

LCOS 10.42

Addendum

05/2024



LANCOM
SYSTEMS

Contents

- 1 Addendum to LCOS version 10.42.....5**
- 2 Routing and WAN connections.....6**
 - 2.1 SD-WAN Dynamic Path Selection.....6
 - 2.1.1 Configuring Dynamic Path Selection.....7
 - 2.1.2 Show commands.....10
 - 2.1.3 Sample configurations.....10
 - 2.1.4 Additions to the Setup menu.....12
- 3 Virtual Private Networks – VPN.....24**
 - 3.1 IKEv2 Auto IP.....24
 - 3.1.1 IKEv2-Auto-IP-Profile.....25
 - 3.1.2 Additions to the Setup menu.....25
 - 3.2 IPv6 address range can be controlled for VPN negotiation.....27
 - 3.2.1 Additions to the Setup menu.....27
- 4 Wireless LAN – WLAN.....28**
 - 4.1 WPA default passphrase deprecated.....28
 - 4.2 RTLS (real-time location system).....28
 - 4.2.1 Stanley AeroScout RTLS.....28
 - 4.2.2 Additions to the Setup menu.....29
 - 4.3 Location-based services (LBS).....33
 - 4.3.1 HTTP interface.....34
 - 4.3.2 Additions to the Setup menu.....38
- 5 WLAN management.....41**
 - 5.1 Configuring Passpoint Release 2 via the WLAN controller.....41
 - 5.1.1 Additions to the Setup menu.....41
 - 5.2 Extension of the Wireless ePaper profiles.....47
 - 5.2.1 Additions to the Setup menu.....47
- 6 Public Spot.....49**
 - 6.1 Extension of the Public Spot port table for the LANCOM Management Cloud.....49
 - 6.1.1 Additions to the Setup menu.....49
- 7 Voice over IP – VoIP.....50**
 - 7.1 Source address for SIP and SIP PBX lines.....50
 - 7.2 SIP-ID transmission.....51
 - 7.2.1 Additions to the Setup menu.....52
- 8 IoT – the Internet of Things.....54**
 - 8.1 Wireless ePaper.....54
 - 8.1.1 Settings for Wireless ePaper.....54
- 9 Other services.....55**
 - 9.1 802.1X authenticator for Ethernet ports.....55
 - 9.1.1 Additions to the Setup menu.....57

10 Enhancements in the menu system.....	61
10.1 Require-Msg-Authenticator.....	61
10.2 L2TP-Require-Msg-Authenticator.....	61
10.3 Require-Msg-Authenticator.....	62
10.4 Require-Msg-Authenticator.....	62
10.5 Backup-Require-Msg-Authenticator.....	63
10.6 Require-Msg-Authenticator.....	63
10.7 Require-Msg-Authenticator.....	64
10.8 Require-Msg-Authenticator.....	64
10.9 Require-Msg-Authenticator.....	65

Copyright

© 2021 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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

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

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

LANCOM, LANCOM Systems, 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 10.42

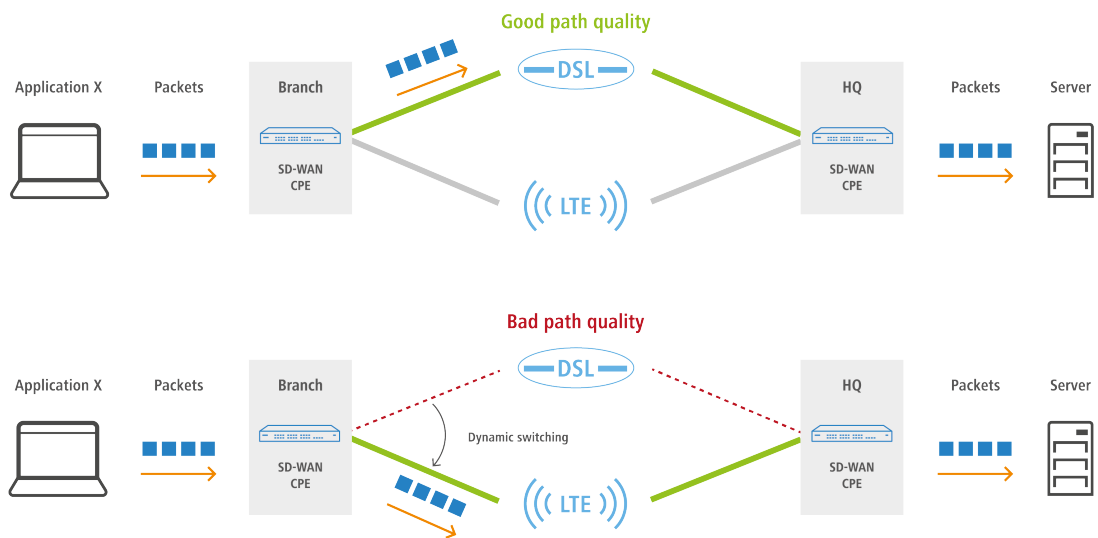
This document describes the changes and enhancements in LCOS version 10.42 since the previous version.

2 Routing and WAN connections

2.1 SD-WAN Dynamic Path Selection

Used in an SD-WAN scenario where several lines are available, Dynamic Path Selection (DPS) optimizes the performance of an application by directing data traffic over the line with the best quality as rated by metrics such as load, packet loss, latency or jitter.

In SD-WAN scenarios, MPLS lines should either be replaced or supplemented by cost-effective Internet connections such as DSL, cable Internet, fiber optic or 4G/5G. Load balancing helps to make use of the total bandwidth of all of the available lines. Dynamic Path Selection can be used to assure the performance of mission-critical applications. All lines are continuously, actively monitored with ICMP packets to calculate metrics for load, packet loss, latency and jitter. Policies are used to define the requirements of business applications: For example, the real-time data traffic on lines can be monitored for the allowed packet loss or the maximum latency of a possible path. The dynamic path selection algorithm selects the best quality line for sessions. If several lines meet the requirements, load balancing distributes the load across these lines by means of round-robin scheduling.



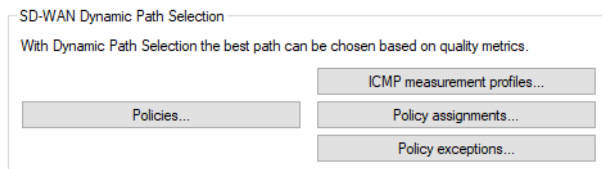
⚠ Policies can be defined as "critical". If none of the lines fulfill the policy, no data traffic is transported at all.

Dynamic path selection is activated on a load balancer. A load balancer can be defined either for Internet connections or for SD-WAN overlay tunnels (VPN). The end point for ICMP test packets can either be any IP address or the central-site SD-WAN gateway.

In the firewall, the defined (load balancer) policies for the applications are used in corresponding firewall rules. There, the traffic or applications to which the load balancer policy is to apply are defined.

2.1.1 Configuring Dynamic Path Selection

To configure dynamic path selection with LANconfig, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection**.



ICMP measurement profiles

ICMP measurement profiles specify a parameter set used by measurements that are based on ICMP pings. Interface metrics are derived from measurements to quantify the connection quality. These metrics are: Average round trip time (RTT, latency), jitter and packet loss rate.

To configure the ICMP measurement profiles, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > ICMP measurement profiles**.

Measurement profile

The name of the profile. This name is used to reference the profile in DPS policies.

DSCP value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

Source address (optional)

References a named loopback address that is used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

IPv4 destination 1-4

Up to 4 measurement destinations as valid IPv4 unicast addresses or DNS hostnames. With 0.0.0.0 entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

Payload size

Specifies the size of the data payload that follows the ICMP header (payload size) of the pings being sent.

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

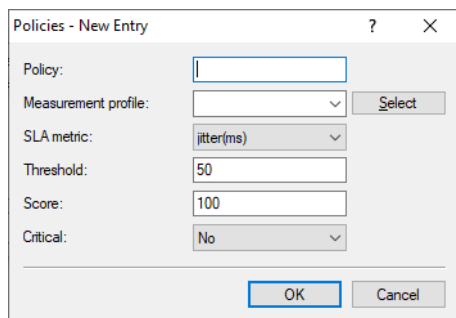
Sliding window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

Policies

To evaluate the connection quality of the interfaces used for Dynamic Path Selection, the metrics calculated from the measurement profiles are compared to threshold values, and points (as a score) are awarded. These points added up to determine which is the “best” interface. Certain thresholds can be specified as being “critical” (e.g. jitter <= 30 ms). Dynamic load balancer decisions are based on the points total in combination with the exceeded critical threshold values. A DPS policy collects the threshold values and criticality markings that are required to calculate the total points.

To configure the DPS policies, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > Policies**.



Policy

The name of the DPS policy. This name is used to reference the policy in firewall rules. All of the rows in this table with the same policy name are combined into one policy. This makes it possible, for instance, to use the same metric multiple times with different thresholds in the same policy. This allows a points-based grading (e.g. 10 points with a latency <= 100, another 10 points with a latency <= 50).

Measurement profile

Either empty or the name of an ICMP measurement profile.

! The field must be empty if and only if the **SLA metric** is set to “Load(%)”. In all other cases, a measurement profile must be specified.

SLA metric

This is the metric generated from the measurements of the set measurement profile. The value of metric is compared to the threshold value. Possible values:

- > Latency (ms)
- > Jitter (ms)
- > Packet loss (%)
- > Load (%)

! The metric “Load(%)” denotes the utilization of the interface in percent of the maximum bandwidth. As this value is not determined using separate measurements, the entry **Threshold** must be left empty.

Threshold


Threshold which the chosen SLA metric should not undershot.

Score

If a metric undershoots the chosen threshold, the points are added to the overall result of the policy.

Critical

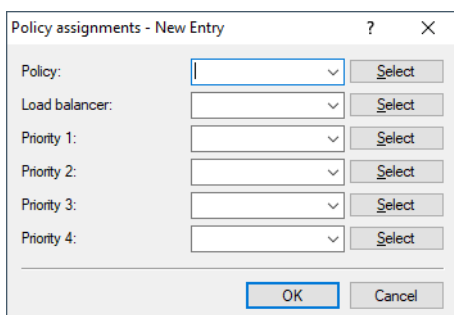
Marks whether a threshold is critical. If a threshold value marked as “critical” is not undershot, the overall result is not defined.

 An interface with an undefined overall result cannot be selected by a dynamic load balancer decision.

Policy-Assignments

Here you set which DPS policy should be used with which load balancer, and what the priorities are if the overall results are equal.

To configure the policy assignments, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > Policy assignments**.




Policy

The name of an existing DPS policy from [Policies](#) on page 8.

Load balancer

Name of a load balancer to be rated by this policy. Measurements are automatically started on all interfaces of this load balancer according to the measurement profiles referenced in the policy.

 Measurements can be suppressed for individual interfaces of this load balancer. See also [Policy exceptions](#) on page 9.

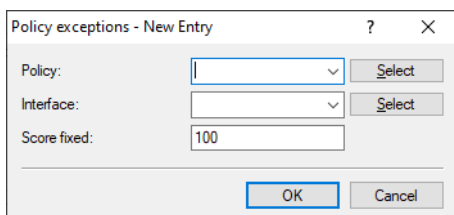
Priority

If several interfaces achieve the same overall policy result during dynamic path selection, the “Priority” values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard “round-robin” strategy.

Policy exceptions

One option is not to apply measurement profiles to certain interfaces, for example if they are charged by data volume.

To configure the policy exceptions, navigate to the view **IP Router > Routing > SD-WAN Dynamic Path Selection > Policy exceptions**.



Policy

The name of an existing DPS policy from [Policies](#) on page 8.

Interface

The name of an interface (e.g. WAN remote sites, VPN tunnels) belonging to a load balancer that is rated by the policy. The measurement profiles referenced in the policy are not used to start measurements on the interface.



Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements must be prevented by making an exception for this interface in all of the affected policies.

Score fixed

Since no dynamic overall result can be derived without making measurements, this score for the interface is used for all decisions relating to dynamic path selection.

2.1.2 Show commands

- > `DPS-v4-Policies <policy> <peer>`: Displays information about the IPv4 policies used by dynamic path selection for the corresponding policy and remote site.
- > `DPS-v4-Score <policy> <load-balancer>`: Shows information about the score for dynamic path selection over IPv4 for the corresponding policy and load balancer.
- > `DPS-v4-Score-Details <policy> <peer>`: Shows detailed information about the IPv4 dynamic path selection score for the corresponding policy and remote site.
- > Extension to the ping command:
`ping -l <policy>`: Uses the specified dynamic path selection load balancer policy to determine the outgoing interface.

2.1.3 Sample configurations**Scenario with two VPN tunnels over two different Internet connections from the branch office to the headquarters**

In this example, dynamic path selection should be set up for all data traffic in a scenario with two VPN tunnels over two different Internet connections from the branch office to the headquarters. The IP address for testing the line quality with ICMP test packets is the private IP address of the central-site gateway, 10.8.0.3. The goal is that only the best line or VPN tunnel should be selected according to the latency.

Dynamic path selection is activated at the branch office only. We are assuming that both of the Internet connections are available and that the two VPN tunnels VPN_A and VPN_B are already configured as a load balancer with the name VPN_LB:

Load balancing - Edit Entry

Name:

Use Client binding

Remote site-1:

Remote site-2:

IPv4 masquerading:

1. Add a new table row under **IP Router > Routing > SD-WAN Dynamic Path Selection > ICMP measurement profiles**.

The first step is to create a new measurement profile. The IPv4 destination is the private IP address of the central gateway, 10.8.0.3. Measurement packets used to evaluate the paths are sent over the VPN tunnels (SD-WAN overlays) every 5 seconds.

2. Add a new table row under **IP Router > Routing > SD-WAN Dynamic Path Selection > Policies**.

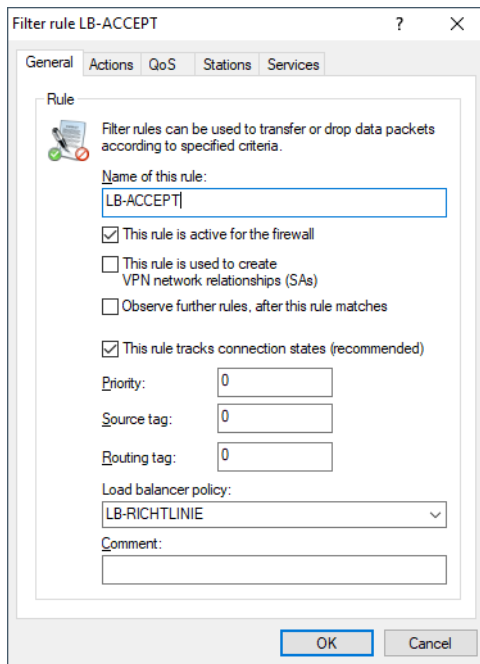
The next step is to create a new policy with an SLA metric "Latency" set with a threshold of 50 ms. If the corresponding VPN tunnel has a latency of less than 50 ms, the path is given a score of 100 (points). A connection that does not meet this criterion receives a score of 0, i.e. it is rated as worse. The path with the highest score is the preferred path and is therefore used for the data traffic. If both paths have an identical score of 100, load balancing is performed with both of the VPN tunnels.

3. Add a new table row under **IP Router > Routing > SD-WAN Dynamic Path Selection > Policy assignments**.

In the following, the newly created policy is linked to the VPN load balancer cluster VPN_LB. The priority fields can be left blank.

4. Add a new table row under **Firewall/QoS > IPv4 rules > Rules**.

Create a new firewall rule that accepts all traffic and that has the value "LB-RICHTLINIE" as the load balancer policy.



2.1.4 Additions to the Setup menu

Dynamic-Path-Selection

Used in an SD-WAN scenario where several lines are available, Dynamic Path Selection optimizes the application performance by directing the data traffic over the line with the best quality according to metrics such as load, packet loss, latency or jitter.

Dynamic Path Selection is activated on a load balancer (see [2.8.10.2.16 LB-Policy](#) on page 23). A load balancer can be defined either for Internet connections or for SD-WAN overlay tunnels (VPN). The end point for ICMP test packets can either be any IP address or the central-site SD-WAN gateway.

SNMP ID:

2.110.4

Console path:

Setup > Firewall

ICMP-Measurement-Profiles

ICMP measurement profiles specify a parameter set used by measurements that are based on ICMP pings. Interface metrics are derived from measurements to quantify the connection quality. These metrics are: Average round trip time (RTT, latency), jitter and packet loss rate.

SNMP ID:

2.110.4.1

Console path:

Setup > Firewall > Dynamic-Path-Selection

Measurement-Profile

The name of the profile. This name is used to reference the profile in DPS policies.

SNMP ID:

2.110.4.1.1

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

DSCP-value

Sets the DSCP value in the IP header of measurement packets. DSCP (Differentiated Services Code Point) is used for QoS (Quality of Service).

SNMP ID:

2.110.4.1.2

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

BE
CS0
CS1
CS2
CS3
CS4
CS5
CS6
CS7
AF11
AF12
AF13
AF21
AF22
AF23
AF31
AF32
AF33
AF41
AF42
AF43
EF

Loopback-Addr.

Optionally references a named loopback address used as the sender in the measurement packets. If the field is left empty, the router automatically selects an address that matches the sending interface.

SNMP ID:

2.110.4.1.3

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

IPv4-Destination-1

The first of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With "0.0.0.0" entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.4

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

Payload-Size

Specifies the size of the data payload that follows the ICMP header (payload size) of the pings being sent.

SNMP ID:

2.110.4.1.6

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

Interval

The interval in seconds between 2 measurements. The maximum round trip time is also specified. Packets not answered within a measurement interval are counted as packet loss.

SNMP ID:

2.110.4.1.7

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

Sliding-Window

Maximum number of measurement values that are used to determine the interface metrics. If a measurement value is received after the number specified here has been reached, the oldest measurement is discarded.

SNMP ID:

2.110.4.1.8

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

Max. 5 characters from [0-9]

IPv4-Destination-2

The second of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With "0.0.0.0" entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.9

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

IPv4-Destination-3

The third of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With "0.0.0.0" entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.10

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

IPv4-Destination-4

The first of up to four measurement destinations as a valid IPv4 unicast address or DNS hostname. With "0.0.0.0" entered, the measurement destination is determined dynamically by the VPN. If the field is left empty, no measurements are made for this family of addresses.

SNMP ID:

2.110.4.1.11

Console path:

Setup > Firewall > Dynamic-Path-Selection > ICMP-Measurement-Profiles

Possible values:

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

Policies

To evaluate the connection quality of the interfaces used for Dynamic Path Selection, the metrics calculated from the measurement profiles are compared to threshold values, and points (as a score) are awarded. These points added up to determine which is the "best" interface. Certain thresholds can be specified as being "critical" (e.g. jitter \leq 30 ms). Dynamic load balancer decisions are based on the points total in combination with the exceeded critical threshold values. A DPS policy collects the threshold values and criticality markings that are required to calculate the total points.

SNMP ID:

2.110.4.16

Console path:

Setup > Firewall > Dynamic-Path-Selection

Policy

The name of the DPS policy. This name is used to reference the policy in firewall rules. All of the rows in this table with the same policy name are combined into one policy. This makes it possible, for instance, to use the same metric multiple times with different thresholds in the same policy. This allows a points-based grading (e.g. 10 points with a latency \leq 100, another 10 points with a latency \leq 50).

SNMP ID:

2.110.4.16.1

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:

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

Measurement-Profile

Either empty or the name of an ICMP measurement profile.



The field must be empty if, and only if, the SLA metric "Load(%)" is selected. In all other cases, a measurement profile must be specified.

SNMP ID:

2.110.4.16.2

Console path:


Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:

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

SLA-Metric

This is the metric generated from the measurements of the set measurement profile. The value of metric is compared to the threshold value.

 The metric "Load(%)" denotes the utilization of the interface in percent of the maximum bandwidth. As this value is not determined using separate measurements, the entry [2.110.4.16.2 Measurement-Profile](#) on page 17 must be left empty.

SNMP ID:

2.110.4.16.3

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:

Latency (ms)
Jitter (ms)
Packet loss (%)
Load (%)

Threshold

Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements need to be prevented by making an an exception for this interface in all of the affected policies.

SNMP ID:

2.110.4.16.4

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:

Max. 10 characters from `[0-9]`

Value

If a metric undershoots the chosen threshold, the points are added to the overall result of the policy.

SNMP ID:

2.110.4.16.5

Console path:


Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:

Max. 5 characters from [0-9]

Critical

Marks whether a threshold is critical. If a threshold value marked as “critical” is not undershot, the overall result is not defined.

 An interface with an undefined overall result cannot be selected by a dynamic load balancer decision.

SNMP ID:

2.110.4.16.6

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policies

Possible values:**No**

Threshold is not marked as critical.

Yes

Threshold is marked as critical.

Policy-Assignments

Here you set which DPS policy should be used with which load balancer, and what the priorities are if the overall results are equal.

SNMP ID:

2.110.4.17

Console path:

Setup > Firewall > Dynamic-Path-Selection

Policy

The name of an existing DPS policy from [2.110.4.16.1 Policy](#) on page 17.

SNMP ID:

2.110.4.17.1

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments

Possible values:

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

Load-Balancer

Name of a load balancer to be rated by this policy. Measurements are automatically started on all interfaces of this load balancer according to the measurement profiles referenced in the policy.



Measurements can be suppressed for individual interfaces of this load balancer. See also [2.110.4.18 Policy-Assignment-Exceptions](#) on page 21.

SNMP ID:

2.110.4.17.2

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments

Possible values:

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

Priority-1

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

SNMP ID:

2.110.4.17.3

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments

Possible values:

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

Priority-2

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

SNMP ID:

2.110.4.17.4

Console path:**Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Priority-3**

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

SNMP ID:

2.110.4.17.5

Console path:**Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Priority-4**

If several interfaces achieve the same overall policy result during dynamic path selection, the "Priority" values determine which interface is actually selected (1 – highest priority, 4 – lowest priority). If the fields are left empty, then load balancing follows the standard "round-robin" strategy.

SNMP ID:

2.110.4.17.6

Console path:**Setup > Firewall > Dynamic-Path-Selection > Policy-Assignments****Possible values:**Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`**Policy-Assignment-Exceptions**

One option is not to apply measurement profiles to certain interfaces, for example if they are charged by data volume.

SNMP ID:

2.110.4.18

Console path:**Setup > Firewall > Dynamic-Path-Selection**

Policy

The name of an existing DPS policy from [2.110.4.16.1 Policy](#) on page 17.

SNMP ID:

2.110.4.18.1

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignment-Exceptions

Possible values:

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

Interface

The name of an interface (e.g. WAN remote sites, VPN tunnels) belonging to a load balancer that is rated by the policy. The measurement profiles referenced in the policy are not used to start measurements on the interface.



Where an interface is used by numerous load balancers, or where multiple policies are used to rate the load balancer that uses this interface, measurements must be prevented by making an exception for this interface in all of the affected policies.

SNMP ID:

2.110.4.18.2

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignment-Exceptions

Possible values:

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

Score-Fixed

Since no dynamic overall result can be derived without making measurements, this score for the interface is used for all decisions relating to dynamic path selection.

SNMP ID:

2.110.4.18.3

Console path:

Setup > Firewall > Dynamic-Path-Selection > Policy-Assignment-Exceptions

Possible values:

Max. 10 characters from `[0-9]`

LB-Policy

Specifies the dynamic path selection policy used for this firewall rule.

SNMP ID:

2.8.10.2.16

Console path:

Setup > IP-Router > Firewall > Rules

Possible values:

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

Default:

empty

3 Virtual Private Networks – VPN

3.1 IKEv2 Auto IP

Using the Auto-IP parameter, a VPN central site can transmit the IP address of the Dynamic Path Selection measurement destination to a VPN branch. For this purpose, the Auto-IP parameter is configured at the central site. At the branch, the measurement destination has to be set (IPv4 " 0.0.0.0" or IPv6 ":::") in order for the branch to automatically take over the measurement destination from the central site.

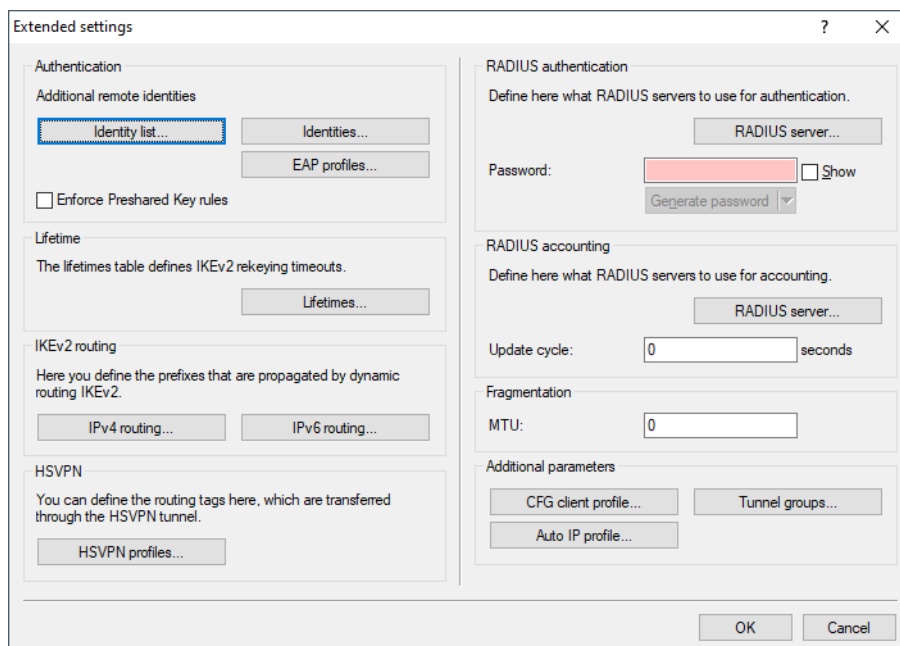
You enter the reference to the Auto-IP profile under **VPN > IKEv2/IPSec > Connection list**.

Auto IP

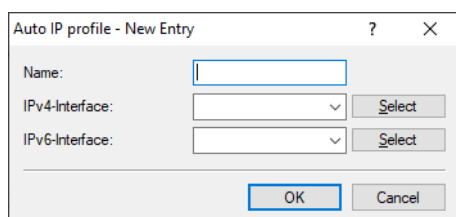
Using the Auto-IP parameter, a VPN central site can transmit the IP address of the *Dynamic Path Selection* measurement destination to a VPN branch. For this purpose, the Auto-IP parameter is configured at the central site. At the branch, the measurement destination has to be set (IPv4 as 0.0.0.0 or IPv6 as ::) in order for the branch to automatically take over the measurement destination from the central site.

Refers to the relevant Auto-IP profile, which you set up under *IKEv2-Auto-IP-Profile* on page 25.

In LANconfig, navigate to the Auto-IP profile under **VPN > IKEv2/IPSec > Extended settings** and, in the section **Additional parameters**, configure the **Auto IP profile**.



3.1.1 IKEv2-Auto-IP-Profile



Name

Unique name of the Auto-IP profile.

IPv4-Interface

IPv4 network used to send the IPv4 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv4 networks

IPv6-Interface

IPv6 network used to send the IPv6 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv6-LAN-Interfaces

3.1.2 Additions to the Setup menu

Auto-IP-Profile

Using the Auto-IP parameter, a VPN central site can transmit the IP address of the Dynamic Path Selection measurement destination to a VPN branch. For this purpose, the Auto-IP parameter is configured at the central site. At the branch,

the measurement destination has to be set (IPv4 " 0.0.0.0" or IPv6 ":::") in order for the branch to automatically take over the measurement destination from the central site.

Enter a reference to an Auto-IP profile here (see [2.19.36.16 Auto-IP-Profiles](#) on page 26).

SNMP ID:

2.19.36.1.25

Console path:

Setup > VPN > IKEv2 > Peers

Possible values:

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

Auto-IP-Profiles

This table is used to configure the Auto-IP profiles.

SNMP ID:

2.19.36.16

Console path:

Setup > VPN > IKEv2

Name

Here you set a name for the Auto-IP profile. This is referenced under [2.19.36.1.25 Auto-IP-Profile](#) on page 25.

SNMP ID:

2.19.36.16.1

Console path:

Setup > VPN > IKEv2 > Auto-IP-Profiles

Possible values:

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

IPv4-Interface

IPv4 network used to send the IPv4 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv4 networks

SNMP ID:

2.19.36.16.2

Console path:

Setup > VPN > IKEv2 > Auto-IP-Profiles

Possible values:

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

IPv6-Interface

IPv6 network used to send the IPv6 address to the VPN remote site for the dynamic path selection measurement destination.

Possible values: IPv6-LAN-Interfaces

SNMP ID:

2.19.36.16.3

Console path:

Setup > VPN > IKEv2 > Auto-IP-Profiles

Possible values:

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

3.2 IPv6 address range can be controlled for VPN negotiation

As of LCOS 10.42 you can control the IPv6 address range for VPN negotiation from the command line.

3.2.1 Additions to the Setup menu

Auto-IP-Profiles

Defines the IPv6 prefix with which no VPN connections should be established. If, for example, an upstream router only assigns a Unique Local Address (ULA) from the prefix "fc00::/7" to the device, it can be prevented that the device establishes a VPN connection to a global IPv6 address with a send address from this prefix. This can be combined with the alternative gateway list where an IPv4 address is listed as an alternative gateway and then used.

Input value: IPv6 prefix, for example "fc00::/7".

SNMP ID:

2.19.36.34

Console path:

Setup > VPN > IKEv2

Possible values:

Max. 253 characters from `[A-Z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_.`

Default:

empty

4 Wireless LAN – WLAN

4.1 WPA default passphrase deprecated

Until now, the default WPA passphrase for LCOS was preset to "L" and the LAN MAC address. As of LCOS 10.42 this preset WLAN passphrase is deprecated. It is now essential for the user to configure an individual secure passphrase. If no passphrase is configured despite the fact that a passphrase is required for the selected encryption mode (WEP, WPA2/3-PSK), the WLAN will simply not operate. The syslog indicates that no passphrase is set, although one is required.

4.2 RTLS (real-time location system)

RTLS enables a device to be localized in real time. This device is a specialized WLAN transmitter that sends out specially coded WLAN packets. The access points in the vicinity receive these packets and forward them with additional data to the real-time localization system. By enabling the precise determination of the location of the WLAN transmitter, the whereabouts of objects or people carrying the WLAN transmitter can be implied.

As of LCOS 10.42, RTLS now additionally supports the Stanley AeroScout RTLS system in addition to the AiRISTA Flow blink mode (previously Ekahau blink mode), which has been supported for a long time already. All current LANCOM WLAN devices with LCOS 10.42 can be used, except for the LANCOM IAP-1781VAW.

4.2.1 Stanley AeroScout RTLS

The AeroScout RTLS system facilitates various tasks such as asset management, environmental monitoring and staff workflows by means of special sensors connected via WLAN and "tags". This feature enables the AeroScout tags (i.e. specifically coded WLAN packets) to be forwarded to the AeroScout Location Engine via a LANCOM WLAN infrastructure.

The following operating modes are supported:

- Forwarding of AeroScout tag messages



The WDS mode is supported. Make sure that the tags in the AeroScout system are configured for WDS mode.
The IBSS mode is not supported.

- Wi-Fi client reports

Configuring Stanley AeroScout RTLS

To configure access to the Stanley AeroScout RTLS server with LANconfig, open the view **Wireless LAN > General > Extended settings > RTLS** and configure the section **Stanley (AeroScout)**.

Stanley (AeroScout) RTLS operating

Enable this option to activate the forwarding to the AeroScout Location Engine.

! This feature is always activated for all WLAN modules of an access point.

Server address

Configure the IP address of the AeroScout Location Engine here.

Server port

Configure the server port of the AeroScout Location Engine if the default value is not being used.

Source address (optional)

Optionally, configure the source network for the connection to the AeroScout Location Engine. This is only necessary if multiple ARF networks are configured.

Vendor ID

Here you configure the vendor ID that the access point reports to the AeroScout Location Engine. If your version of the AeroScout Location Engine does not yet support the dedicated LANCOM vendor ID, you can switch to the vendor ID "Motorola".

4.2.2 Additions to the Setup menu

RTLS

This menu contains the settings for communications with an RTLS server.

SNMP ID:

2.12.131

Console path:

Setup > WLAN

Ekahau

This menu contains the settings for the AiRISTA Flow blink mode (formerly Ekahau blink mode).

SNMP ID:

2.12.131.4

Console path:

Setup > WLAN > RTLS

Server-Address

Contains the IP address or the DNS name of the RTLS server.

SNMP ID:

2.12.131.4.1

Console path:

Setup > WLAN > RTLS > Ekahau

Possible values:

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

Default:

empty

Server-Port

Contains the UDP port number of the RTLS server.

SNMP ID:

2.12.131.4.2

Console path:

Setup > WLAN > RTLS > Ekahau

Possible values:

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

Default:

8569

Loopback-Address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

SNMP ID:

2.12.131.4.3

Console path:**Setup > WLAN > RTLS > Ekahau****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+,/:;<=>?[\]^_.`**Special values:****Name of the IP networks whose address should be used****"INT"**

for the address of the first intranet

"DMZ"

for the address of the first DMZ

LBO to LBF

for the 16 loopback addresses

Any valid IP address**Default:***empty***AeroScout**

This menu contains the Stanley AeroScout RTLS settings.

SNMP ID:

2.12.131.5

Console path:**Setup > WLAN > RTLS****Server-Address**

Contains the IP address or the DNS name of the RTLS server.

SNMP ID:

2.12.131.5.1

Console path:**Setup > WLAN > RTLS > AeroScout****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+,/:;<=>?[\]^_.`**Default:***empty*

Server-Port

Contains the server port of the AeroScout Location Engine.

SNMP ID:

2.12.131.5.2

Console path:

Setup > WLAN > RTLS > AeroScout

Possible values:

Max. 5 characters from [0-9]

Default:

12092

Loopback-Address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

SNMP ID:

2.12.131.5.3

Console path:

Setup > WLAN > RTLS > AeroScout

Possible values:

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

Special values:**Name of the IP networks whose address should be used**

"INT"

for the address of the first intranet

"DMZ"

for the address of the first DMZ

LBO to LBF

for the 16 loopback addresses

Any valid IP address

Default:

empty

Operating

Enable the forwarding to the Aeroscout Location Engine here.

SNMP ID:

2.12.131.5.4

Console path:**Setup > WLAN > RTLS > AeroScout****Possible values:****Yes**

Forwarding enabled.

No**Default:**

No

Vendor-ID

Here you configure the vendor ID that the access point reports to the AeroScout Location Engine. If your version of the Aeroscout Location Engine does not yet support the dedicated LANCOM vendor ID, you can switch to the "Motorola" vendor ID.

SNMP ID:

2.12.131.5.5

Console path:**Setup > WLAN > RTLS > AeroScout****Possible values:****Motorola****LANCOM****Default:**

LANCOM

4.3 Location-based services (LBS)

LANCOM access points are able to work as LBS clients with an LBS server. In this case, they report any connected clients to the LBS server, which can then offer location-based services to those clients. An HTTP API is supported as of LCOS 10.42, along with a Thrift interface that has been available for some time already.

Using the HTTP interface, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

LANconfig: **Miscellaneous Services > Services > Location Based Services (LBS)**

Location Based Services (LBS)

Location based services (LBS) enabled

LBS engine address:

LBS engine port:

Own position

Description:

Floor: 0-based

Height:

Location based services (LBS) enabled

Enables or disables the location-based services.

Server type

Here you configure whether to use the HTTP interface or the Thrift interface.

4.3.1 HTTP interface

Using the HTTP API, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

HTTP server URL

Configure the URL of the HTTP endpoint here.



HTTP and HTTPS are supported. When using HTTPS, certificate verification may be disabled, based on a server certificate, or performed a both ends by server and client authentication. For this purpose, a PKCS#12 container with CA and client certificate can be uploaded to the device that contains the

CA certificate or the CA and client certificates. This can be performed using LANconfig or WEBconfig. If no PKCS#12 container is uploaded, no certificate verification is carried out when HTTPS is used.

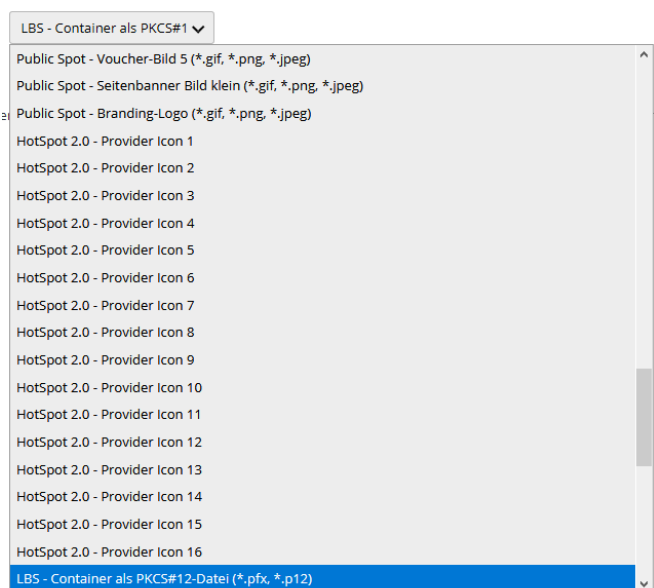


Figure 1: Screenshot WEBconfig

HTTP server secret

The HTTP server secret is transmitted in the JSON messages from the access point to the end point and can be used to additionally authenticate the messages.

HTTP data sources

Here you configure whether to transmit WLAN, BLE, or both types of LBS data.



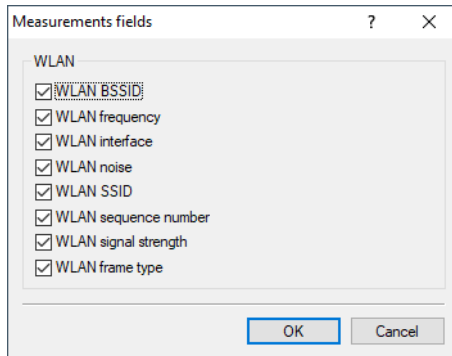
The setting **BLE** is only supported on devices featuring BLE. These are currently the LN-1700B, LN-1702B, LN-1700UE, OAP-1700B and OAP-1702B.

Source address

Use this item to configure which loopback address should be used for communication with the HTTP endpoint. This may be necessary if multiple IP networks are configured on the device.

Measurements fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.



Data format of the messages sent to the endpoint

> For **WLAN**:

```
{
  "version": "1.0",
  "secret": "secret",
  "type": "WLAN",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "clientMac": "334455667788",
      "seenTime": 1579792598996,
      "frameSeqNum": 1074,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -56,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    },
    {
      "clientMac": "554433aabbcc",
      "seenTime": 1579792601334,
      "frameSeqNum": 2742,
      "ssid": "",
      "module": 0,
      "bssid": "00a057000000",
      "rssi": -45,
      "frequency": 2462,
      "noise": -70,
      "frameType": "PROBE"
    }
  ]
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the access point configuration.

type

The type of data sent. Can be either WLAN or BLE.

deviceMac

The LAN MAC address of the access point.

measurements

This contains at least one measured value. This could also be a number of measurements.

clientMac

The MAC address of the WLAN client.

seenTime

The time stamp (in Unix time) when the WLAN frame from the client was received by the access point.

frameSeqNum

The sequence number of the received WLAN frame.

ssid

The SSID contained in the WLAN frame, if available.

module

Describes the access-point WLAN interface that the WLAN frame was received from. Typically 0 for the first WLAN interface or 2 for the second WLAN interface.

bssid

The BSSID contained in the WLAN frame.

rssi

The signal strength in dBm of the received WLAN frame.

frequency

The frequency in MHz of the WLAN channel that the WLAN frame was received on.

noise

The noise level in dBm on the channel that the WLAN frame was received on.

frameType

The frame type of the received WLAN frame. The following types are available: PROBE, AUTHENTICATION, ASSOCIATION, DEAUTHENTICATION or DEASSOCIATION.

> For BLE:

```
{
  "version": "1.0",
  "secret": "secret",
  "type": "BLE",
  "deviceMac": "00a057000000",
  "measurements": [
    {
      "deviceAddress": "001122334455",
      "seenTime": 1579792601269,
      "addressType": "Random",
      "rssi": -77
    },
    {
      "deviceAddress": "ffeaddccbbaa",
      "seenTime": 1579792601273,
      "addressType": "Random",
      "rssi": -61
    },
    {
      "name": "test",
      "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
      "scanResponseData": "050974657374"
    }
  ]
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the AP configuration.

type

The type of data sent. Can be either `WLAN` or `BLE`.

deviceMac

The LAN MAC address of the AP.

measurements

This contains at least one measured value. This could also be a number of measurements.

deviceAddress

The address of the BLE device or client.

seenTime

The time stamp (in Unix time) when the BLE frame from the client was received by the AP.

addressType

The type of BLE address. The following address types are available: `Public` or `Random`.

rsi

The signal strength in dBm of the received BLE frame.

name

The name submitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

advertisingData

The complete advertisement transmitted by the BLE device.

scanResponseData

The complete scan response transmitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

4.3.2 Additions to the Setup menu

LBS-Server-Type

Here you configure whether the HTTP API uses JSON-format data packets or the Thrift API.

SNMP ID:

2.100.17

Console path:

Setup > LBS

Possible values:

Apache-Thrift
HTTP-JSON

HTTP-Server

This item determines the settings of the HTTP server when using the HTTP API.

SNMP ID:


2.100.18

Console path:

Setup > LBS

URL

Configure the URL of the HTTP endpoint here.

 HTTP and HTTPS are supported. If you use HTTPS, a PKCS#12 container with CA and client certificate must also be uploaded to the device. This can be done using LANconfig or WEBconfig.

SNMP ID:

2.100.18.1

Console path:

Setup > LBS > HTTP-Server

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-./:;<=>?[\]^_``

Loopback address

Use this item to configure which loopback address should be used for communication with the HTTP endpoint. This may be necessary if multiple IP networks are configured on the device.

SNMP ID:

2.100.18.2

Console path:

Setup > LBS > HTTP-Server

Possible values:

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

Secret

The HTTP server secret is transmitted in the JSON messages from the access point to the end point and can be used to additionally authenticate the messages.

SNMP ID:

2.100.18.3

Console path:**Setup > LBS > HTTP-Server****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()*+,-./:;<=>?[\]^_``**Data-Sources**

Here you configure whether to transmit WLAN, BLE, or both types of LBS data.



The setting **BLE** is only supported on devices featuring BLE.

SNMP ID:

2.100.18.4

Console path:**Setup > LBS > HTTP-Server****Possible values:****WLAN****BLE**

5 WLAN management

5.1 Configuring Passpoint® Release 2 via the WLAN controller

As of LCOS 10.42, a WLAN controller can now also be used to configure the Passpoint® Release 2 that was introduced with LCOS 10.32 RU4.

The settings for this can be found in LANconfig under **WLAN Controller > 802.11u > Hotspot 2.0 profiles** or under **WLAN Controller > 802.11u > OSU providers**.


The configuration corresponds to the feature described under **Wireless LAN > 802.11u > Hotspot 2.0**.

 The distribution of files such as the icons for the OSU provider is not yet automated. These have to be uploaded individually to each access point.

5.1.1 Additions to the Setup menu

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:

2.37.1.17.3.5

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.3.6

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.3.7

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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 [2.37.1.17.12 OSU-Providers](#) on page 42 that are supported in the profile.

SNMP ID:

2.37.1.17.3.8

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12

Console path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u****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:

2.37.1.17.12.1

Console path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.2

Console path:**Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.3

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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](#). Options are "OMA-DM" or "SOAP-XML-SPP".

SNMP ID:

2.37.1.17.12.4

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.5

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.6

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.7

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > OSU-Providers

Possible values:

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

Icon-Filename

Select 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:

2.37.1.17.12.8

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > 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:

2.37.1.17.12.9

Console path:

Setup > WLAN-Management > AP-Configuration > IEEE802.11u > OSU-Providers

Possible values:

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

5.2 Extension of the Wireless ePaper profiles

As of LCOS 10.42, a WLAN controller can now also be used to set the extension of the TCP protocol introduced with LCOS 10.40 that enables TLS-encrypted connections between the Wireless ePaper Server and Wireless ePaper access points or routers with a USB interface and a Wireless ePaper USB Stick.

The settings for this can be found in LANconfig under **WLAN Controller > Profiles > Advanced Profiles > Wireless ePaper profiles**

5.2.1 Additions to the Setup menu

Outbound-Server

IP address of the Wireless ePaper Server.

SNMP ID:

2.37.1.23.4

Console path:

Setup > WLAN-Management > AP-Configuration > Wireless-ePaper-Profile

Possible values:

Max. 128 characters from [A-Z] [a-z] [0-9] . - : %

Loopback-Address

Enter loopback address here.

SNMP ID:

2.37.1.23.5

Console path:

Setup > WLAN-Management > AP-Configuration > Wireless-ePaper-Profile

Possible values:

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

Default:

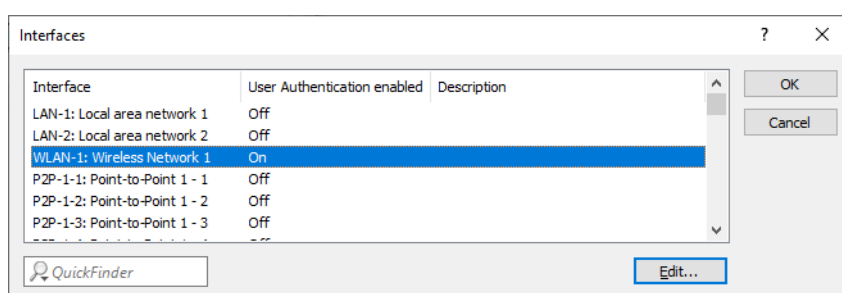
empty

6 Public Spot

6.1 Extension of the Public Spot port table for the LANCOM Management Cloud

As of LCOS 10.42, a new field **Description** in the port table can either be used to enter an individual description or it can be used by the LANCOM Management Cloud for the cloud-managed hotspot feature.

The port table in LANconfig is located under **Public Spot > Server > Operational Settings > Interfaces**



6.1.1 Additions to the Setup menu

Description

Field for a description of the port. This field is also used for the cloud-managed hotspot feature of the LANCOM Management Cloud to uniquely identify the hotspot. In this case, the LANCOM Management Cloud stores a UUID here.

SNMP ID:

2.24.15.4

Console path:

Setup > Public-Spot-Module > Port-Table

Possible values:

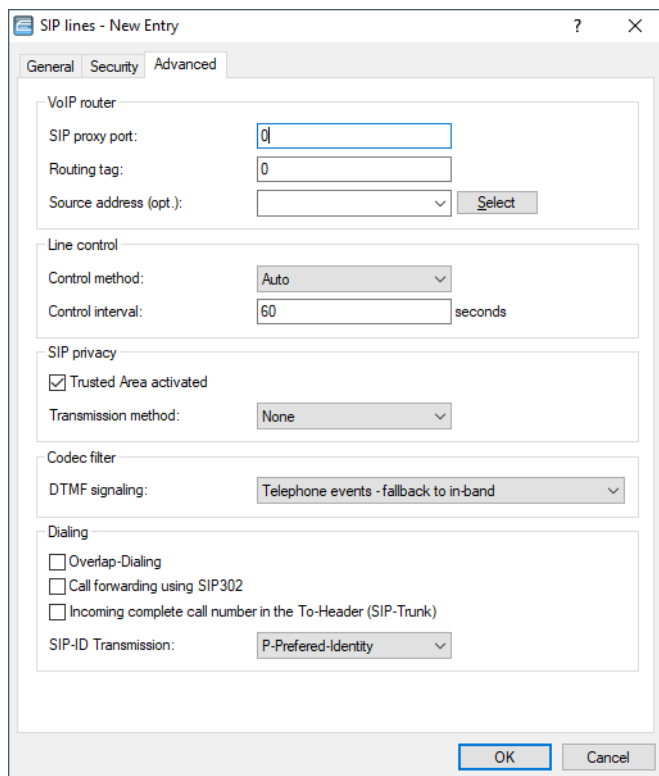
Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]^_``

7 Voice over IP – VoIP

7.1 Source address for SIP and SIP PBX lines

As of LCOS 10.42, the optional source address, which specifies the interface for each SIP line created, can also be set via LANconfig. This simplifies operation and simplifies error analysis for support.

You can find the option for SIP lines under **Voice Call Manager > Lines > SIP lines > Advanced**.



Source address

The device automatically determines the correct source IP address for the destination network. If you want to use a fixed source IP address instead, enter it symbolically or directly here.

You can find the option for SIP PBX lines under **Voice Call Manager > Lines > SIP PBX lines > General**.

Source address

The device automatically determines the correct source IP address for the destination network. If you want to use a fixed source IP address instead, enter it symbolically or directly here.

7.2 SIP-ID transmission

LCOS 10.42 comes with additional options for the **SIP-ID transmission** under **Voice Call Manager > Lines > SIP lines > Advanced**.

SIP-ID transmission

The field SIP-ID transmission sets the way in which the SIP ID is transmitted for outgoing calls when operating a SIP trunk. Depending on the provider, it may be necessary to transmit the SIP ID via a different field, as otherwise the call might be rejected by the provider.

The following values can be selected:

- > P-Asserted-Identity (default value)
- > FROM
- > None
- > P-Preferred-Identity without DDI
- > P-Preferred-Identity
- > None – P-Preferred-Identity

➤ None – P-Asserted-Identity

Selecting the option **P-Asserted Identity** (PAI) transmits the SIP ID inclusive DDI with the PAI. The source telephone number is transmitted via the FROM field.

Selecting the option **P-Preferred Identity** (PPI) transmits the SIP ID inclusive DDI with the PPI. The source telephone number is transmitted via the FROM field.

Selecting the option **FROM** transmits the SIP ID with the FROM field. The source telephone number is transmitted via the PPI / PAI.

With the setting **None**, the SIP ID is not transmitted. The first calling number is transmitted via the FROM field, the second number is transmitted via PPI / PAI.

In contrast to the P-Preferred-Identity, the setting **P-Preferred-Identity without DDI** does not transmit an extension number (DDI) in the SIP ID via the PPI field.

Selecting the option **None – P-Preferred-Identity**, the SIP ID is not transmitted. The first calling number is transmitted in the FROM field, the second number in the PPI field.

Selecting the option **None – P-Asserted-Identity**, the SIP ID is not transmitted. The first calling number is transmitted in the FROM field, the second number in the PAI field.



With a single account, outgoing calls always signal the SIP ID in the **FROM** field.

7.2.1 Additions to the Setup menu

User-Id-Field

Specifies the field used to transmit the SIP ID.



With a single account, outgoing calls always signal the SIP ID in the FROM field.

SNMP ID:

2.33.4.1.1.39

Console path:

Setup > Voice-Call-Manager > Lines > SIP-Provider > Line

Possible values:

PPI

The SIP ID including the DDI is transmitted via the PAI. The source telephone number is transmitted via the FROM field.

From

The SIP ID is transmitted via the FROM field. The source telephone number is transmitted via the PPI / PAI field.

None

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI / PAI.

PPI-woDDI

In contrast to the P-Preferred-Identity, an extension number (DDI) is not transmitted in the SIP ID via the PPI.

PPI-PPI

The SIP ID including the DDI is transmitted via the PPI. The source telephone number is transmitted via the FROM field.

None-PPI

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PPI.

None-PAI

The SIP ID is not transmitted. The first calling number is transmitted with FROM, the second in the PAI.

Default:

PPI

8 IoT – the Internet of Things

8.1 Wireless ePaper

As of LCOS 10.42 RU2, you can set the port over which, depending on the direction of the connection setup, either the Wireless ePaper device is reached by the Wireless ePaper Server or, when using the TLS protocol, the Wireless ePaper device addresses the Wireless ePaper Server by itself.

8.1.1 Settings for Wireless ePaper

Activate the Wireless ePaper radio module in LANconfig under **IoT > Wireless ePaper**,

Radio module operation mode:

Wireless ePaper Server

Address:

Port:

Source address (optional):

Channel selection

Channel:

Depending on the used Wireless ePaper radio channel, the connection to the server may take up to 30 minutes (applies for channels 3, 5, 8, 9, 10) and up to 120 minutes (applies for channels 0, 1, 2, 4, 6, 7).

Using coordinated Wireless ePaper channel selection access points in local area networks automatically select the optimal channel for Wireless ePaper communications avoiding the multiple use of channels.

Coordinated Wireless ePaper channel selection enabled

Network name:

Wireless ePaper Server

Port

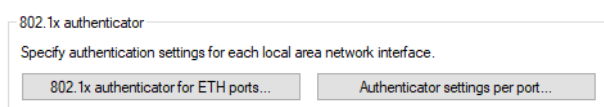
Here you set the port for communication between the Wireless ePaper device, e.g. access point or router, and the Wireless ePaper Server. The default port is 7353 for establishing a connection from the Wireless ePaper Server to the Wireless ePaper device. If the connection from the Wireless ePaper device to the Wireless ePaper Server is to be established using TLS, set the port to 7354.

9 Other services

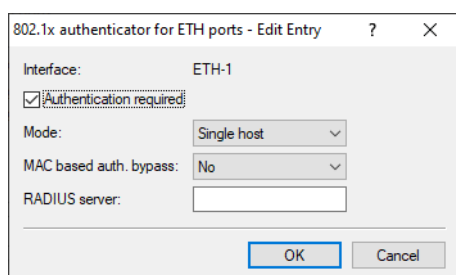
9.1 802.1X authenticator for Ethernet ports

Using the 802.1X authenticator, devices connected to the Ethernet ports of a LANCOM device can be authenticated using 802.1X. This increases security against unauthorized access to the network via Ethernet cables and ports.

In LANconfig you configure the 802.1X authenticator for Ethernet ports under **Interfaces > LAN** in the section **802.1x authenticator**.



You perform the configuration in the table **802.1x authenticator for ETH ports**. Each interface is specified here and indicates the existing Ethernet ports.



Authentication required

Use this control to specify whether 802.1X authentication is required for this port.

Mode

Possible values:

Single host

Just one client can authenticate and then operate on this port. If a further client with its own MAC address is detected on this port, the port is reset to the unauthenticated state.

Multiple hosts

Several clients (with different MAC addresses) can operate on this port. Authentication only needs to be performed once. This mode can be used, for example, if a WLAN access point is operated on a port configured in this way and the payload data is not tunneled to a central controller. In this case, data packets from WLAN clients that have their own MAC addresses would also be seen on the Ethernet port configured in this way.


Multiple authentications


Several clients can each perform their own 802.1X authentication on this port.

MAC-based auth. bypass

This specifies whether a failed attempt to start an 802.1X negotiation should be followed by a check of the client's MAC address via RADIUS and a subsequent opening of the port. In this case, the MAC address is

transmitted as a RADIUS user name and password in the format "aabbccddeeff". It must also be stored in the RADIUS server in this format.

 The MAC address is easy to fake and does not protect against malicious attacks.

 In the standard configuration, the 802.1X authenticator will try to start an 802.1X negotiation for 90 seconds before falling back to the MAC address check. This time can be set for each port by changing the command-line parameters **Setup > IEEE802.1X > Ports > Max Req** (default: 3 attempts) and **Setup > IEEE802.1X > Ports > Supp-Timeout** (default: 30 seconds). Alternatively, the mode for **MAC Auth Bypass** can be set to "Immediate". This mode immediately starts a MAC address check without waiting for a timeout.

Possible values:

No

MAC address authentication is not possible.

Yes

MAC address authentication is possible.

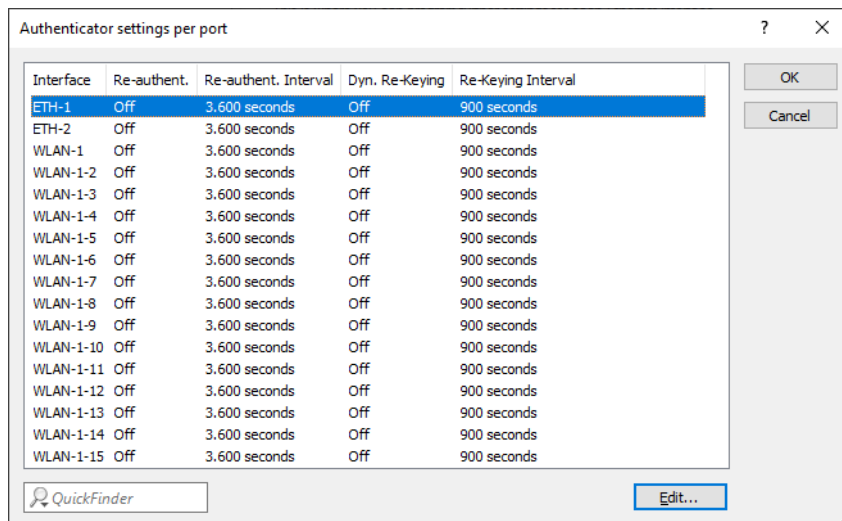
Immediately

Authentication is immediately performed by MAC address.

RADIUS server

Specifies which RADIUS server is used both for 802.1X and for MAC address validation. To do this, reference one of the entries under **Wireless-LAN > 802.1X > Radius servers** or create a new entry there if necessary.

In the table **Authenticator settings per port** you set the login information for the local network interfaces.



Interface	Re-authent.	Re-authent. Interval	Dyn. Re-Keying	Re-Keying Interval
ETH-1	Off	3.600 seconds	Off	900 seconds
ETH-2	Off	3.600 seconds	Off	900 seconds
WLAN-1	Off	3.600 seconds	Off	900 seconds
WLAN-1-2	Off	3.600 seconds	Off	900 seconds
WLAN-1-3	Off	3.600 seconds	Off	900 seconds
WLAN-1-4	Off	3.600 seconds	Off	900 seconds
WLAN-1-5	Off	3.600 seconds	Off	900 seconds
WLAN-1-6	Off	3.600 seconds	Off	900 seconds
WLAN-1-7	Off	3.600 seconds	Off	900 seconds
WLAN-1-8	Off	3.600 seconds	Off	900 seconds
WLAN-1-9	Off	3.600 seconds	Off	900 seconds
WLAN-1-10	Off	3.600 seconds	Off	900 seconds
WLAN-1-11	Off	3.600 seconds	Off	900 seconds
WLAN-1-12	Off	3.600 seconds	Off	900 seconds
WLAN-1-13	Off	3.600 seconds	Off	900 seconds
WLAN-1-14	Off	3.600 seconds	Off	900 seconds
WLAN-1-15	Off	3.600 seconds	Off	900 seconds

Interface

Each interface is specified here and indicates the available Ethernet and WLAN interfaces.

Re-authentication required

Here you activate regular re-authentication. If a new authentication starts, the user remains registered during the negotiation.

Re-authentication interval

The default value for re-authentication interval for regular re-authentication is 3,600 seconds.

Enable dynamic re-keying

Here you activate the regular generation and transmission of a dynamic WEP key.

Re-keying interval

The default value for the re-keying interval is 900 seconds.

9.1.1 Additions to the Setup menu

Authenticator-lfc-Setup

This menu contains the settings for the RADIUS authentication (802.1X authentication) of clients connecting to the device via the LAN interfaces.

SNMP ID:

2.4.10.3

Console path:

Setup > LAN > IEEE802.1X

lfc

Name of the port.

SNMP ID:

2.4.10.3.1

Console path:

Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup

Operating

Use this parameter to specify whether 802.1X authentication is required for this port.

SNMP ID:

2.4.10.3.2

Console path:

Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup

Possible values:

No
Yes

Default:

No

Mode

This item sets whether one or more clients may login at this interface via IEEE 802.1X.

SNMP ID:

2.4.10.3.3

Console path:

Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup

Possible values:**Single host**

Just one client can authenticate and then operate on this port. If a further client with its own MAC address is detected on this port, the port is reset to the unauthenticated state.

Multiple host

Several clients (with different MAC addresses) can operate on this port. Authentication only needs to be performed once. This mode can be used, for example, if a WLAN access point is operated on a port configured in this way and the payload data is not tunneled to a central controller. In this case, data packets from WLAN clients that have their own MAC addresses would also be seen on the Ethernet port configured in this way.

Multiple auth

Several clients can each perform their own 802.1X authentication on this port.

Default:

Single host

RADIUS-Server

Specifies which RADIUS server is used both for 802.1X and for MAC address validation. To do this, reference one of the entries under [2.30.3 RADIUS server](#) or create a new entry there if necessary. You can adjust the format of the transmitted MAC address under [2.4.10.4 Username-Attribute-Format](#) on page 59.

SNMP ID:

2.4.10.3.4

Console path:

Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup


Possible values:


Name from **Setup > IEEE802.1X > RADIUS-Server**

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

MAC-Auth.-Bypass

This specifies whether a failed attempt to start an 802.1X negotiation should be followed by a check of the client's MAC address via RADIUS and a subsequent opening of the port. In this case, the MAC address is transmitted as a RADIUS user name and password in the format "aabbccddeeff". It must also be stored in the RADIUS server in this format.

 The MAC address is easy to fake and does not protect against malicious attacks.

 In the standard configuration, the 802.1X authenticator will try to start an 802.1X negotiation for 90 seconds before falling back to the MAC address check. This time can be adjusted for each port by changing the parameters [2.30.4.5 Max-Req](#) (default: 3 attempts) and [2.30.4.7 Supp-Timeout](#) (default: 30 seconds). Alternatively, the mode for MAC Auth Bypass can be set to "Immediate". This mode immediately starts a MAC address check without waiting for a timeout.

SNMP ID:

2.4.10.3.5

Console path:

Setup > LAN > IEEE802.1X > Authenticator-lfc-Setup

Possible values:

No

MAC address authentication is not possible.

Yes

MAC address authentication is possible.

Immediate

Authentication is immediately performed by MAC address.

Default:

No

Username-Attribute-Format

The format of the MAC address that is transmitted to the RADIUS server during MAC authentication can be configured here.

The individual bytes of the MAC address are represented here as variables %a to %f. In the default setting specified here, the bytes of the MAC address are output one after the other. In addition to these variables, any characters supported by LCOS can be added. A frequently used, additional format for the MAC address "aabbcc-ddeeff" (with "-" as separator) could be configured as follows "%a%b%c-%d%e%f"

SNMP ID:

2.4.10.4

Console path:

Setup > LAN > IEEE802.1X

Possible values:

Max. 30 characters from `# [A-Z] [a-z] [0-9] @ { | } ~ ! $ % & ' () * + - , / : ; < = > ? [\] ^ _ . ``

9 Other services

Default:

%a%b%c%d%e%f

10 Enhancements in the menu system

10.1 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.28

Console path:

Setup > WAN > RADIUS

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.2 L2TP-Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.2.22.29

Console path:

Setup > WAN > RADIUS

Possible values:

No

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.3 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.11.81.1.10

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

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.4 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.21

Console path:**Setup > WLAN > RADIUS-Access-Check****Possible values:****No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.5 Backup-Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.12.29.22

Console path:

Setup > WLAN > RADIUS-Access-Check

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.6 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.19.36.9.1.1.11

Console path:

Setup > VPN > IKEv2 > RADIUS > Authorization > Server

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.7 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.2.6

Console path:

Setup > RADIUS > Server > Clients

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Proxy-Only

If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No

10.8 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.3.18

Console path:

Setup > RADIUS > Server > Forward-Servers

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Default:

No

10.9 Require-Msg-Authenticator

New switch as of LCOS 10.42 SU14. Defines whether the presence of the message authenticator attribute in RADIUS messages is enforced on the client side. The client side is the side that receives the RADIUS accept/fail.

SNMP ID:

2.25.10.16.6

Console path:

Setup > RADIUS > Server > IPv6-Clients

Possible values:**No**

Access requests do not have to contain a message authenticator.

Yes

Access requests must always contain a message authenticator.

Proxy-Only

If an access request contains a proxy state attribute, a message authenticator must be included.

Default:

No