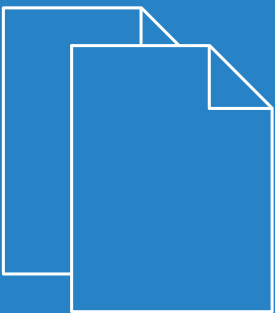


LCOS LX 5.34

Addendum



Contents

1 Addendum to LCOS LX version 5.34.....	4
2 Multicast Snooping.....	5
2.1 Additions to the Setup menu.....	7
2.1.1 Multicast-Snooping.....	7
2.1.2 Multicast-To-Unicast.....	8
3 USB Ethernet support.....	9
3.1 Additions to the Setup menu.....	9
3.1.1 USB.....	9

Copyright

© 2021 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 5.34

This document describes the changes and enhancements in LCOS LX version 5.34 since the previous version.

2 Multicast Snooping

As of LCOS LX 5.34, you can enable multicast snooping.

All devices with WLAN interfaces have a “LAN bridge” that transfers data between the Ethernet ports and the WLAN interfaces. The LAN bridge works like a switch in many respects. The central task of a switch is to forward packets only to the port to which the receiver is connected. To do this, the switch automatically forms a table from the incoming data packets in which the sender MAC addresses are assigned to the ports.

If a destination address of an incoming packet is found in this table, the switch can forward the packet specifically to the correct port. If the destination address is not found, the switch forwards the packet to all ports. This means that a switch can only forward a packet specifically if the destination address has already been received by it once as the sender address of a packet via a specific port. However, broadcast or multicast packets can never be entered as the sender address in a packet, which is why these packets are always “flooded” to all ports.

While this behavior is the correct action for broadcasts, since broadcasts should eventually reach all possible recipients, it is not necessarily the desired solution for multicasts. Multicasts are usually aimed at a specific group of recipients on a network, not all of them.

For example, video streams are often multicast, but not all stations on the network should receive a particular stream.

Various applications in the medical field use multicasts to transmit data to specific terminals that should not be viewed at all stations.

With a LAN bridge in the device, there will therefore also be ports to which no single receiver of the multicast is connected. The “unnecessary” sending of multicasts on ports without receivers is not a mistake, but it leads to performance problems, especially in WLAN networks. There, the unnecessary sending of multicasts can lead to a significant restriction of the available bandwidth, since multicasts in the WLAN—just like broadcasts—are sent at the lowest possible transmission rate so that they can be received by every WLAN subscriber.

With the Internet Group Management Protocol (IGMP) for IPv4 as well as Multicast Listener Discovery (MLD) for IPv6, the TCP/IP protocol family provides a protocol with which the network stations can inform the router to which they are connected of their interest in certain multicasts. To do this, the stations register with the routers for specific multicast groups from which you want to obtain the corresponding packets (multicast registration). IGMP uses special messages to register (join messages) and deregister (leave messages) for this purpose.

Multicast snooping makes use of these messages to decide to which port (i.e., also to which WLAN SSID) multicasts must be sent.

LANconfig: **Miscellaneous Services > Multicast Snooping**



Multicast Snooping

Operating: Yes

Operating

Turn multicast snooping on or off.

In addition, optional conversion of multicast data streams to unicast is possible. After activation of the feature, multicast data streams that are transmitted via WLAN interfaces are converted into individual unicast data streams for each client on the MAC layer or WLAN layer. The packets are duplicated for each client, but since they are now unicasts, they can be transmitted at the highest possible data rate for this client. Even though the packets are now duplicated, in most scenarios, the much faster transmission consumes much less airtime, which is then available for other transmissions.

Multicast to unicast conversion

LANconfig: **Wireless LAN > WLAN Networks > Network**

The screenshot shows a configuration window titled "Network - New Entry". It contains the following fields and options:

- Network-Name: NETWORK
- SSID-Name: LANCOM
- Key (PSK): [Redacted] Show
- Generate password: [Dropdown]
- Radios: 2.4 + 5 GHz
- Encryption-Profile: P-PSK [Select]
- Idle-Timeout: 300
- Tx bandwidth limit: 0 kBit/s
- Rx bandwidth limit: 0 kBit/s
- VLAN-ID: 0
- Inter-Station-Traffic: Yes
- Suppress SSID broadcast: No
- Maximum client count: 0
- Minimal client signal str.: 0
- Exclude From Client Mgmt: No
- Timeframe: ALWAYS [Select]
- Block Multicast: No [Select]
- Client Tx bandwidth limit: 0 kBit/s
- Client Rx bandwidth limit: 0 kBit/s
- Multicast-To-Unicast: None

Buttons for "OK" and "Cancel" are at the bottom.

Multicast-to-Unicast

Configure individually for each WLAN network whether and how multicasts are to be converted to unicasts.

None


Do not perform any conversion.


Conversion

The multicasts are converted to unicasts (layer-2 unicast on the WLAN layer with unicast MAC address as destination). This corresponds to the behavior in LCOS.

Encapsulation

The multicasts are encapsulated in unicast aggregates (A-MSDU with unicast MAC address as destination containing a single layer-2 multicast). This variant should be used when target applications check the target MAC address. However, it should be noted that aggregates are not supported by 802.11a/b/g clients.

 For the feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. Via IGMP snooping, the device determines which client wants to receive which multicast stream. The multicast conversion thus has the appropriate target clients or addresses available for conversion.

 The LW-500 uses a basic variant of multicast snooping that does not support conversion to unicast.

2.1 Additions to the Setup menu

2.1.1 Multicast-Snooping

All devices with WLAN interfaces have a “LAN bridge” that transfers data between the Ethernet ports and the WLAN interfaces. The LAN bridge works like a switch in many respects. The central task of a switch is to forward packets only to the port to which the receiver is connected. To do this, the switch automatically forms a table from the incoming data packets in which the sender MAC addresses are assigned to the ports.

If a destination address of an incoming packet is found in this table, the switch can forward the packet specifically to the correct port. If the destination address is not found, the switch forwards the packet to all ports. This means that a switch can only forward a packet specifically if the destination address has already been received by it once as the sender address of a packet via a specific port. However, broadcast or multicast packets can never be entered as the sender address in a packet, which is why these packets are always “flooded” to all ports.

While this behavior is the correct action for broadcasts, since broadcasts should eventually reach all possible recipients, it is not necessarily the desired solution for multicasts. Multicasts are usually aimed at a specific group of recipients on a network, not all of them.

For example, video streams are often multicast, but not all stations on the network should receive a particular stream.

Various applications in the medical field use multicasts to transmit data to specific terminals that should not be viewed at all stations.

With a LAN bridge in the device, there will therefore also be ports to which no single receiver of the multicast is connected. The “unnecessary” sending of multicasts on ports without receivers is not a mistake, but it leads to performance problems, especially in WLAN networks. There, the unnecessary sending of multicasts can lead to a significant restriction of the available bandwidth, since multicasts in the WLAN—just like broadcasts—are sent at the lowest possible transmission rate so that they can be received by every WLAN subscriber.

With the Internet Group Management Protocol (IGMP) for IPv4 as well as Multicast Listener Discovery (MLD) for IPv6, the TCP/IP protocol family provides a protocol with which the network stations can inform the router to which they are connected of their interest in certain multicasts. To do this, the stations register with the routers for specific multicast groups from which you want to obtain the corresponding packets (multicast registration). IGMP uses special messages to register (join messages) and deregister (leave messages) for this purpose.

Multicast snooping makes use of these messages to decide to which port (i.e., also to which WLAN SSID) multicasts must be sent.

SNMP ID:

2.40

Console path:

Setup

Operating

Turn multicast snooping on or off.

SNMP ID:

2.40.1

2 Multicast Snooping

Console path:

Setup > Multicast-Snooping

Possible values:**No**

Multicast snooping disabled.

Yes

Multicast snooping enabled.

2.1.2 Multicast-To-Unicast

Configure individually for each WLAN network whether and how multicasts are to be converted to unicasts.

SNMP ID:

2.20.1.29

Console path:

Setup > WLAN > Network

Possible values:**None****Conversion**

The multicasts are converted to unicasts (layer-2 unicast on the WLAN layer with unicast MAC address as destination). This corresponds to the behavior in LCOS.

Encapsulation

The multicasts are encapsulated in unicast aggregates (A-MSDU with unicast MAC address as destination containing a single layer-2 multicast). This variant should be used when target applications check the target MAC address. However, it should be noted that aggregates are not supported by 802.11a/b/g clients.

3 USB Ethernet support

As of LCOS LX 5.34, selected USB Ethernet devices are supported on access points with USB port. The CDC-EEM protocol is used here. For this purpose, the USB Ethernet device is bridged with the LAN of the access point. It is possible to specify a VLAN ID for network segmentation. Therefore, make sure that the USB Ethernet device can communicate in your network and, if necessary, VLAN according to the manufacturer's specifications. The following USB Ethernet devices can be operated with LCOS LX-based access points:

- > Hanshow HS_C09978 ESL Controller
- > SoluM EGU200NA0X ESL GEN2 USB Gateway

The special settings for USB Ethernet support are made in LANconfig under **IoT > USB**.



USB Ethernet	
Operating:	No
VLAN-ID:	0

Operating

Switch on the USB Ethernet support here.

VLAN ID

Optional specification of a VLAN ID.

3.1 Additions to the Setup menu

3.1.1 USB

Configure the settings for USB Ethernet support here.

SNMP ID:

2.111.1

Console path:

Setup > IoT

CDC-EEM-Support

Configure the settings of the CDC-EEM protocol for USB Ethernet support here.

SNMP ID:

2.111.1.1

Console path:

Setup > IoT > USB

3 USB Ethernet support

Operating

Switch USB Ethernet support on or off here.

SNMP ID:

2.111.1.1.1

Console path:

Setup > IoT > USB > CDC-EEM-Support

Possible values:

No

USB Ethernet support disabled.

Yes

USB Ethernet support enabled.

Default:

No

VLAN-ID

Optional specification of a VLAN ID.

SNMP ID:

2.111.1.1.2

Console path:

Setup > IoT > USB > CDC-EEM-Support

Possible values:

0 ... 4095