / MAC address assignment from the DHCP messages that are exchanged between the WLAN client and the DHCP server. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

i If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to "On".

! If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to "Strict". This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

Off

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. ARP requests are only forwarded to the WLAN if the IP address/MAC address assignment could not be determined.

Strict


ARP handling enabled. ARP requests are not routed to the WLAN.


6.1 Additions to the Setup menu

6.1.1 ARP handling

Clients in the wireless network that are on standby do not reliably answer the ARP requests from other network stations. If "ARP handling" is activated, the access point takes over this task and answers the ARP requests on behalf of stations that are on standby. In large networks, this means more efficient use is made of the medium time because ARP queries and responses no longer have to be sent to the WLAN client, but are instead answered by the access point.

The LCOS LX access point identifies the IP address / MAC address assignment from the DHCP messages that are exchanged between the WLAN client and the DHCP server. If the assignment is known, ARP requests are answered by the access point and no longer forwarded to the client.

 If the IP address/MAC address assignment could not be determined, ARP requests are still routed to the WLAN with the operating mode set to "On".

 If the IP address/MAC address assignment could not be determined, ARP requests are not routed to the WLAN with the operating mode set to "Strict". This means, for example, that no connection can be initiated from the LAN to WLAN clients with fixed IP addresses (no DHCP). In this case, this feature should not be employed.

SNMP ID:

2.20.1.28

Console path:**Setup > WLAN > Network****Possible values:****Off**

ARP handling disabled. ARP requests are always routed to the WLAN.

On

ARP handling enabled. ARP requests are only forwarded to the WLAN if the IP address/MAC address assignment could not be determined.

Strict

ARP handling enabled. ARP requests are not routed to the WLAN.

Default:

Off

7 Opportunistic Key Caching

Configuration by LANconfig

Opportunistic Key Caching is configured under **Wireless-LAN > WLAN-Networks > Encryption**.

The screenshot shows the 'Encryption - New Entry' dialog box with the following settings:

- Profile-Name: P-PSK
- Encryption: Yes
- Method: WPA(2/3)-PSK
- WPA-Version: WPA2
- WPA1-Session-Keytypes: TKIP
- WPA2-3-Session-Keytypes: AES
- Encrypt manag. frames: No
- WPA-Rekeying-Cycle: 0
- Pre-Authentication: Yes
- OKC: No
- WPA2-Key-Management: Standard
- SAE/OWE-Groups:
 - DH-19
 - DH-20
 - DH-21
- PMK-IAPP-Secret: [Redacted] Show
- Generate password: [Dropdown]
- RADIUS-Server-Profile: [Dropdown]

OKC (Opportunistic Key Caching)

This option enables or disables the Opportunistic Key Caching (OKC).

The authentication of WLAN clients via EAP and 802.1X is now standard in company networks, and for public Internet access, too, it is part of the Hotspot 2.0 specification. The disadvantage of authentication via 802.1X is the noticeably longer time between authenticating and connecting due to the exchange of up to twelve data packets between the WLAN client and access point. This may not matter for most applications that only involve exchanging data. However, time-critical applications such as Voice-over-IP rely on fast authentication when moving between WLAN radio cells so as not to impair communications.

Various authentication strategies have been established to counteract this, including PMK caching and pre-authentication, although pre-authentication by no means solves all of the problems. For one thing, there is no guarantee that the WLAN client can detect whether the access point is capable of pre-authentication. Also, pre-authentication causes a considerable load on the RADIUS server, because it has to process the authentications of all clients and all access points on the WLAN network.

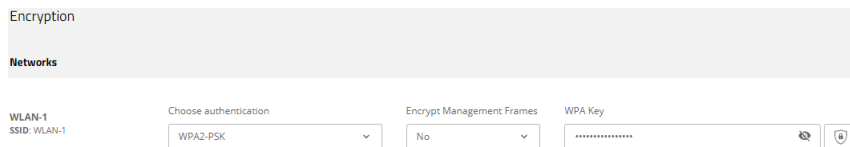
With Opportunistic Key Caching, the management of WLAN client keys is moved to a WLAN controller (WLC) or central switch, which manages all of the access points in the network. When a client authenticates at an access point, the downstream WLC, which acts as the authenticator, performs the key management and returns the PMK to the access point for forwarding to the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID, and it sends this to the new access point in the expectation that OKC is enabled (i.e. "opportunistic"). If the access point is unable to handle the PMKID, it negotiates a regular 802.1X authentication with the client.

A LANCOM access point is even able to perform OKC if the WLC is temporarily unavailable. In this case it stores the PMK and sends it to the WLC, once available again. The WLC then sends the PMK to all of the access points in the network so that the client can continue to use OKC when moving between cells.

In networks managed from the LANCOM Management Cloud (LMC) or networks from standalone access points, the PMKs are transmitted via the IAPP protocol. In LMC-managed networks, the IAPP is configured automatically. In networks made up with standalone access points, you have to ensure that the PMK-IAPP secret is configured and identical on every access point in the network.

Configuration by WEBconfig

Opportunistic Key Caching is configured under **Wi-Fi configuration > Encryption**.



OKC (Opportunistic Key Caching)

This option enables or disables the Opportunistic Key Caching (OKC).

The authentication of WLAN clients via EAP and 802.1X is now standard in company networks, and for public Internet access, too, it is part of the Hotspot 2.0 specification. The disadvantage of authentication via 802.1X is the noticeably longer time between authenticating and connecting due to the exchange of up to twelve data packets between the WLAN client and access point. This may not matter for most applications that only involve exchanging data. However, time-critical applications such as Voice-over-IP rely on fast authentication when moving between WLAN radio cells so as not to impair communications.

Various authentication strategies have been established to counteract this, including PMK caching and pre-authentication, although pre-authentication by no means solves all of the problems. For one thing, there is no guarantee that the WLAN client can detect whether the access point is capable of pre-authentication. Also, pre-authentication causes a considerable load on the RADIUS server, because it has to process the authentications of all clients and all access points on the WLAN network.

With Opportunistic Key Caching, the management of WLAN client keys is moved to a WLAN controller (WLC) or central switch, which manages all of the access points in the network. When a client authenticates at an access point, the downstream WLC, which acts as the authenticator, performs the key management and returns the PMK to the access point for forwarding to the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID, and it sends this to the new access point in the expectation that OKC is enabled (i.e. "opportunistic"). If the access point is unable to handle the PMKID, it negotiates a regular 802.1X authentication with the client.

A LANCOM access point is even able to perform OKC if the WLC is temporarily unavailable. In this case it stores the PMK and sends it to the WLC, once available again. The WLC then sends the PMK to all of the access points in the network so that the client can continue to use OKC when moving between cells.

In networks managed from the LANCOM Management Cloud (LMC) or networks from standalone access points, the PMKs are transmitted via the IAPP protocol. In LMC-managed networks, the IAPP is configured automatically. In networks made up with standalone access points, you have to ensure that the PMK-IAPP secret is configured and identical on every access point in the network.

7.1 Additions to the Setup menu

7.1.1 OKC

This option enables or disables the Opportunistic Key Caching (OKC).

SNMP ID:

2.20.3.17

Console path:

Setup > WLAN > Encryption

Possible values:

No

OKC is enabled.

Yes

OKC is not enabled.

8 LANCOS Layer 2 Management protocol (LL2M)

From LCOS LX 5.36 you can use LL2M for device configuration. The configuration settings in WEBconfig are located under **System configuration > LL2M configuration**.

8.1 LL2M configuration

The settings for LL2M in WEBconfig are located under **System configuration > LL2M configuration**.

LL2M configuration >

Operating: Yes
Status: running, reachable from LAN

Interfaces >

Operation

A basic pre-requisite for all methods device configuration is for an IP connection to exist between the configuration computer and the device. No matter whether you use LANconfig, WEBconfig or SSH; it is impossible to send any configuration commands to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. The only option in this case is to access the device via the serial configuration interface, which however is not available on all devices, or to reset the device to its factory settings. However, both options require physical access to the device—this may not always be the case for the concealed installation of access points and can represent considerable overhead for larger-scale installations.

The **LANCOM Layer 2 Management Protocol (LL2M)** is used to also enable configuration access to a device even without an IP connection. All this protocol requires is a connection on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server, which then responds to the requests or runs the commands. Both the LL2M client and the LL2M server are integrated in the LCOS LX. The LL2M client commands are executed via the command line or WEBconfig.

An encrypted tunnel is set up for every LL2M command to protect the transmitted log-in information. To use the integrated LL2M client, start a terminal session on a device that has local access to the LL2M server via the available physical medium (LAN, WLAN). In this CLI session you can use the following commands to contact the LL2M server: `LL2Mdetect` and `LL2Mexec`.

Enable LL2M here.



Access points of type LANCOM LW-500 can only be found and configured via LL2M if LL2M packets reach the access point with a VLAN tag which is included in the configuration of the access point (WLAN SSID configuration or management VLAN configuration).

Status

Shows the status of the current LL2M configuration.

Interfaces

This item is used to specify the interfaces or Ethernet ports where the LL2M server can be reached. The presetting provides accessibility on all Ethernet ports.

LL2M configuration: Interfaces
✕

🔍
🗑️

Port ↕	Active ↕
ETH1	Yes
ETH2	Yes

Showing 2 of 2 records

<
1
>

Close
Save

CLI commands `ll2mdetect` and `ll2mexec`

Command	Description
<code>ll2mdetect</code>	<p>LL2Mdetect finds LL2M-capable devices in the network.</p> <p>The LL2M client uses this command to send a SYSINFO request to the LL2M server. The server then sends its system information, such as hardware and serial number, back to the client for display. The LL2Mdetect command can be restricted with the following parameters:</p> <p>-a <MAC-address></p> <p>Restricts the command to those devices with the specified MAC address only. Enter the MAC address in the format <code>00a057010203</code>, <code>00-a0-57-01-02-03</code> or <code>00:a0:57:01:02:03</code>.</p> <p>If no MAC limitations are set, the "detect" is sent as a multicast (or alternatively using <code>-b</code> as a broadcast) to all LL2M-compatible devices. To contact groups of MAC addresses, <code>*</code> and <code>x</code> can be used as wildcards in individual MAC address positions, e.g., <code>00-a0-57-xx-xx-xx</code> for all device MAC addresses.</p> <p>! In a command line with multiple parameters, the final parameter must be <code>-a</code>. A different order is not allowed.</p>

Command	Description
	<p>-b</p> <p>Explicitly sends the LL2Mdetect request as a broadcast and not as a multicast.</p> <p>-f <Version></p> <p>Restricts the command to those devices with the corresponding firmware version only.</p> <p>-r <Hardware-Release></p> <p>Restricts the command to those devices with the corresponding hardware release only.</p> <p>-s <Serial number></p> <p>Restricts the command to those devices with the corresponding serial number only.</p> <p>-t <Hardware-Type></p> <p>Restricts the command to those devices of the corresponding hardware type only.</p> <p>-v <VLAN-ID></p> <p>Only sends the LL2Mdetect request on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.</p>
	<p>The command <code>ll2mdetect -r A</code> sends a SYSINFO request to all devices of the hardware release "A". The response from the LL2M server then contains the following information:</p> <ul style="list-style-type: none"> > Device name > Device type > Serial number > MAC address > Hardware release > Firmware version with date
ll2mexec	<p>The command <code>ll2mexec</code> sends commands to or initiates terminal sessions on devices found by <code>ll2mdetect</code>.</p> <p>The LL2M client uses this command to send a single-line command to run on the LL2M server. Multiple commands can be combined in one LL2M command by using semicolons as separators. Depending on the command, the actions are run on the remote device and the responses from the remote device are sent to the LL2M client for display. The LL2Mexec command conforms to the following syntax:</p> <pre>ll2mexec <User>[:<Password>]@<MAC address></pre>
	<p>The LL2Mexec command can be restricted with the following parameters:</p> <p>-i <(W) LAN-Interface></p> <p>Sends the LL2Mexec command via the specified (W)LAN interface only.</p>

Command	Description
	<p>-v <VLAN-ID></p> <p>Only sends the LL2Mexec command on the VLAN specified. If no VLAN ID is specified, the VLAN ID of the first defined IP network is used.</p> <p>For example, the command line <code>ll2mexec root@00a057010203 set /setup/name MyDevice</code> logs in the LL2M client as "root" on the LL2M server with the MAC address "00a057010203". Since the password was not included, the device first looks for the corresponding username in the local database and automatically uses the password for this user. If the username is also not included, the login data of the currently registered user for the CLI session is used. Then the LL2M client sets the name of the remote device to the value 'MyDevice'.</p>

8.2 Additions to the Setup menu


8.2.1 LL2M


A basic pre-requisite for all methods device configuration is for an IP connection to exist between the configuration computer and the device. No matter whether you use LANconfig, WEBconfig or SSH; it is impossible to send any configuration commands to the device without an IP connection. In the event of erroneous configuration of the TCP/IP settings or VLAN parameters, this IP connection may be impossible to establish. In these cases, the only help is to reset the device to its factory default settings. This option requires physical access to the device, which may not always be possible with concealed access point installations and may mean a considerable overhead for large-scale installations.

The **LANCOM Layer 2 Management Protocol (LL2M)** is used to also enable configuration access to a device even without an IP connection. All this protocol requires is a connection on layer 2 (i.e. via Ethernet directly or via layer-2 switches) to establish a configuration session. LL2M connections are supported on LAN or WLAN connections, but not via WAN. Connections via LL2M are password protected and are resistant to replay attacks.

LL2M establishes a client-server structure for this purpose: The LL2M client sends requests or commands to the LL2M server, which then responds to the requests or runs the commands. Both the LL2M client and the LL2M server are integrated in LCOS LX. The LL2M client commands are executed via the command line or WEBconfig.

An encrypted tunnel is set up for every LL2M command to protect the transmitted log-in information. To use the integrated LL2M client, start a terminal session on a device that has local access to the LL2M server via the available physical medium (LAN, WLAN). In this CLI session you can use the following commands to contact the LL2M server: `LL2Mdetect` and `LL2Mexec`. See [Command-line interface – command summary](#).

 You must have root rights on the LL2M server to run commands on the LL2M client.

 Access points of type LANCOM LW-500 can only be found and configured via LL2M if LL2M packets reach the access point with a VLAN tag which is included in the configuration of the access point (WLAN SSID configuration or management VLAN configuration).

The menu contains the settings for LANCOM layer 2 management.

SNMP ID:

2.50

Console path:**Setup****Operating**

Enables/disables the LL2M server.

SNMP ID:

2.50.1

Console path:**Setup > LL2M****Possible values:****No**

LL2M server is disabled.

Yes

LL2M server is enabled.

Default:

Yes

Interfaces

This item is used to specify the interfaces or Ethernet ports where the LL2M server can be reached. The presetting provides accessibility on all Ethernet ports. Access via WLAN is not planned.

SNMP ID:

2.50.2

Console path:**Setup > LL2M****Port**

Port designation, e.g. ETH1.

SNMP ID:

2.50.2.1

Console path:**Setup > LL2M > Interfaces**

Possible values:

Max. 5 characters from [A-Z] [a-z] [0-9] #@{|}~!\$%&'()*+,-./:;<=>?[\]"^_`.

Active

Enables/disables the LL2M server on this port.

SNMP ID:

2.50.2.2

Console path:

Setup > LL2M > Interfaces

Possible values:

No
Yes

Default:

Yes