

LCOS 10.32

Addendum



Contents

| | |
|--|-----------|
| 1 Addendum to LCOS version 10.32..... | 5 |
| 2 Configuration..... | 6 |
| 2.1 Configuration software..... | 6 |
| 2.1.1 WEBconfig with TLS 1.3..... | 6 |
| 2.1.2 Commands for the CLI..... | 6 |
| 3 Routing and WAN connections..... | 8 |
| 3.1 Filter list for redistribution in BGP..... | 8 |
| 3.1.1 Additions to the Setup menu..... | 10 |
| 3.2 BGP: Switch for default route propagation..... | 14 |
| 3.2.1 Additions to the Setup menu..... | 14 |
| 4 IPv6..... | 15 |
| 4.1 DHCPv6..... | 15 |
| 4.1.1 DHCPv6 server..... | 15 |
| 5 Firewall..... | 18 |
| 5.1 SD-WAN application routing / Layer-7 application control..... | 18 |
| 5.1.1 Configuration..... | 19 |
| 5.1.2 Additions to the Setup menu..... | 21 |
| 6 Wireless LAN – WLAN..... | 25 |
| 6.1 Return to the original 5 GHz channel when preference is configured..... | 25 |
| 6.2 Reduction of sensitivity for received packets..... | 25 |
| 6.2.1 Additions to the Setup menu..... | 26 |
| 6.3 Separate switch to enable e-mail notification..... | 28 |
| 6.3.1 Additions to the Setup menu..... | 29 |
| 6.4 IEEE 802.11k Roaming Targets..... | 29 |
| 6.4.1 Additions to the Setup menu..... | 30 |
| 6.5 Setting target EIRP..... | 31 |
| 6.5.1 Additions to the Setup menu..... | 32 |
| 7 WLAN management..... | 34 |
| 7.1 WLC features in the LANCOM vRouter..... | 34 |
| 7.2 New mode for antenna gain..... | 34 |
| 7.2.1 Additions to the Setup menu..... | 35 |
| 8 Virtual Private Networks – VPN..... | 37 |
| 8.1 IKEv2..... | 37 |
| 8.1.1 Elliptic Curve Digital Signature Algorithm (ECDSA)..... | 37 |
| 8.1.2 IKEv2 configuration payload with a specified source for prefix delegation..... | 38 |
| 8.1.3 Split DNS..... | 39 |
| 8.1.4 IKEv2 fragmentation..... | 40 |
| 8.1.5 IKEv2 password rules..... | 40 |
| 8.1.6 Additions to the Setup menu..... | 40 |

| | |
|---|-----------|
| 9 Public Spot..... | 49 |
| 9.1 Double the number of Public Spot users..... | 49 |
| 9.2 Passpoint [®] Release 2..... | 49 |
| 9.2.1 Additions to the Setup menu..... | 50 |
| 10 IoT – the Internet of Things..... | 60 |
| 10.1 Wireless ePaper..... | 60 |
| 10.1.1 Installation and Configuration of a Wireless ePaper USB..... | 61 |
| 10.2 BLE scanner and beacon..... | 62 |
| 10.2.1 Settings for BLE..... | 62 |
| 10.2.2 Monitoring..... | 64 |
| 10.3 Additions to the Setup menu..... | 65 |
| 10.3.1 IoT..... | 65 |
| 11 Other services..... | 82 |
| 11.1 DHCP server – suppress ARP request..... | 82 |
| 11.1.1 Additions to the Setup menu..... | 82 |
| 11.2 Simple Network Management Protocol (SNMP)..... | 83 |
| 11.2.1 SNMPv3 Password Rules..... | 83 |
| 11.2.2 Additions to the Setup menu..... | 83 |
| 11.3 TACACS+..... | 84 |
| 11.3.1 Configuring the TACACS+ server..... | 84 |

Copyright

© 2019 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, LCOS, 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 which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

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

Products from LANCOM Systems 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

www.lancom-systems.com

1 Addendum to LCOS version 10.32

This document describes the changes and enhancements in LCOS versions 10.30 and 10.32 since the previous version.

2 Configuration

2.1 Configuration software

2.1.1 WEBconfig with TLS 1.3

As of LCOS 10.30 your device supports TLS 1.3 for accessing WEBconfig. TLS 1.3 represents the latest advancement of the TLS standard and offers, for example, the exclusive use of state-of-the-art cipher suites and Perfect Forward Secrecy to provide improved security compared to previous versions.



An LCOS update automatically supplements the configuration with TLS 1.3 support for WEBconfig. If necessary, remove older methods that should no longer be available for WEBconfig.

Additions to the Setup menu

Versions

This bitmask specifies which versions of the protocol are allowed.

SNMP ID:

2.21.40.3

Console path:

Setup > HTTP > SSL

Possible values:

SSLv3
 TLSv1
 TLSv1.1
 TLSv1.2
 TLSv1.3

Default:

TLSv1.2

TLSv1.3

2.1.2 Commands for the CLI

As of LCOS 10.30 your device supports the following new commands and options.

Table 1: Overview of all new commands on the CLI

| Command | Description |
|--------------------|---|
| <code>clear</code> | Clears the current CLI output. All previously entered commands can be viewed by means of the log. |

New ping command options

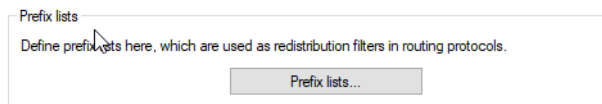
As of LCOS 10.30 your device supports the following new parameters for the ping command:

| Parameter | Meaning |
|----------------|--|
| -b | Do not stop pinging when a PacketTooBig (DF) is received, to ensure you have "Path MTU Discovery". |
| [-x x] | Atomic fragments: (n)ever, (f)orce, (a)utomatic |
| %scope | Name of the interface used to send the packet when link-local addresses are used as the destination. |
| %scope@rtg-tag | Name of the interface used to send the packet when link-local addresses are used as the destination, with additional specification of the routing tag. |
| %%interface | Name of the destination interface. The packet is sent directly to the interface without taking the routing table into account. |
| @rtg-tag | Routing tag used to send the packet. |

3 Routing and WAN connections

3.1 Filter list for redistribution in BGP

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP. To do this, create the prefix filter list under **IP router > General > Prefix lists**.



Name

Give this entry a name here.

IP address

Specify the IPv4 or IPv6 address of the network here.

Prefix length

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Min. prefix length** and **Max. prefix length** are set to values not equal to zero.

If the value is "0", the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

Min. prefix length

Here you specify the minimum prefix length value required for the prefix to match.

Max. prefix length

Here you specify the maximum prefix length value required for the prefix to match.

Comment

Comment on this entry.

Using prefix lists with BGP

These **prefix lists** can be referenced for the IPv4 and IPv6 address families of the BGP protocol, and you can specify whether these prefix lists should be allowed or rejected

Routing protocols > BGP > IPv4 address family

IPv4 address family - New Entry

Entry active

Neighbor profile:

Routing tag:

Weight:

Locale preference:

Prefix limit:

Communities:

Use self as next hop:

Routes redistribution

Static Connected

RIP OSPF

LISP

Redistribution filter:

Default action:

Comment:

Routing protocols > BGP > IPv6 address family

IPv6 address family - New Entry

Entry active

Neighbor profile:

Routing tag:

Weight:

Locale preference:

Prefix limit:

Communities:

Use self as next hop:

Routes redistribution

Static Connected

LISP

Redistribution filter:

Default action:

Comment:

Redistribution filter

Name of the prefix-filter list.

Default action

Defines the default handling of prefixes that are not configured in the prefix list. Possible values:

Accept

Deny

3.1.1 Additions to the Setup menu

Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

SNMP ID:

2.93.1.4.1.11

Console path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

Possible values:

Max. 16 characters from [A-Z] [a-z] [0-9] -

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.1.4.1.12

Console path:

Setup > Routing-Protocols > BGP > Addressfamily > IPv4

Possible values:

Allow

Reject

Default:

Allow

Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

SNMP ID:

2.93.1.4.2.11

Console path:**Setup > Routing-Protocols > BGP > Addressfamily > IPv6****Possible values:**

Max. 16 characters from [A-Z] [a-z] [0-9] -

Default:*empty***Default-Action**

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.1.4.2.12

Console path:**Setup > Routing-Protocols > BGP > Addressfamily > IPv6****Possible values:****Allow**
Reject**Default:**

Allow

Filter

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP.

SNMP ID:

2.93.5

Console path:**Setup > Routing-Protocols****Prefix-List**

Here you specify a prefix list that can be referenced by BGP.

SNMP ID:

2.93.5.1

Console path:**Setup > Routing-Protocols > Filter****Name**

Contains the name of this entry.

SNMP ID:

2.93.5.1.1

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]-_`**Default:***empty***IP-Address**

Contains the IPv4 or IPv6 address of the network.

SNMP ID:

2.93.5.1.2

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**Max. 39 characters from `[A-F][a-f][0-9]:.`**Default:***empty***Prefix-Length**

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Length-min** and **Length-max** are set to values not equal to zero.

If the value is "0", the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

SNMP ID:

2.93.5.1.3

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**

Max. 3 characters from [0-9]

Default:*empty***Length-Min**

Specifies the minimum prefix length value required for the prefix to match.

SNMP ID:

2.93.5.1.4

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**

Max. 3 characters from [0-9]

Default:*empty***Length-Max**

Specifies the maximum prefix length value required for the prefix to match.

SNMP ID:

2.93.5.1.5

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**

Max. 3 characters from [0-9]

Default:*empty***Comment**

Comment on this entry.

SNMP ID:

2.93.5.1.6

Console path:**Setup > Routing-Protocols > Filter > Prefix-List****Possible values:**

Max. 254 characters from [A-Z] [a-z] [0-9] #@ { | } ~ ! \$ % & ' () + - , / : ; < = > ? [\] ^ _ . `

Default:*empty*

3.2 BGP: Switch for default route propagation

As of LCOS 10.32 RU4 your device has the option to handle default routes like normal routes with BGP.

3.2.1 Additions to the Setup menu

Send-Default-Route

This switch determines the behavior of the propagation of default routes.

SNMP ID:

2.93.1.3.11

Console path:**Setup > Routing-Protocols > BGP > Neighbor-Profiles****Possible values:****Yes**

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table ([2.93.1.6.1 IPv4](#) or [2.93.1.6.2 IPv6](#)).

Default:

No

4 IPv6

4.1 DHCPv6

4.1.1 DHCPv6 server

Enhancements for client reservations in the DHCPv6 server

As of LCOS 10.30, the parameter **Client ID** has been replaced by the two new parameters **Identifier** and **Identifier type**. This means that the DHCPv6 server can now assign client addresses or prefixes on the basis of the DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649). The corresponding settings in LANconfig are made under **IPv6 > DHCPv6 > Reservations**:

Identifier type

This type specifies how the **Identifier** is to be interpreted.

Client ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

MAC address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- > Specification as a client DUID, e.g. 0003000100a057000001

- > Specification as a MAC address, e.g. 00a057000001
- > Specification as an interface ID or remote ID, e.g. "INTRANET"

Additions to the Setup menu

Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- > Specification as a client DUID, e.g. 0003000100a057000001
- > Specification as a MAC address, e.g. 00a057000001
- > Specification as an interface ID or remote ID, e.g. INTRANET

SNMP ID:

2.70.3.1.6.3

Console path:

Setup > IPv6 > DHCPv6 > Server > Reservations

Possible values:

A hex string with max. 127 characters `[a-z][0-9]:-`

Default:

empty

Identifier-Type

This type specifies how the identifier in 2.70.3.1.6.3 is to be interpreted.

SNMP ID:

2.70.3.1.6.8

Console path:

Setup > IPv6 > DHCPv6 > Server > Reservations

Possible values:

Client-ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

Mac-Address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface-ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote-ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.70.3.1.6.9

Console path:

Setup > IPv6 > DHCPv6 > Server > Reservations

Possible values:

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

Default:

empty

5 Firewall

5.1 SD-WAN application routing / Layer-7 application control

You can benefit from significant performance gains by operating modern business applications in the cloud (e.g. Microsoft Office 365, AWS, etc). Application routing uses rules to direct trusted applications from the branch office directly to the Internet. This relieves the load on the VPN connection to the main office and also on the Internet connection at the main office.

Microsoft explicitly recommends this mode for Office 365. Because these web-based services often have no fixed IP address, they can only be recognized by DNS names. For this purpose, the corresponding DNS targets can be created in the firewall with an appropriate wildcard expression. These packets are marked with a different routing tag so that the router directs them straight to the Internet. As an alternative, layer-7 application control can be implemented in the firewall. This gives you full control over how applications operate on your network. By defining rules for DNS-based applications, you decide which Internet applications are allowed, blocked, limited or prioritized.

If a user now invokes one of these DNS targets in his or her browser, the computer sends a DNS request for this domain. The DNS forwarder in the LANCOM router then forwards this request to the Internet Service Provider. When the response arrives the router stores the returned IP address, and from that moment on this resolution is available in the firewall. The response then continues on to the computer that made the original request. This allows the browser to open the connection to the returned IP address. The firewall recognizes the previously learned IP address and can assign a routing tag correspondingly. Other defined firewall actions can also be applied to this destination, such as allow, block, limit, or prioritize.

Because the firewall remembers the exact DNS address that the user uses for the domain, this mechanism will also work if the domain name resolves to many different IP addresses or to IP addresses that change over time.

Recommendations

The LANCOM router must operate as a DNS server or DNS forwarder on the network, i.e. clients on the local network must use the router as the DNS server. In addition, clients need to be prevented from using DNS-over-TLS and DNS-over-HTTPS (also in the browser) directly with external DNS servers.

This can be done as follows:

- > The DHCP server has to communicate the IP address of the router as a DNS server (set by default by the Internet wizard)
- > Firewall rules have to be set up that prevent the direct use of external DNS servers, e.g. by blocking the outgoing port 53 (UDP) for clients on the source network
- > Firewall rules have to be set up that prevent the direct use of external DNS servers that support DNS-over-TLS, e.g. by blocking the outgoing port 853 (TCP) for clients on the source network
- > Disable DNS-over-HTTPS (DoH) in the browser



Notes on how to synchronize the firewall's DNS database:

Since the firewall learns its information from the DNS requests of the clients, in certain situations the DNS database will be incomplete. This can happen in the following situations:

- > A new firewall rule is added, but the client still has a cached DNS entry
- > The router was recently restarted, and the client still has a cached DNS entry

Helpful in these cases are emptying the DNS cache on the client, rebooting the client, or a time-out of the DNS record on the client.

The router's own services, such as ping, are not handled by the firewall rules. By sending a ping to a full DNS name (without wildcard expressions), the generation of rule resolutions (DNS to IP addresses) can be performed on-demand either from the CLI (once) or by a cron job.

! Different DNS names that resolve to the same IP address cannot be distinguished. In this case, the first rule that references one of these DNS names will apply. That should not be a problem for large service providers. However, it could occur with small websites hosted by the same vendor.

show fw-dns-destinations

This new parameter for the CLI command `show` accepts an optional space-separated list of names of DNS destinations. It lists all DNS destinations or the ones specified in the parameter list sequentially. For each destination, it displays the counter from **Status > Firewall > DNS-Database > Destination-Usage** followed by the list of wildcard expressions. For each wildcard expression, it shows the currently resolved addresses and the data records that are a direct or indirect match.

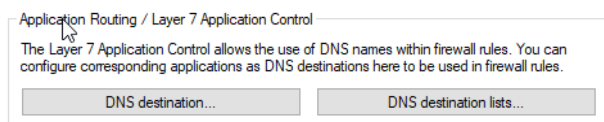
Trace

For application-based routing, there is the new parameter `FW-DNS` for the trace command. It can monitor changes to the firewall database of DNS destinations:

- > If a DNS packet arrives, it outputs the packet along with the affected wildcard expressions and destinations.
- > If the TTL (time-to-live) of an entry expires, it outputs the associated record along with the relevant wildcard expressions and destinations.
- > If one of the two firewalls registers or de-registers a DNS destination because its configuration has changed.
- > If there is a change to the table **Set up > Firewall > DNS-Destinations** or **Set up > Firewall > DNS-Destination-List**.

5.1.1 Configuration

Settings for the application-based routing or the Layer 7 application control are located under **Firewall/QoS > General > Application Routing / Layer 7 Application Control**.



DNS-Destinations

In LANconfig, you specify the names and wildcard expressions for the DNS destinations that you want to treat separately in the firewall under **Firewall/QoS > General > Application-based routing > DNS destinations**.

Name

The name for this DNS destination. This name is used to reference this object.

Wildcard expressions

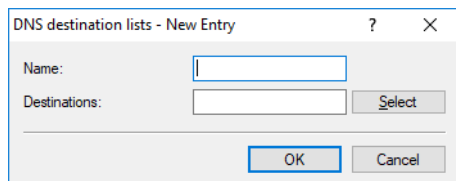
Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. "*.lancom.*". The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- > UTF-8: Here, one to four bytes must be entered individually as '\x' followed by two hexadecimal digits.
- > UTF-16: Here, one or two double bytes must be entered as '\u' followed by four hexadecimal digits.
- > UTF-32: Here, the value must be entered as '\U' followed by eight hexadecimal digits.

DNS destination list

In LANconfig, specify the DNS destinations that you want to reference as one object in the firewall under **Firewall/QoS > General > Application-based routing > DNS destinations list**.



The screenshot shows a dialog box titled "DNS destination lists - New Entry". It has a "Name:" label followed by an empty text input field. Below that is a "Destinations:" label followed by another empty text input field and a "Select" button. At the bottom of the dialog are "OK" and "Cancel" buttons.

Name

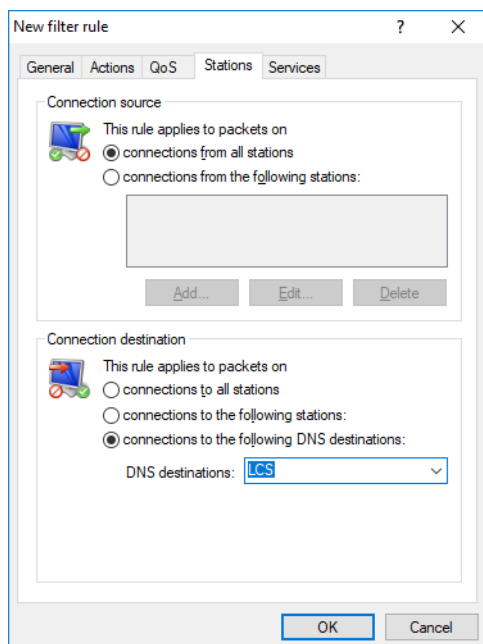
Name of the list of DNS destinations

Targets

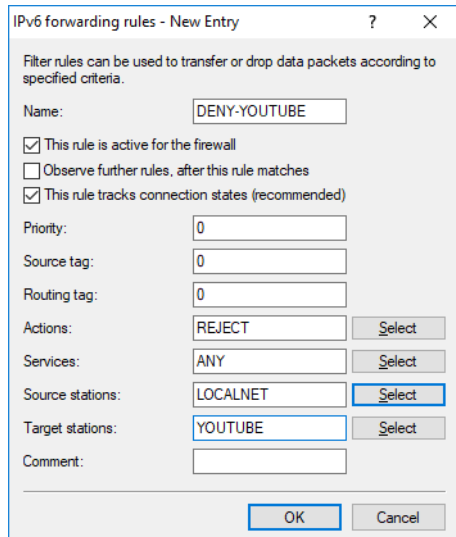
Contains a comma-separated or space-separated list of names of the DNS destinations.

Referencing in firewall rules

In **Firewall / QoS > IPv4-Rules > Rules** you can create a new filter rule and, then, go to the **Stations** tab and select from the configured DNS destinations under **Connections to the following DNS destinations**.



In **Firewall / QoS > IPv6 Rules > IPv6 forwarding rules** you can create a new rule. Entries from the **DNS destinations** or **DNS destination list** tables can be used as **Target stations**.



5.1.2 Additions to the Setup menu

DSCP-support

If you set this parameter to Yes, then the DiffServ field in the IPv6-packet header is observed and evaluated as follows:

- > **CSx (including CS0 = BE)**: Normal transmission
- > **AFxx**: Secure transmission
- > **EF**: Preferred transmission

SNMP ID:

2.70.5.25

Console path:**Setup > IPv6 > Firewall****Possible values:****No**
Yes**Default:**

No

Firewall

Firewall settings

SNMP ID:

2.110

Console path:**Setup****DNS-Destinations**

As of LCOS 10.30 DNS names can be used in the firewall. DNS names can be defined in full, e.g. "www.lancom.de", or as a wildcard expression, e.g. "*lancom*". These objects can be used in firewall rules as destinations. Layer-7 (web) applications can be blocked, allowed, limited, prioritized, or redirected to another routing context.

Further information and recommendations are available in the Reference Manual under the Firewall section.

SNMP ID:

2.110.1

Console path:**Setup > Firewall****Name**

The name for this DNS destination. This name is used to reference this object.

SNMP ID:

2.110.1.1

Console path:

Setup > Firewall > DNS-Destinations

Possible values:

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+,-./:;<=>?[\]^_.`

Default:

empty

Wildcard-Expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. `*.lancom.*`. The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- > UTF-8: Here, one to four bytes must be entered individually as 'x' followed by two hexadecimal digits.
- > UTF-16: Here, one or two double bytes must be entered as 'u' followed by four hexadecimal digits.
- > UTF-32: Here, the value must be entered as 'U' followed by eight hexadecimal digits.

SNMP ID:

2.110.1.2

Console path:

Setup > Firewall > DNS-Destinations

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_.\``

Default:

empty

DNS-Destination-List

In the DNS destination list, you can group multiple DNS destinations into one referenced object.

SNMP ID:

2.110.2

Console path:

Setup > Firewall

Name

The name for this DNS destination list. This name is used to reference this object.

SNMP ID:

2.110.2.1

Console path:**Setup > Firewall > DNS-Destination-List****Possible values:**Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-/,/:;<=>?[\]^_.`**Default:***empty***Targets**

Contains a comma-separated or space-separated list of names of the DNS destinations.

SNMP ID:

2.110.2.2

Console path:**Setup > Firewall > DNS-Destination-List****Possible values:**Max. 252 characters from `[A-Z][0-9]#@{|}~!$%&'()+-/,/:;<=>?[\]^_.`**Default:***empty*

6 Wireless LAN – WLAN

6.1 Return to the original 5 GHz channel when preference is configured

From LCOS 10.30 RU1 all LCOS devices with WLAN module support the return to the original 5 GHz channel if a preference is configured. This feature allows you to keep to a channel plan as far as possible, even for installations that do not use indoor-only mode and may therefore be affected by channel changes due to radar detection.

If a WLAN channel or the WLAN channel list is configured for a WLAN module operated at 5 GHz and not in indoor-only mode, the channels entered there are preferred. Only if the channels set there have been blocked by radar detection will they be deviated from.

With the feature described here, the access point will attempt to switch back to the set channel after the DFS lock time has elapsed. If this channel is still not available, a channel configured in the channel list will be used. The DFS lock time takes effect as soon as a channel has been locked due to radar detection and is usually 30 minutes.

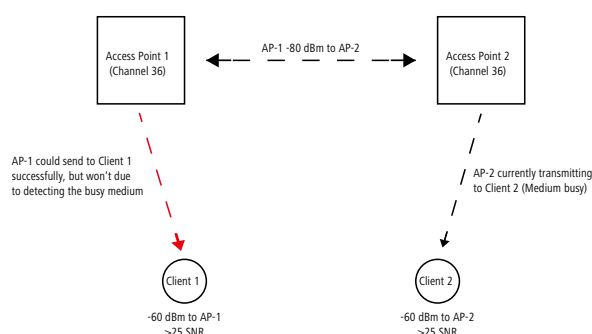
If no dedicated channel is configured for the WLAN module (channel list empty and radio channel "0" or "Automatic"), the previous behavior does not change. If a channel change is triggered by radar detection, the new channel is retained and not changed back to the last channel used.

This preference helps to be able to use fixed channel schemes in 5 GHz, since the full capacity of the network can be used faster after DFS events.

i There is no configuration possibility. If you configure a WLAN channel or WLAN channel list for a WLAN module that is operated at 5 GHz and is not in indoor-only mode, this feature is automatically active.

6.2 Reduction of sensitivity for received packets

In high-density scenarios such as stadiums, exhibition halls or auditoriums, it is inevitable that access points that use the same channel will use the medium to a high capacity. This can result in a situation where the access points withhold their transmissions to the clients because the channel is recognized more often as busy.




An access point can be set artificially "deaf" by reducing the reception sensitivity from LCOS 10.30 RU1 onwards. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer “heard”. This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

You set the reduction via the console in value **Setup > Interfaces > WLAN > Radio-Settings > Rx-Packet-Sens.-Reduction**. The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

For WLAN controllers, this setting can also be made via the console in the profile of an access point. Under **Setup > WLAN-Management > AP-configuration > Accesspoints** adjust the values **Module-1-Rx-Packet-Sens.-Reduction** resp. **Module-2-Rx-Packet-Sens.-Reduction** accordingly.

 This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

 Supported devices:

- > Only WLAN-2 with LN-630, L-822, LN-830x, LN-86x, L-1302, L-1310, LN-170x
- > WLAN-1 and WLAN-2 with O/IAP-8xx, OAP-170x
- > All WLAN controllers with LCOS 10.30 RU1


6.2.1 Additions to the Setup menu

Rx-Packet-Sens.-Reduction

An access point can be set artificially “deaf” by reducing the reception sensitivity. This means that transmissions further away from the access point are “overheard” and the channel is detected more often as “free”. In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer “heard”. This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

 This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.23.20.8.35

Console path:**Setup > Interfaces > WLAN > Radio-Settings****Possible values:**


0 ... 20

Module-1-Rx-Packet-Sens.-Reduction

An access point can be set artificially “deaf” by reducing the reception sensitivity. This means that transmissions further away from the access point are “overheard” and the channel is detected more often as “free”. In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer “heard”. This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

 This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.37.1.4.37

Console path:**Setup > WLAN-Management > AP-configuration > Accesspoints****Possible values:**


0 ... 20

Module-2-Rx-Packet-Sens.-Reduction

An access point can be set artificially “deaf” by reducing the reception sensitivity. This means that transmissions further away from the access point are “overheard” and the channel is detected more often as “free”. In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer “heard”. This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

 This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.37.1.4.38

Console path:**Setup > WLAN-Management > AP-configuration > Accesspoints****Possible values:**

0 ... 20

6.3 Separate switch to enable e-mail notification

Previously, e-mail notifications were sent whenever an e-mail address was present in the corresponding field of the configuration. This implicit behavior has now been replaced by an additional operating mode switch that controls the sending of notifications.

You can find the new switch under **Wireless LAN > General. Send e-mails** controls whether notifications are sent to the e-mail address specified in **E-Mail address for WLAN events**.

Email address for WLAN events:

 Send emails

6.3.1 Additions to the Setup menu

Mail-Address

Information about events in the WLAN is sent to this e-mail address if this is enabled with the 2.12.141 switch.

 An SMTP account must be set up to make use of the e-mail function.

SNMP ID:

2.12.41

Console path:

Setup > WLAN

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

Default:

empty

Send-Mails

Determines whether notifications about WLAN events are sent to the e-mail address specified in 2.12.41 .

SNMP ID:

2.12.141

Console path:

Setup > WLAN

Possible values:

No
Yes

Default:

No

6.4 IEEE 802.11k Roaming Targets

The IEEE 802.11k standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the client in the "Neighbor Report" as defined for the standard. 802.11k has so far been used as part of the client management, so it does not need to be configured separately. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately.

You can find the new table under **Wireless LAN > General > Extended settings > 802.11k Roaming Targets**. Enter the potential roaming targets here.

6.4.1 Additions to the Setup menu

Roaming-Targets

With Client Management enabled, the table under `/Status/WLAN/Roaming-Targets` is filled out automatically. Additionally, any targets added manually to this table are also included in the list of neighbors in an 802.11k advertisement, even if they are out of range. The number of automatically added roaming targets is limited by [2.12.87.11 Maximum-Neighbor-Count](#).

SNMP ID:

2.12.132

Console path:


Setup > WLAN

Name

As a part of client management, the names of the roaming targets for this access point are entered here after an environment scan. This is a part of the standard IEEE 802.11k. This standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the WLAN client in the "Neighbor Report" as defined for the standard.

Client management makes these entries automatically. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately. In this case, you enter the device names of the potential roaming targets here, i.e. other access points of the same SSID.

The device name is used so that further required information about the potential roaming target (e.g. the channel number) can be communicated via IAAP. For this reason it is necessary for the participating access points to communicate with one another via IAPP.

 Depending on the scenario, it may be desirable for a dual-radio access point to communicate its own, second WLAN module as a potential roaming target. In this case, the device's own name can also be entered into the table.

SNMP ID:

2.12.132.1

Console path:

Setup > WLAN > Roaming-Target

Possible values:

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

6.5 Setting target EIRP

In versions before LCOS 10.30, the current WLAN transmission power could be reduced by a fixed, configured value. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5-GHz subbands. For example, higher transmission powers are permitted in the 5-GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. As of LCOS 10.30, the actual maximum transmission power can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

Configure this in LANconfig under **Wireless LAN > General > Physical WLAN settings > Radio** using the fields **Power setting** and **Tx Power**.


The **Automatic** mode describes the previous behavior, whereas **Manual** allows an absolute value in dBm to be specified in the field **Tx power**.

i Under no circumstances will the access point exceed the legal limits for transmission power. These are always respected automatically, regardless of the settings made here.

6.5.1 Additions to the Setup menu

Power-Setting

In versions before LCOS 10.30, the current WLAN transmission power could be reduced by a fixed, configured value. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5-GHz subbands. For example, higher transmission powers are permitted in the 5-GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. As of LCOS 10.30, the actual maximum transmission power can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

 Under no circumstances will the access point exceed the legal limits for transmission power. These are always respected automatically, regardless of the settings made here.

SNMP ID:

2.23.20.8.33

Console path:

Setup > Interfaces > WLAN > Radio-settings

Possible values:

Automatic

The maximum permitted transmission power that can be realized by the hardware of the access point is used.

Manual

The desired transmission power is to be set in dBm in the EIRP field.



If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically. The actual value can be checked in LANmonitor or on the CLI by means of the command `show wlan`.

Default:

Automatic

EIRP

With the setting for WLAN transmission power in 2.23.20.8.33 is set to manual, the value set here is taken in dBm.

SNMP ID:

2.23.20.8.34

Console path:

Setup > Interfaces > WLAN > Radio-settings

Possible values:


Max. 4 characters from [0-9] –

7 WLAN management

7.1 WLC features in the LANCOM vRouter

As of LCOS 10.30 the LANCOM vRouter additionally supports the functions of a WLAN controller. You decide which role your LANCOM vRouter should play: VPN gateway or WLAN controller. The LANCOM vRouter now supports the role of a virtual WLC (vWLC), which means it is capable of managing access points. This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the vRouter license category. All vRouter licenses issued after the release of LCOS 10.30 include a vWLC option.

| Product | VPN licenses | AP licenses |
|-------------------|--------------|-------------|
| vRouter 50 | 10 | 10 |
| vRouter 250 | 50 | 50 |
| vRouter 500 | 100 | 100 |
| vRouter 1000 | 200 | 200 |
| vRouter unlimited | 1000 | 1000 |

-  LANCOM Systems GmbH recommends running a vRouter instance either primarily as a VPN gateway/router or as a WLAN controller. The recommended usage may also be split: For example, at the license level "vRouter 1000" (200 VPN licenses and 200 AP licenses):
- > 100 concurrent VPN connections and 100 managed APs or
 - > 150 concurrent VPN connections and 50 managed APs.

7.2 New mode for antenna gain

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is transmitted to the WLAN controller and used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

This is configured in LANconfig under **WLAN Controller > AP Configuration > Access point table** using the fields **Antenna gain mode** for each WLAN interface.

Antenna gain mode

Possible values:

Standard

The antenna gain value preset in the access point is used.

Userdefined

The value entered in the field **Antenna gain** is used.

7.2.1 Additions to the Setup menu

Module-1-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

SNMP ID:

2.37.1.4.35

Console path:

Setup > WLAN-Management > AP-Configuration > Accesspoints

Possible values:**Standard**

The antenna gain value preset in the access point is used.

User defined

The value for **Module-1-Ant-Gain** is used.

Default:

Standard

Module-2-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. In particular for outdoor access points with integrated high-gain antennas, this value had to be adjusted manually. As of LCOS 10.30 the standard antenna gain of a managed access point is automatically transmitted to and used by the WLAN controller. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.30. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

SNMP ID:

2.37.1.4.36

Console path:

Setup > WLAN-Management > AP-Configuration > Accesspoints

Possible values:**Standard**

The antenna gain value preset in the access point is used.

User defined

The value for **Module-2-Ant-Gain** is used.

Default:

Standard

8 Virtual Private Networks – VPN

8.1 IKEv2

8.1.1 Elliptic Curve Digital Signature Algorithm (ECDSA)

As of LCOS 10.30, IKEv2 now supports Elliptic Curve Digital Signature Algorithm (ECDSA) as per RFC 4754 in addition to the authentication methods RSA Signature and Digital Signature.

ECDSA signatures are generally smaller than RSA signatures with comparable cryptographic strength. ECDSA keys and certificates also have significantly smaller file sizes than RSA-based keys and certificates. Furthermore, ECDSA operations are generally faster on most devices. The following methods are supported in IKEv2:

- > ECDSA with SHA-256 on the P-256 curve
- > ECDSA with SHA-384 on the P-384 curve
- > ECDSA with SHA-512 on the P-521 curve



When using OpenSSL to generate certificates, the following predefined curves must be used as parameters for ECDSA in IKEv2:

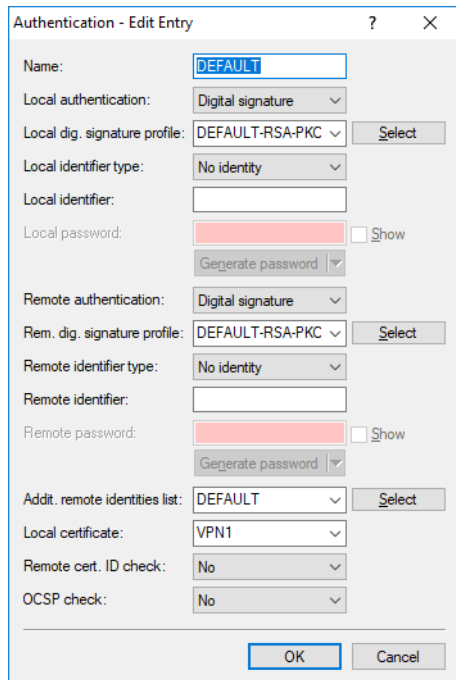
- > prime256v1 with ECDSA-256
- > secp384r1 with ECDSA-384
- > secp521r1 with ECDSA-512



The following restrictions apply when using ECDSA:

- > The negotiation of ECDSA within the Digital Signature method is not supported.
- > ECDSA-based certificates currently cannot be generated by the LCOS's own CA. Similarly, it is not possible to obtain certificates automatically by means of SCEP. ECDSA certificates must be generated using an external application such as OpenSSL or XCA and then loaded into the device.

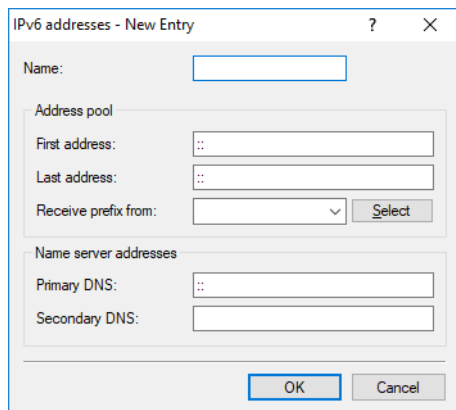
In LANconfig under **VPN > IKEv2/IPSec > Authentication**, you can now select these methods for both **Local authentication** and **Remote authentication**.



8.1.2 IKEv2 configuration payload with a specified source for prefix delegation

As of LCOS 10.30, the IKEv2 configuration payload supports the specification of a source for prefix delegation.

In LANconfig, the configuration is located under **VPN > IKEv2/IPSec > IPv6 addresses**.




Address pool

Receive prefix from

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter **First address** to the value "::1" in the **Last address** to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g., "/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- > Assigned provider prefix: 2001:db8:abcd:aa::/56
- > /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- > First address: 0:0:0:0001::1
- > Last address: 0:0:0:0001::9

 Currently no Neighbor Discovery Proxy is supported for IPv6. For this reason, the address range of the pool must not overlap with address ranges or prefixes that are already used for other networks on the router.

8.1.3 Split DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. “*.company.com”) to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

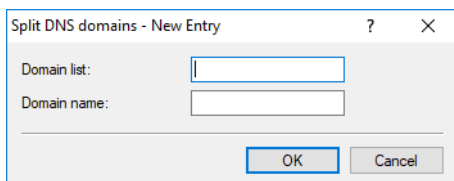
Split DNS for IKEv2 is supported by LANCOM VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

The split-DNS configuration is assigned in the IKEv2 connection list when the CFG mode is set to “Server” and the split DNS profile has been selected.

In LANconfig you first specify the required domains under **VPN > IKEv2/IPSec > Split DNS domains** and assign these to a profile under **VPN > IKEv2/IPSec > Split DNS profiles**. This profile can then be selected in the **Connection list** under IKE config mode when **IKE-CFG** is set to **Server**.

Split DNS domains

In LANconfig, the split DNS domains are configured under **VPN > IKEv2/IPSec > Split DNS domains**.



Domain list

Enter a name for the domain lists.

Domain name

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. “company.internal”. Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

Split DNS profile

In LANconfig, the split DNS profiles are configured under **VPN > IKEv2/IPSec > Split DNS profiles**.

Name

Enter a name for this profile.

Domain list

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

Send DNS forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.


Send local domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

8.1.4 IKEv2 fragmentation

LCOS as of version 10.30 supports IKEv2 fragmentation according to RFC 7383. This enables the VPN router to fragment IKEv2 messages by itself, which is more efficient than having IKE-packet fragmentation performed by the transport network. Two methods of IKEv2 fragmentation are supported:

- > Manufacturer-specific fragmentation, compatible with third-party manufacturers
- > Fragmentation as per RFC 7383

 The device sets the best method automatically. If a VPN remote site supports both methods, fragmentation as per RFC 7383 is preferred.

8.1.5 IKEv2 password rules

LCOS as of version 10.32 supports enforcing password rules for pre-shared keys. Navigate to **VPN > IKEv2/IPSec > Extended settings** and set the option **Enforce Preshared Key rules**. The following rules then apply for Pre-Shared Keys (PSK) with IKEv2:

- > The length of the password must be at least 32 characters.
- > The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

 These rules do not apply to PSK managed and obtained by a RADIUS server.

8.1.6 Additions to the Setup menu

Split-DNS-Profile

Name of the Split DNS profile. The split DNS profile is only active if **IKE-CFG** is set to the value **Server**.

SNMP ID:

2.19.36.1.22

Console path:**Setup > VPN > IKEv2 > Peers****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-/,;=<=>?[\]^_.`**Local-Auth**

Sets the authentication method for the local identity.

SNMP ID:

2.19.36.3.1.2

Console path:**Setup > VPN > IKEv2 > Auth > Parameter****Possible values:****RSA-Signature**

Authentication by RSA signature.

PSK

Authentication by pre-shared key (PSK).

Digital signature

Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.1.6

Console path:

Setup > VPN > IKEv2 > Auth > Parameter

Possible values:**RSA-Signature**

Authentication by RSA signature.

PSK

Authentication by pre-shared key (PSK).

Digital signature

Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.3.2

Console path:

Setup > VPN > IKEv2 > Auth > Addit.-Remote-IDs

Possible values:**RSA-Signature**

Authentication by RSA signature.

PSK

Authentication by pre-shared key (PSK).

Digital signature

Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

PD-Source

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter "First address" to the value "::1" in the "Last address" to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g., "/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- > Assigned provider prefix: 2001:db8:abcd:aa::/56
- > /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- > First address: 0:0:0:0001::1
- > Last address: 0:0:0:0001::9

SNMP ID:

2.19.36.7.2.6

Console path:

Setup > VPN > IKEv2 > IKE-CFG > IPv6

Possible values:

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

Default:

empty

Split-DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. "*.company.com") to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

Split DNS for IKEv2 is supported by LANCOM VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

SNMP ID:

2.19.36.7.3

Console path:**Setup > VPN > IKEv2 > IKE-CFG****Domain-Lists**

Here you specify the domain lists for split DNS.

SNMP ID:

2.19.36.7.3.1

Console path:**Setup > VPN > IKEv2 > IKE-CFG > Split-DNS****Domain-name**

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. "company.internal". Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

SNMP ID:

2.19.36.7.3.1.1

Console path:**Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Domain-Lists****Possible values:**Max. 64 characters from `[A-Z][0-9]@{|}~!$%&'()+-/, :;<=>?[\]^_.`**Default:***empty***Domain-List**

Enter a name for the domain lists.

SNMP ID:

2.19.36.7.3.1.3

Console path:**Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Domain-Lists**

Possible values:

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

Default:

empty

Profiles

Here you set the profiles for split DNS.

SNMP ID:

2.19.36.7.3.4

Console path:

Setup > VPN > IKEv2 > IKE-CFG > Split-DNS

Name

Enter a name for this profile.

SNMP ID:

2.19.36.7.3.4.1

Console path:

Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Profiles

Possible values:

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

Default:

empty

Send-DNS-Forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

SNMP ID:

2.19.36.7.3.4.2

Console path:

Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Profiles

Possible values:

No
Yes

Default:

No

Send-local-Domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

SNMP ID:

2.19.36.7.3.4.3

Console path:

Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Profiles

Possible values:

No
Yes

Default:

No

Domain-List

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

SNMP ID:

2.19.36.7.3.4.4

Console path:

Setup > VPN > IKEv2 > IKE-CFG > Split-DNS > Profiles

Possible values:

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

Default:

empty

Cookie-Challenge

IKEv2 offers cookie notification, a challenge-response procedure that the IKEv2 responder can trigger if it has too many half-open IKEv2 connections. This makes the responder more resistant to DDoS attacks.

Cookie notification has been implemented to improve the compatibility with third-party VPN-enabled devices. It must be enabled on both VPN participants in order for a VPN connection to be established.

The IKEv2 cookie notification prevents the establishment of excessive numbers of half-open VPN connections and the attack on VPN-gateway resources (DDOS) that they cause. With cookie notification enabled, the responder only reacts to incoming VPN connections if the remote site is verified as reachable.

Enabling the IKEv2 cookie challenge adds two additional IKE messages to the VPN connection setup.

The switch activates the Cookie Challenge on the responder or gateway side.

On the initiator side, the cookie challenge is done automatically if the other side requests it. The switch has no effect on the initiator side or on the client side.

Please note that both initiator and responder must support the cookie challenge feature. If the remote site does not support cookie challenge, the VPN tunnel cannot be established. LANCOM VPN routers at both ends must have at least LCOS 10.30.

SNMP ID:

2.19.36.12

Console path:

Setup > VPN > IKEv2

Possible values:

Off

Always

Default:

Off

Enforce-Pre-Shared-Key-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for Pre-Shared Keys (PSK) with IKEv2:

- > The length of the password must be at least 32 characters.
- > The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

 These rules do not apply to PSK managed and obtained by a RADIUS server.

SNMP ID:

2.19.36.14

Console path:

Setup > VPN > IKEv2

Possible values:**No**

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

No

RSA-Padding-Method

Specifies the RSA padding method for certificates issued by the SCEP-CA.

SNMP ID:

2.39.2.15

Console path:

Setup > Certificates > SCEP-CA

Possible values:**PKCS1**

Certificate padding is performed with the RSASSA-PKCS1-v1_5 method.

PSS

Certificate padding is performed with the RSASSA-PSS method

Default:

PKCS1

9 Public Spot

9.1 Double the number of Public Spot users

As of LCOS 10.30, the following routers of the 178x- and 179x-series are now able to manage up to 128 concurrent Public Spot users, instead of the former 64:

- > LANCOM 179x-Serie
- > LANCOM 1781Vx-Serie
- > LANCOM 1781EF+
- > LANCOM 1781EW+
- > LANCOM 1783-Serie
- > LANCOM 88x-Serie

9.2 Passpoint® Release 2

As of LCOS 10.32 RU4, your WLAN device supports advanced Hotspot-2.0 functions according to Passpoint® Release 2 as specified by the Wi-Fi Alliance. For WLAN controllers, this feature is in preparation. As of 10.32 version RU4, the RADIUS server in the LCOS is equipped with the necessary features.

Passpoint® Release 2 simplifies the onboarding of devices into a network using the WPA2-Enterprise (802.1X) encryption method. A dedicated onboarding SSID allows a user with a device that supports Passpoint® Release 2 to install a profile and automatically switch to the encrypted network using the stored credentials. This helps to implement hotspots that provide encrypted wireless communication. An onboarding SSID can be used to give guests temporary access credentials.


Similarly, a mobile service provider can relieve the load on their cellular network by introducing Wi-Fi offloading and allowing mobile devices with a SIM card to automatically log into their WLAN network. Customers' devices find the WLAN network from the mobile service provider and automatically login to the operator's WLAN network using the user data stored on the SIM card.


Passpoint® Release 2 adds the following features to Hotspot 2.0:

- > Online Sign-Up (OSU) – with Passpoint® Release 2, companies and network operators can use "Online Sign-Up" servers (OSU servers) to deliver profiles to their users. Using an open OSU SSID, users can identify various OSU servers by their icons and thus select the one that suits them best. The OSU server can optionally ask the user for credentials before providing a profile that best suits the user's device. In addition to the open OSU-SSID, an encrypted SSID can be used to exchange user data by means of "anonymous EAP-TLS". This requires the use of a RADIUS server that supports "anonymous EAP-TLS".

 An OSU server is not included with LCOS. However, solutions are available from LANCOM partners.

- > OSU icons – icons corresponding to the supported OSU servers can be uploaded to the LCOS as files using the WEBconfig feature **File management**. We recommend PNG as the file format.
- > Notification – the network can notify the user about an imminent logout from the RADIUS server. This may be the case if the user credentials have expired or if the specified connection duration has been reached.
- > QoS Map – the "QoS Map Set" function enables an access point to instruct its clients to use a specific QoS map. This defines the values for the contention window (media access via EDCA) of the various access categories (voice, video, best effort and background data packets) and the corresponding DSCP parameters. At the same time, the access points also use the values stored in the QoS map.

 Currently, only the standard LCOS QoS map is available in addition to the two QoS maps specified by the Wi-Fi Alliance.

 These new features have to be configured through the command-line interface. Support in LANconfig will be available as of LCOS 10.40.

9.2.1 Additions to the Setup menu

QoS

Use this menu to specify a QoS map set.

SNMP ID:

2.12.134

Console path:

Setup > WLAN

QoS-Map-Source

Set one of the predefined QoS map sets here.

SNMP ID:

2.12.134.1

Console path:

Setup > WLAN > QoS

Possible values:

LAN-Config

Standard QoS map of the LCOS.

ID1

One of the QoS maps predefined by the Wi-Fi Alliance.

ID2

One of the QoS maps predefined by the Wi-Fi Alliance.

Default:

LAN-Config

Hotspot2.0

Use this menu to adjust settings that are specific to HotSpot 2.0/Passpoint.

SNMP ID:

2.12.135

Console path:**Setup > WLAN****Check-Release**

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

SNMP ID:

2.12.135.1

Console path:**Setup > WLAN > Hotspot2.0****Possible values:****Yes****Off****Default:**

Yes

ARP-Handling-Settings

The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. In most cases an alternative is to suppress broadcasts/multicasts by using [Transmit-only-Unicasts](#).

SNMP ID:

2.12.136

Console path:**Setup > WLAN****Unknown-Address-Action**

In case of an unknown address, the packet is either forwarded or discarded.

SNMP ID:

2.12.136.2

Console path:**Setup > WLAN > ARP-Handling-Settings**

Possible values:

Forward
Discard

Default:

Forward

Broadcast-Response-Action

In case of a broadcast, the packet is either forwarded or discarded.

SNMP ID:

2.12.136.3

Console path:

Setup > WLAN > ARP-Handling-Settings

Possible values:

Forward
Discard

Default:

Forward

Method

Select the default EAP authentication method.

SNMP ID:

2.25.10.10.9.1

Console path:

Setup > RADIUS > Server > EAP > Allow-Methods

Possible values:

None
MD5
GTC
MSCHAPv2
TLS
TTLS
PEAP
WFA-Unauth

This method only needs to be enabled when using the RADIUS server in the LCOS for an encrypted OSU SSID.

Default:

MD5

GTC

MSCHAPv2


TLS

TTLS

PEAP

Hotspot2.0-Release

Set the Hotspot-2.0 release supported by this profile.

 A client must support this release in order to connect.

SNMP ID:

2.71.7.9.5

Console path:

Setup > IEEE802.11u > Hotspot2.0 > Hotspot2.0-Profiles

Possible values:

Release-1
Release-2

Domain-Id

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16-bit value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

SNMP ID:

2.71.7.9.6

Console path:**Setup > IEEE802.11u > Hotspot2.0 > Hotspot2.0-Profiles****Possible values:**

Max. 5 characters from [0-9]

Default:

0

OSU-Network-Name

Name of the SSID that provides access to the OSU server.

SNMP ID:

2.71.7.9.7

Console path:**Setup > IEEE802.11u > Hotspot2.0 > Hotspot2.0-Profiles****Possible values:**

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

Default:*empty***OSU-Providers**

List of OSU provider names in [2.71.7.10 OSU-Providers](#) on page 55 that are supported in the profile.

SNMP ID:

2.71.7.9.8

Console path:**Setup > IEEE802.11u > Hotspot2.0 > Hotspot2.0-Profiles****Possible values:**

Max. 250 characters from [A-Z][a-z][0-9]#@[|]~!\$%&'()*+,-./:;<=>?[\]^_`~`

Default:*empty*

OSU-Providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.

SNMP ID:

2.71.7.10

Console path:

Setup > IEEE802.11u > Hotspot2.0

Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

SNMP ID:

2.71.7.10.1

Console path:

Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers

Possible values:

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

Language

Set the language supported by this OSU provider.

SNMP ID:

2.71.7.10.2

Console path:

Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers

Possible values:

None
 English
 Deutsch
 Chinese
 Spanish
 French
 Italian
 Russian
 Dutch
 Turkish
 Portuguese
 Polish
 Czech
 Arabian
 Korean

Friendly-Name

Give this OSU provider a descriptive name.

SNMP ID:

2.71.7.10.3

Console path:

Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers

Possible values:

Max. 250 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_`~``

OSU-Methods

Set the OSU methods used by this OSU provider. See also [2.71.7.11 OSU-Methods](#) on page 59. Options are "OMA-DM" or "SOAP-XML-SPP".

SNMP ID:

2.71.7.10.4

Console path:

Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers

Possible values:

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

URI

Enter a URI where a client can reach the OSU server.

SNMP ID:

2.71.7.10.5

Console path:**Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers****Possible values:**

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

NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

SNMP ID:

2.71.7.10.6

Console path:**Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers****Possible values:**

Max. 65 characters from [A-Z] [a-z] [0-9] #@{ } ~!\$%&'()*+,-./:;<=>?[\]^_`~`

Service-Description

Enter a descriptive text for this service here.

SNMP ID:

2.71.7.10.7

Console path:**Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers****Possible values:**

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

Icon-FilenameSelect an icon for this OSU provider. Icons can be uploaded as files with WEBconfig by using the **File management** feature. We recommend PNG as the file format.**SNMP ID:**

2.71.7.10.8

Console path:**Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers**

Possible values:

- None
- OSU-Prov-Img-1
- OSU-Prov-Img-2
- OSU-Prov-Img-3
- OSU-Prov-Img-4
- OSU-Prov-Img-5
- OSU-Prov-Img-6
- OSU-Prov-Img-7
- OSU-Prov-Img-8
- OSU-Prov-Img-9
- OSU-Prov-Img-10
- OSU-Prov-Img-11
- OSU-Prov-Img-12
- OSU-Prov-Img-13
- OSU-Prov-Img-14
- OSU-Prov-Img-15
- OSU-Prov-Img-16

Icon-Language

This item sets the language for the selected icon.

SNMP ID:

2.71.7.10.9

Console path:

Setup > IEEE802.11u > Hotspot2.0 > OSU-Providers

Possible values:

None
English
German
Chinese
Spanish
French
Italian
Russian
Dutch
Turkish
Portuguese
Polish
Czech
Arabic
Korean

OSU-Methods

This table contains a fixed list of methods available on the online sign-up server when using Passpoint® Release 2.

- > OMA – Open Mobile Alliance
- > DM – Device Management
- > SOAP – Simple Object Access Protocol
- > XML – eXtended Markup Language
- > SPP – Subscription Provisioning Protocol

SNMP ID:

2.71.7.11

Console path:

Setup > IEEE802.11u > Hotspot2.0

Load-Meas.-Duration

Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

SNMP ID:

2.71.7.12

Console path:

Setup > IEEE802.11u > Hotspot2.0

Possible values:

Max. 5 characters from [0-9]


Default:

0


10 IoT – the Internet of Things

The configuration of IoT technologies supported by LCOS have been collected under the new menu item “IoT”. This change concerns not only LANconfig, but the LCOS menu as well. As a consequence, the paths for the features Wireless ePaper, iBeacon, and Bluetooth Low Energy are changing to:

- > **Setup > IoT > Wireless ePaper**
- > **Status > IoT > Wireless ePaper**
- > **Setup > IoT > Bluetooth > iBeacon** (E-series devices only)
- > **Status > IoT > Bluetooth > iBeacon** (E-series devices only)
- > **Setup > IoT > Bluetooth** (E-series devices only)
- > **Status > IoT > Bluetooth** (E-series devices only)

 Existing devices are unaffected by this changeover on the command line. This allows the continued use of existing configuration backups that still contain the old menu structure. This pertains to

- > L-151E
- > L-322E
- > LN-830E

 In LANconfig, the new structure is used for **all** devices, since the display here is independent of the menu structure of the command line.

Here you will find the settings for IoT technologies supported by LCOS, such as Wireless ePaper, iBeacon and Bluetooth Low Energy.

IoT networks interconnect physical and virtual objects to facilitate the exchange of data and information. Typical examples include sensors, smart home appliances, digital room signs, and electronic shelf labels. IoT devices are largely networked by radio, using a variety of wireless technologies such as modified ZigBee variants (retail IoT), Bluetooth Low Energy (BLE), or the various cellular offshoots. There is no uniform “IoT wireless standard”, and new IoT radio technologies are emerging in rapid cycles.

The special settings for IoT are made in LANconfig under **IoT**.

10.1 Wireless ePaper

Centralized management of your Wireless ePaper infrastructure

As of LCOS 10.32, LANCOM access points with Wireless ePaper support now support a new protocol that ensures efficient and reliable communications between the Wireless ePaper server and access points. Thanks to the support of this new protocol, your LANCOM Wireless ePaper Displays can now be managed remotely from the Wireless ePaper Server at your data center and controlled via VPN. The new protocol will be used if both ends support the protocol and it is enabled on the Wireless ePaper server.

In the top right corner of the Wireless ePaper management, you can click the gear icon and then **Settings** to access general settings options for the Wireless ePaper Server. There you can activate the new protocol.

In LANmonitor, the display of the device under **IoT > Wireless ePaper > Protocol version** displays the protocol that is in use:

- > None – there is no connection to a controller/server
- > ThinAP1.0/UDP – protocol version 1.0 (UDP-based, legacy)
- > ThinAP2.0/TCP – protocol version 2.0 (TCP-based, recommended from LCOS 10.32)

i The Wireless ePaper Server supports “protocol version 2.0” from version 1.91. If you already use this and yet only “protocol version 1.0” is displayed here, the protocol was probably not yet enabled in the Wireless ePaper server settings. Please proceed as follows, whereby the activation of the new protocol version is shown here alternatively via the command line:

1. Check the following prerequisites:
 - > LANCOM Wireless ePaper Server version 1.91 or higher is installed
 - > cURL is installed
2. Open the command line on your operating system and enter the following command:


```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=true
```
3. Restart the Wireless ePaper Server.
4. Then enter the following command to verify that the feature was successfully enabled:


```
curl -X GET http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode
```

If activation was successful the output is as follows:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Configuration key="lancomUseTcpThinMode" type="BOOLEAN" defaultValue="false" value="true"/>
```

The command

```
curl -X PUT http://<server-ip>:8001/service/configuration/lancomUseTcpThinMode?value=false
```

disables the function of the TCP-based Wireless ePaper protocol.

10.1.1 Installation and Configuration of a Wireless ePaper USB

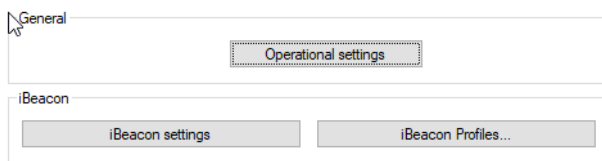
As of LCOS 10.32, ePaper support can be provided for LANCOM devices with a USB port but without direct ePaper support via the LANCOM Wireless ePaper USB. For more information, refer to the LANCOM Wireless ePaper Server user manual.

10.2 BLE scanner and beacon

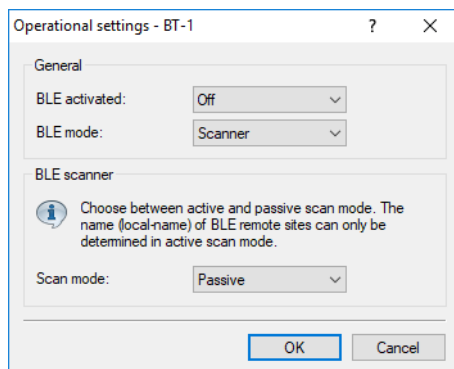
B-series wi-fi devices feature Bluetooth Low Energy (BLE) support for the following technologies: Beacon transmission (e.g. iBeacon) and BLE environment scanning, which in combination with a suitable processing system can be used for applications such as asset tracking or visitor counting.

10.2.1 Settings for BLE

The settings for BLE are made in LANconfig under **IoT > Bluetooth LE**.



Operational settings




BLE activated

Activate the BLE module here.

BLE mode

This entry allows you to set the operating mode of the BLE module. Choose whether to use the Bluetooth interface for sending beacons or for scanning the environment.

 The two operating modes cannot be operated simultaneously.

Scanner

The BLE module is used for scanning the environment.

BLE-Beacon

The BLE module sends out beacons.

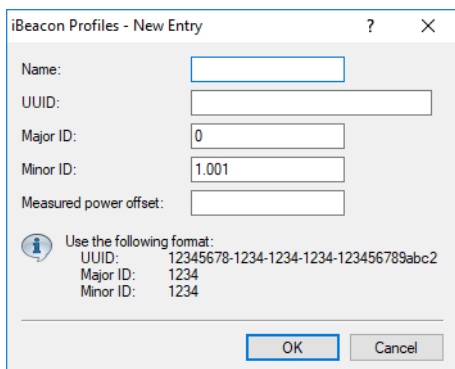
Scan mode

Select here whether to use active or passive scanning. With active scanning, requests are sent actively and any BLE clients in the surroundings can respond to them. This is necessary to determine the names of the clients, for example.

! Please note that continuously responding to scan requests can affect client battery life. With passive scanning, no scan requests are sent but only passively listened for.

iBeacon profiles

Here you define profiles that you can later assign to a BLE interface.



Name

Give the iBeacon profile a name.

UUID

A 16-byte identifier used to group together larger groups of beacons. For example, all iBeacons of a company could share the same iBeacon UUID.

Major ID

A 2-byte identifier used to distinguish subgroups of iBeacons. For example, all iBeacons at a company branch office could share the same major identifier.

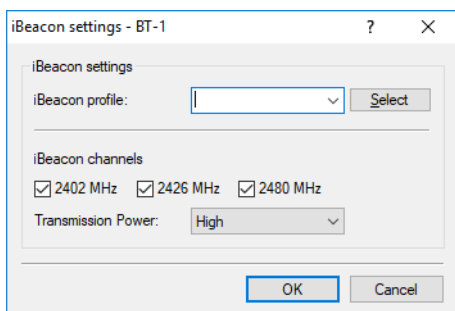
Minor ID

A 2-byte identifier used to distinguish individual iBeacons. For example, each individual iBeacon in a branch office could have its own minor identifier.

Empfangsleistungsverschiebung

Normally, a power value measured according to the set transmit power is used to detect the approximation and exact distance of devices emitting a beacon. On the basis of the corresponding measurement series, a deviation can be determined between the measured reception power and actual distance from the device emitting the beacon. Based on this deviation, experts can specify a offset of the reference value of the device in order to increase the measurement accuracy.

iBeacon settings



iBeacon profile

Here you select iBeacon profile to set the UUID, Major ID and Minor ID, etc.

iBeacon channels

Here you select the channels used to broadcast the iBeacon.

Transmission power

Select the transmission power here. The exact meaning of the values that can be selected here is explained in the iBeacon specification. The following values are possible:

High

The module sends with maximum power (default).

Medium

The module sends with medium power.

Low

The module sends with minimum power.

10.2.2 Monitoring

Monitoring on the CLI

In scanning mode, the scan results are viewed in the table **Status > IoT > Bluetooth > Scan-Results**.



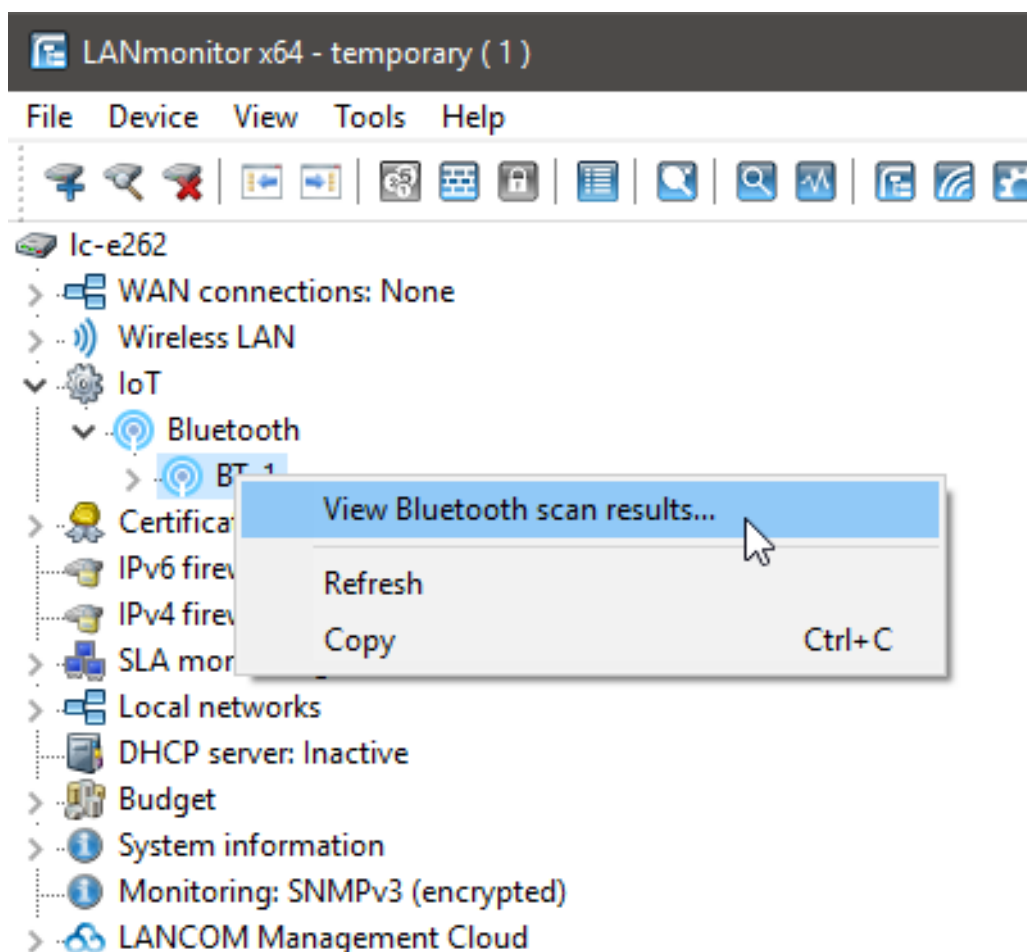
Note that the iBeacon-related values are only filled in when the scanned client actually is an iBeacon.



The implementation of applications such as asset tracking requires these values to be read out by an external system. This can be done with the usual methods for accessing LANCOM devices, preferably by SNMP.

Monitoring with LANmonitor

In Scanning mode, the scan results in LANmonitor can be viewed in tabular form. The scan result table can be accessed via the context menu of the corresponding Bluetooth module:



i Note that the iBeacon-related values are only filled in when the scanned client actually is an iBeacon.

i The implementation of applications such as asset tracking requires these values to be read out by an external system. This can be done with the usual methods for accessing LANCOM devices, preferably by SNMP.

10.3 Additions to the Setup menu

10.3.1 IoT

Settings for IoT technologies supported by LCOS, such as Wireless ePaper, iBeacon and Bluetooth Low Energy.

SNMP ID:

2.111

Console path:
Setup

Wireless-ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:
2.111.88

Console path:
Setup > IoT

Operating

This entry allows you to set the operating mode of the module.

SNMP ID:
2.111.88.1

Console path:
Setup > IoT > Wireless-ePaper

Possible values:

No
The module is not enabled.

Manual
Wireless ePaper configurations are done manually.

Managed
The module is managed by a WLAN controller.

Default:
Manual

Port

Assign a port to the Wireless ePaper module.

SNMP ID:
2.111.88.2

Console path:
Setup > IoT > Wireless-ePaper

Possible values:

Max. 5 characters from [0–9]

Default:

2002

Channel

Set which channel the Wireless ePaper module should use.



If you need to *coordinate the channel selection* due to several APs being within range of one another, you should select automatic channel selection here.

SNMP ID:

2.111.88.3

Console path:

Setup > IoT > Wireless-ePaper

Possible values:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:

2425MHz

Channel-Coordination

Prevents collisions on ePaper channels due to APs within range of each other.

SNMP ID:

2.111.88.4

Console path:

Setup > IoT > Wireless-ePaper

Operating

The coordinated channel selection is activated or deactivated here.

SNMP ID:

2.111.88.4.1

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

0

No

1

Yes

Default:

1

Network

Here you specify the network that the access points are to use to communicate with each other.

SNMP ID:

2.111.88.4.2

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

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

Announce-address

Set the announce address here.

SNMP ID:

2.111.88.4.3

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

39 characters from the following character set: [0-9 A-F a-f :.]

Announce-port

Set the announce port here.

SNMP ID:

2.111.88.4.4

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

5 characters from the following character set: [0–9]

Announce-interval

Set the announce interval here.

SNMP ID:

2.111.88.4.5

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

10 characters from the following character set: [0–9]

Announce-timeout-factor

Set the announce timeout factor here.

SNMP ID:

2.111.88.4.6

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

5 characters from the following character set: [0–9]

Announce-timeout-interval

Set the announce timeout interval here.

SNMP ID:

2.111.88.4.7

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

10 characters from the following character set: [0-9]

Announce-master-backoff-interval

Set the announce master backoff interval here.

SNMP ID:

2.111.88.4.8

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

3 characters from the following character set: [0-9]

Coordination-port

Set the coordination port here.

SNMP ID:

2.111.88.4.9

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

5 characters from the following character set: [0-9]

Coordination-keep-alive-interval

Here you set the coordination keep-alive interval.

SNMP ID:

2.111.88.4.10

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

10 characters from the following character set: [0-9]

Coordination-reconnect-interval

Here you set the coordination reconnect interval.

SNMP ID:

2.111.88.4.11

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

10 characters from the following character set: [0-9]

Assignment-switch-threshold

Here you set the assignment switch threshold.

SNMP ID:

2.111.88.4.12

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

3 characters from the following character set: [0-9]

Distance-weighting

Here you set the weighting of WLAN distance.



A higher value means a better weighting.

SNMP ID:

2.111.88.4.13

Console path:

Setup > IoT > Wireless-ePaper > Channel-Coordination

Possible values:

0 ... 255

Channel-weighting

Here you set the weighting of a preferred channel.



A higher value means a better weighting.

SNMP ID:

2.111.88.4.14

Console path:**Setup > IoT > Wireless-ePaper > Channel-Coordination****Possible values:**

0 ... 255

Bluetooth

This menu allows you to configure Bluetooth devices.

SNMP ID:

2.111.90

Console path:**Setup > IoT****iBeacon**

This entry allows you to configure the iBeacon module in E-series devices.

SNMP ID:

2.111.90.1

Console path:**Setup > IoT > Bluetooth****Operating**

This entry allows you to set the operating mode of the module.

SNMP ID:

2.111.90.1.1

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:****No**

The module is not enabled.

Manual

iBeacon configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Managed

UUID

This entry allows you to assign a “universally unique identifier” (UUID) to the iBeacon module.

SNMP ID:

2.111.90.1.2

Console path:

Setup > IoT > Bluetooth > iBeacon

Possible values:

Max. 36 characters from `[0-9] [a-f] [A-F] -`

Default:

00000000-0000-0000-0000-000000000000

Major

Assign a unique major ID to the iBeacon module.

SNMP ID:

2.111.90.1.3

Console path:

Setup > IoT > Bluetooth > iBeacon

Possible values:

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

1 ... 65535 Integer value

Default:

2002

Minor

Assign a unique minor ID to the iBeacon module.

SNMP ID:

2.111.90.1.4

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:**

Max. 5 characters from [0-9]

1 ... 65535 Integer value

Default:

1001

Reception-power-shift

Specify the reception power shift.

SNMP ID:

2.111.90.1.5

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:**

Max. 4 characters from [0-9] -

-128 ... 127

Default:

0

Transmission-power

Set the transmission power of the iBeacon module.

SNMP ID:

2.111.90.1.6

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:****Low**

The module sends with minimum power.

Medium

The module sends with medium power.

High

The module sends with maximum power.

Default:

High

Channels

Set which channels the iBeacon module should use to transmit.

SNMP ID:

2.111.90.1.7

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:****2402MHz**

The module transmits on channel 2402.

2426MHz

The module transmits on channel 2426.

2480MHz

The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz

The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

Coexistence

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

SNMP ID:

2.111.90.1.8

Console path:**Setup > IoT > Bluetooth > iBeacon****Possible values:****No****Yes****Default:**

Yes

Module-restart

This command causes the iBeacon module to restart.

SNMP ID:

2.111.90.1.9

Console path:

Setup > IoT > Bluetooth > iBeacon

Operational

This entry allows you to configure the operating settings for the BLE module in B-series devices.

SNMP ID:

2.111.90.2

Console path:

Setup > IoT > Bluetooth

Ifc

Select the device BLE interface that is relevant to the settings, e.g. BT-1.



The selection options depend on the equipment of the device.

SNMP ID:

2.111.90.2.1

Console path:

Setup > IoT > Bluetooth > Operational

Operating

This entry allows you to activate the module.

SNMP ID:

2.111.90.2.2

Console path:

Setup > IoT > Bluetooth > Operational

Possible values:**Yes**

The module is enabled.

No

The module is not enabled.

Default:

No

Operation-Mode

This entry allows you to set the operating mode of the BLE module. Choose whether to use the Bluetooth interface for sending beacons or for scanning the environment.

 The two operating modes cannot be operated simultaneously.

SNMP ID:

2.111.90.2.3

Console path:

Setup > IoT > Bluetooth > Operational

Possible values:**BLE-Beacon**

The BLE module sends out beacons.

Scanner


The BLE module is used for scanning the environment.

Default:

Scanner

Scan-Mode

Select here whether to use active or passive scanning. With active scanning, requests are sent actively and any BLE clients in the surroundings can respond to them. This is necessary to determine the names of the clients, for example.

 Please note that continuously responding to scan requests can affect client battery life. With passive scanning, no scan requests are sent but only passively listened for.

SNMP ID:

2.111.90.2.4

Console path:

Setup > IoT > Bluetooth > Operational

Possible values:

Passive
Active

Default:

Passive

Beacon-Settings

Use this item to configure additional iBeacon parameters on B-series devices.

SNMP ID:

2.111.90.3

Console path:

Setup > IoT > Bluetooth

lfc

Select the device BLE interface that is relevant to the settings, e.g. BT-1.



The selection options depend on the equipment of the device.

SNMP ID:

2.111.90.3.1

Console path:

Setup > IoT > Bluetooth > Beacon-Settings

Beacon-Profiles

Use this item to enter the name of the iBeacon profile created in the Beacon-Profiles table.

SNMP ID:

2.111.90.3.2

Console path:

Setup > IoT > Bluetooth > Beacon-Settings

Possible values:

Max. 17 characters from `[A-Z][0-9]@{|}~!$%&'()+,-./:;<=>?[\]^_.`

Default:

empty

Channels

Here you select the BLE channels used to broadcast the iBeacon.

SNMP ID:

2.111.90.3.3

Console path:

Setup > IoT > Bluetooth > Beacon-Settings

Possible values:

2402MHz

The module transmits on channel 2402.

2426MHz

The module transmits on channel 2426.

2480MHz

The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz

The module transmits on all channels.

Default:

2402MHz, 2426MHz, 2480MHz

Transmit-Power

Select the transmission power here. The exact meaning of the values that can be selected here is explained in the iBeacon specification.

SNMP ID:

2.111.90.3.4

Console path:

Setup > IoT > Bluetooth > Beacon-Settings

Possible values:

Low

The module sends with minimum power.

Medium

The module sends with medium power.

High

The module sends with maximum power.

Default:

High

Beacon-Profiles

Use this item to configure the iBeacon parameters on B-series devices.

SNMP ID:

2.111.90.4

Console path:

Setup > IoT > Bluetooth

Name

Configure a name for this beacon profile here.

SNMP ID:

2.111.90.4.1

Console path:

Setup > IoT > Bluetooth > Beacon-Profiles

Possible values:

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

Default:

empty

iBeacon-UUID

A 16-byte identifier used to group together larger groups of beacons. For example, all iBeacons of a company could share the same iBeacon UUID.

SNMP ID:

2.111.90.4.2

Console path:

Setup > IoT > Bluetooth > Beacon-Profiles

Possible values:

Max. 36 characters from `[A-Z][a-f][0-9]-`

Default:

empty

iBeacon-Major

A 2-byte identifier used to distinguish subgroups of iBeacons. For example, all iBeacons at a company branch office could share the same major identifier.

SNMP ID:

2.111.90.4.3

Console path:**Setup > IoT > Bluetooth > Beacon-Profiles****Possible values:**

Max. 5 characters from [0-9]

Default:*empty***iBeacon-Minor**

A 2-byte identifier used to distinguish individual iBeacons. For example, each individual iBeacon in a branch office could have its own minor identifier.

SNMP ID:

2.111.90.4.4

Console path:**Setup > IoT > Bluetooth > Beacon-Profiles****Possible values:**

Max. 5 characters from [0-9]

Default:*empty***Measured-Power-Offset**

Normally, a power value measured according to the set transmit power is used to detect the approximation and exact distance of devices emitting a beacon. On the basis of the corresponding measurement series, a deviation can be determined between the measured reception power and actual distance from the device emitting the beacon. Based on this deviation, experts can specify a offset of the reference value of the device in order to increase the measurement accuracy.

SNMP ID:

2.111.90.4.5

Console path:**Setup > IoT > Bluetooth > Beacon-Profiles****Possible values:**

Max. 16 characters from [0-9] -

-128 ... 127

Default:*empty*

11 Other services

11.1 DHCP server – suppress ARP request

As of LCOS 10.32 RU4 your device supports the option to suppress the ARP request that usually precedes the assignment of an IP address.

11.1.1 Additions to the Setup menu

Suppress-ARP-check

Before the DHCP server assigns an IP address, an ARP request is usually used to check whether the address has been assigned already. If there is no response to the ARP request within 3 seconds, the assignment goes ahead. This query is especially useful when computers are booting in normal networks that use fixed IP addresses. In a Public Spot network where, for example, a smartphone has to recognize that there is no Internet connection in order to display the login popup, this ARP request leads to an unnecessary delay. For scenarios such as this, this check can be disabled here.

SNMP ID:

2.10.20.23

Console path:**Setup > DHCP > Network-List****Possible values:****Yes**

Do not carry out check by ARP request.

No

Perform check by ARP request.

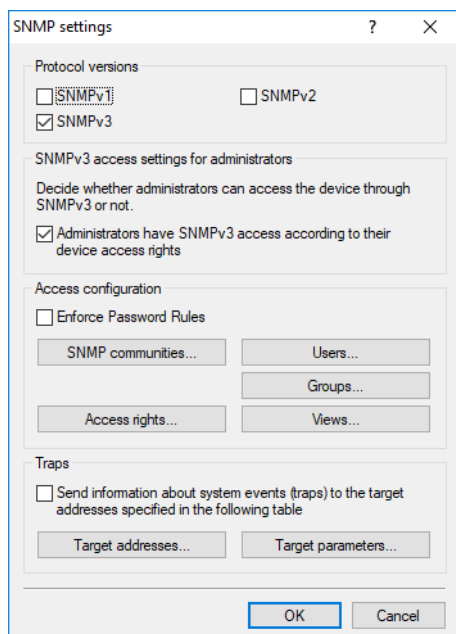
Default:

No

11.2 Simple Network Management Protocol (SNMP)

11.2.1 SNMPv3 Password Rules

LCOS as of version 10.32 supports enforcing password rules for SNMPv3 authentication and the password for SNMPv3 encryption. The setting is made under **Management > Admin > SNMP settings > Access configuration** using the **Enforce Password Rules** option.



The following rules become active:

- > The length of the password must be at least 16 characters.
- > The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

⚠ Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

11.2.2 Additions to the Setup menu

Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for the SNMPv3 passwords:

- > The length of the password must be at least 16 characters.
- > The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

⚠ Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

⚠ Please note that SNMPv3 only uses passwords, when in the table **Setup > SNMP > Users** neither **Authentication-Protocol** nor **Privacy-Protocol** is set to **None**.

SNMP ID:

2.11.93

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

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

No

11.3 TACACS+

11.3.1 Configuring the TACACS+ server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

As of LCOS 10.30, TACACS+ supports IPv6. Consequently, the server address can be configured as a DNS name, an IPv4 address, and also as an IPv6 address.

The parameters for configuring the TACACS+ server are to be found under:

Command line: **Setup > TACACS+ > Server**

Server address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Possible values:

> Valid DNS resolvable name, or valid IPv4 or IPv6 address.

Default

> Blank

Additions to the Setup menu

Server-address

DNS name, or IPv4 or IPv6 address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

SNMP ID:

2.54.9.1

Console path:

Setup > Tacacs+ > Server

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@[|}~!$%&'()*+,-./:;<=>?[\]^_``

Default:

empty