LCOS LX 7.12

Addendum

10/2025

LANCOM SYSTEMS

Contents

Copyright

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

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

1 Addendum to LCOS LX version 7.12

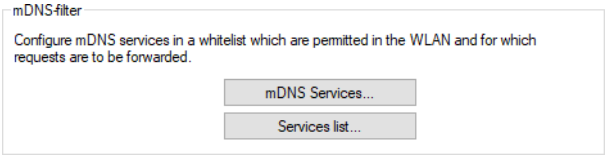
This document describes the changes and enhancements in LCOS LX version 7.12 since the previous version.

2 mDNS filter

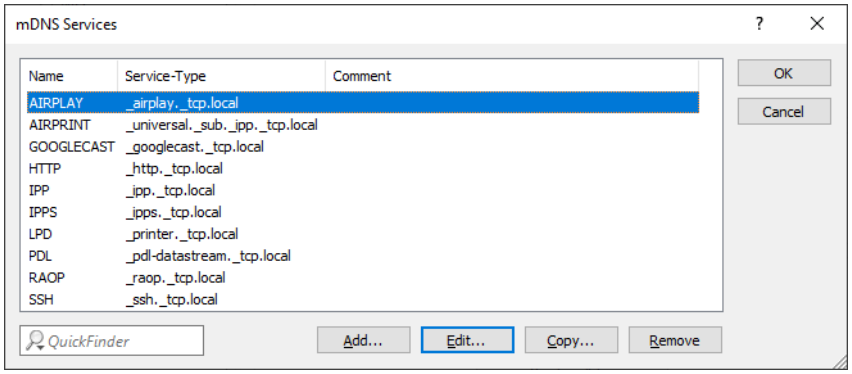
mDNS (Multicast DNS) is used for simple service discovery in the (W)LAN. Prominent applications based on this are Bonjour / AirPlay and Google Cast.

Since mDNS requests are sent as multicast, transmission at the WLAN level must use the lowest permitted data rate, which can consume significant airtime depending on the volume of mDNS requests. With the mDNS filter, requests to definable mDNS services can be selectively allowed for forwarding over the WLAN.

Configure the mDNS filter under **Wireless LAN** > **WLAN Networks** > **mDNS filter**.



mDNS Services contains the most common mDNS-based services by default, but it can also be manually extended.



Name

The name of a service.

Service-Type

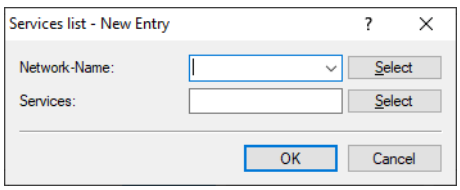
The type of this service.

Comment

Comment for this entry.

In the **Services list**, configure filters based on the services from the **mDNS Services** table.

The Services list works as a whitelist: If the list is not populated, all mDNS services are allowed. If the list contains entries, only the permitted services are allowed. All other services are filtered.



Network-Name

Here you can configure the WLAN network name for which the filter should apply.

Services

Here you can add one or more of the mDNS-based services defined in the Services table for which requests should be forwarded.

2.1 Additions to the Setup menu

2.1.1 mDNS-Filter

mDNS (Multicast DNS) is used for simple service discovery in the (W)LAN. Prominent applications based on this are Bonjour / AirPlay and Google Cast.

Since mDNS requests are sent as multicast, transmission at the WLAN level must use the lowest permitted data rate, which can consume significant airtime depending on the volume of mDNS requests. With the mDNS filter, requests to definable mDNS services can be selectively allowed for forwarding over the WLAN.

SNMP ID:

2.46

Console path:

Setup

2.1.1.1 Services

The Services table contains the most common mDNS-based services by default, but it can also be manually extended.

SNMP ID:

2.46.1

Console path:

Setup > **mDNS-Filter**

2.1.1.1.1 Name

The name of a service.

SNMP ID:

2.46.1.1

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.1.1.1.2 Service-Type

The type of this service.

SNMP ID:

2.46.1.2

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.1.1.1.3 Comment

Comment for this entry.

SNMP ID:

2.46.1.3

Console path:

Setup > **mDNS-Filter** > **Services**

Possible values:

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

2.1.1.2 Services-List

Configure filters here based on the services from the Services table.

The Services list works as a whitelist: If the list is not populated, all mDNS services are allowed. If the list contains entries, only the permitted services are allowed. All other services are filtered.

SNMP ID:

2.46.2

Console path:

Setup > **mDNS-Filter**

2.1.1.2.1 Network-Name

Here you can configure the WLAN network name for which the filter should apply.

SNMP ID:

2.46.2.1

Console path:

Setup > **mDNS-Filter** > **Services-List**

Possible values:

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

2.1.1.2.2 Services

Here you can add one or more of the mDNS-based services defined in the Services table for which requests should be forwarded.

SNMP ID:

2.46.2.2

Console path:

Setup > **mDNS-Filter** > **Services-List**

Possible values:

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

3 Cloud-managed Hotspot: Walled Garden

Walled Garden allows you to define IP addresses or hostnames that should be reachable for hotspot clients who are not yet logged in. Typically, these are hosts that provide additional resources required by the landing page (e.g., graphics, fonts, or even entire third-party login services).

Full integration of the Walled Garden configuration into the LANCOM Management Cloud hotspot configuration is planned.

3.1 Additions to the Setup menu

3.1.1 Walled-Garden

Walled Garden allows you to define IP addresses or hostnames that should be reachable for hotspot clients who are not yet logged in. Typically, these are hosts that provide additional resources required by the landing page (e.g., graphics, fonts, or even entire third-party login services).

To configure the Walled Garden, proceed as follows:

1. Create a Cloud-managed Hotspot in the LANCOM Management Cloud.
2. Next, determine the name of this Cloud-managed Hotspot from the table under **Setup** > **WLAN** > **Hotspot** > **Hotspots**.
3. Now create one or more entries in this table, with “Hotspot” containing the name of the hotspot configuration and “Hostname” containing the host or IP address to be allowed. The use of wildcards such as “*.lancom.de” is possible.
4. If a Walled Garden host should only be accessible without login when the LANCOM Management Cloud is not reachable, then for each entry the switch “LMC-unreachable-only” can additionally be set.
5. Finally, save the configuration using the command “flash”.

DNS requests from unauthenticated clients in the hotspot network are analyzed, and the resolved IP addresses are cached in the background to support the use of wildcards.

To simplify the process, it is recommended to perform these configuration steps in the LANCOM Management Cloud using an add-in.

SNMP ID:

2.20.12.2

Console path:

Setup > **WLAN** > **Hotspot**

3.1.1.1 Hotspot

Name of the hotspot.

SNMP ID:

2.20.12.2.1

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

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

3.1.1.2 Hostname

Enter here the host to be enabled or its IP address. The use of wildcards such as "*.lancom.de" is possible.

SNMP ID:

2.20.12.2.2

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-*`

3.1.1.3 LMC-unreachable-only

If a Walled Garden host should only be accessible without login when the LANCOM Management Cloud is not reachable, this switch can additionally be set to "Yes".

SNMP ID:

2.20.12.2.3

Console path:

Setup > **WLAN** > **Hotspot** > **Walled-Garden**

Possible values:

No
Yes

4 Cloud-managed Hotspot: Make local RFC1918 networks accessible

In networks operated as a Cloud-managed Hotspot, traffic to RFC1918 networks is generally prohibited. This affects the following networks:

- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12

With this feature, traffic to these networks or to individual hosts can be selectively allowed.

An add-in is required in the LANCOM Management Cloud.

The configuration is only possible via the CLI.

4.1 Additions to the Setup menu

4.1.1 Allowed-Targets

In networks operated as a Cloud-managed Hotspot, traffic to RFC1918 networks is generally prohibited. This affects the following networks:

- 10.0.0.0/8
- 192.168.0.0/16
- 172.16.0.0/12

With this feature, traffic to these networks or to individual hosts can be selectively allowed.

An add-in is required in the LANCOM Management Cloud.

SNMP ID:

2.20.12.3

Console path:

Setup > **WLAN** > **Hotspot**

4.1.1.1 Hotspot

Name of the hotspot.

SNMP ID:

2.20.12.3.1

Console path:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

Possible values:

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

4.1.1.2 IP-Network

Allowed IPv4 network for this hotspot.

SNMP ID:

2.20.12.3.1

Console path:

Setup > **WLAN** > **Hotspot** > **Allowed-Targets**

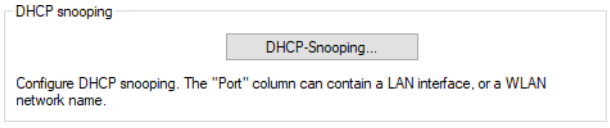
Possible values:

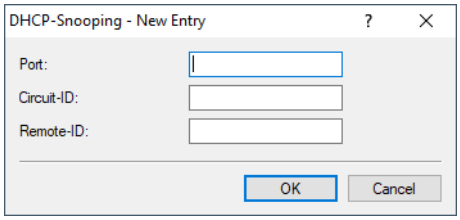
Max. 19 characters from `IPv4 address: a.b.c.d/xx`

5 DHCP: Add Circuit ID (Option 82) and Remote ID

The access point can add the Circuit ID and/or Remote ID to relayed DHCP packets. The DHCP server can make decisions based on this information, such as assigning specific IP addresses.

LANconfig: **Interfaces** > **DHCP Snooping**





Port

Here you can configure the WLAN network name or a LAN port (depending on the device model ETHx or LANx) on which DHCP requests should be supplemented.

Circuit-ID

The Circuit ID can be configured here using these placeholders:

- %i: Inserts the name of the interface where the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

Remote-ID

Here you can configure the Remote ID using these placeholders:

- %i: Inserts the name of the interface through which the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

5.1 Additions to the Setup menu

5.1.1 Bridge

SNMP ID:

2.45

Console path:

Setup

5.1.1.1 DHCP-Snooping

The access point can add the Circuit ID and/or Remote ID to relayed DHCP packets. The DHCP server can make decisions based on this information, such as assigning specific IP addresses.

SNMP ID:

2.45.1

Console path:

Setup > **Bridge**

5.1.1.1.1 Port

Here you can configure the WLAN network name or a LAN port (depending on the device model ETHx or LANx) on which DHCP requests should be supplemented.

The identifiers of the LAN ports can be viewed in the CLI table **Status** > **LAN** > **Ports**.

SNMP ID:

2.45.1.1

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

5.1.1.1.2 Circuit-ID

The Circuit ID can be configured here using these placeholders:

- %i: Inserts the name of the interface where the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.

- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

SNMP ID:

2.45.1.2

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

5.1.1.1.3 Remote-ID

Here you can configure the Remote ID using these placeholders:

- %i: Inserts the name of the interface through which the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %r: Inserts the system-wide MAC address.
- %%: Inserts a percent sign.

SNMP ID:

2.45.1.3

Console path:

Setup > **Bridge** > **DHCP-Snooping**

Possible values:

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

6 Factory default active services according to EN 18031 GEC-4

In LCOS LX 7.12, the following network services are active in the factory default state:

Service	Function	Port
SSH	Device management	TCP 22
HTTPS	Device management	TCP 443
LL2M	Device management	Layer 2
WTP	WLAN controller connection	UDP 1027
LMC	Connection to LANCOM Management Cloud	TCP 443
TFTP	Device search with LANconfig	UDP 69