

■ connecting your business



Addendum

LCOS 9.18 RU1

Contents

1 Addendum to LCOS version 9.18 RU1.....	4
2 Configuration.....	5
2.1 Preventing password form fields in the browser from storing passwords.....	5
2.1.1 Preventing password form fields in the browser from storing passwords.....	5
2.1.2 Additions to the Setup menu.....	5
2.2 DHCP client with vendor DHCP option for LSR rollouts.....	5
2.2.1 Receiving LSR information via DHCP server.....	6
2.2.2 Additions to the Setup menu.....	8
3 WLAN.....	14
3.1 Adaptive RF Optimization.....	14
3.1.1 Setting up Adaptive RF Optimization with LANconfig.....	14
3.1.2 Additions to the Setup menu.....	16
3.2 Airtime Fairness.....	19
3.2.1 Setting up Airtime Fairness with LANconfig.....	20
3.2.2 Additions to the Setup menu.....	21
3.3 Encrypted OKC via IAPP.....	21
3.3.1 Encrypted OKC via IAPP.....	21
3.3.2 Additions to the Setup menu.....	22
3.4 Fast roaming.....	23
3.4.1 Fast roaming with IAPP.....	23
3.4.2 Additions to the Setup menu.....	23
3.5 Wireless Intrusion Detection System (WIDS).....	24
3.5.1 Setting up the Wireless Intrusion Detection System with LANconfig.....	24
3.5.2 Additions to the Setup menu.....	26
3.6 Status counters for failed WPA-PSK/IEEE 802.1X login attempts.....	46
3.6.1 Status counters for WPA-PSK login attempts.....	46
3.6.2 Status counters for IEEE 802.1X login attempts.....	46
3.6.3 Additions to the Status menu.....	47
3.7 Adaptive Transmission Power.....	49
3.7.1 Configuring Adaptive Transmission Power with LANconfig.....	49
3.7.2 Additions to the Setup menu.....	50
3.8 Improved start-up conditions for WLAN RADIUS accounting.....	51
3.8.1 Configuring start-up conditions for RADIUS accounting with LANconfig.....	52
3.8.2 Configuring start-up conditions for RADIUS accounting with WEBconfig.....	52
3.9 Selecting a RADIUS server profile for 802.1X authentication.....	53
3.9.1 Additions to the Setup menu.....	53
3.10 Configurable data rates per WLAN module.....	53
3.10.1 Configurable data rates per WLAN module.....	54
3.10.2 Additions to the Setup menu.....	56
4 WLAN management.....	86

4.1 Automatically switch off IAPP if a CAPWAP tunnel exists.....	86
5 LANCOM Location Based Services (LBS).....	87
5.1 Dynamic and persistent tracking lists for WLAN clients.....	87
5.1.1 Using the LBS tracking lists of Public Spot users.....	88
5.1.2 Additions to the Setup menu.....	89
6 RADIUS.....	91
6.1 User-definable attributes in the RADIUS client.....	91
6.2 Automatic clean-up of access information on the RADIUS server.....	92
6.2.1 Additions to the Setup menu.....	92
6.3 Vendor-specific RADIUS attribute "LCS-Routing-Tag".....	93
7 Public Spot.....	94
7.1 Shorter units for absolute expiry.....	94
7.1.1 Configuring shorter units with LANconfig.....	94
7.2 Circuit ID as a Public Spot URL-redirect variable.....	94
7.2.1 Using the URL redirect variable.....	94
7.3 Create Public Spot user on a remote Public Spot Gateway.....	94
7.3.1 Create Public Spot user on a remote Public Spot Gateway.....	95
7.3.2 Additions to the Setup menu.....	95
7.4 PMS template: Accept GTC.....	96
7.5 Hiding fields in the setup wizard "Manage Public Spot Account".....	96
7.5.1 Hiding fields in WEBconfig.....	96
7.6 Redirect for HTTPS connections switchable.....	104
7.6.1 Redirect for HTTPS connections.....	104
7.6.2 Additions to the Setup menu.....	105
7.7 Printout of bandwidth profile on the voucher.....	105
7.8 Template preview.....	106
7.8.1 Template preview in WEBconfig.....	106
7.9 Logging DNS requests and responses to external SYSLOG servers.....	107
7.9.1 Logging DNS requests and responses to external SYSLOG servers.....	107
7.9.2 Additions to the Setup menu.....	108
7.10 Protection against brute force attacks.....	112
7.10.1 Protection against brute force attacks.....	112
7.10.2 Additions to the Setup menu.....	112
8 Routing and WAN connections.....	115
8.1 Route monitor.....	115
8.1.1 Route monitor.....	115
8.1.2 Additions to the Setup menu.....	116
8.2 DiffServ field enabled by default.....	120
8.2.1 Additions to the Setup menu.....	120
9 Other services.....	121
9.1 IPv6 support for (S)NTP client and server.....	121

1 Addendum to LCOS version 9.18 RU1

This document describes the changes and enhancements in LCOS version 9.18 RU1 since the previous version.

2 Configuration

2.1 Preventing password form fields in the browser from storing passwords

As of LCOS version 9.18 RU1, the storage of passwords in browser login forms can be suppressed with WEBconfig.

2.1.1 Preventing password form fields in the browser from storing passwords

Input dialogs on web pages allow web browsers to store any passwords that are entered. This makes things easier for a user accessing the page again in future. This web browser feature is a vulnerability that malicious software can exploit to read out the confidential form data.

To force the manual input of login passwords each time a page is invoked, use WEBconfig and navigate to **Setup > HTTP > Disable password autocompletion** and stop the storage of form field content with the setting "Yes".

2.1.2 Additions to the Setup menu

Disable password autocompletion

Here you configure whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

SNMP ID:

2.21.22

Telnet path:

Setup > HTTP

Possible values:

No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

Yes


The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

Default:

No

2.2 DHCP client with vendor DHCP option for LSR rollouts

As of version 9.18 RU1, LCOS in an unconfigured state uses the vendor-specific DHCP option 43 to transfer LSR information to the DHCP server, which then returns the LSR contact information to the device.

 The following LANCOM devices support this feature: L-3xx, L-4xx, L-13xx, L-151 LN-830, L-822, 178x-series OAPs, IAPs, WLCs, 7100(+), 9100(+), 831A, 1631E, E-series.

2.2.1 Receiving LSR information via DHCP server

An unconfigured LANCOM device boots with an activated DHCP client and uses this to retrieve an IP address, netmask, DNS address, and gateway address from the network's DHCP server.

By means of the vendor-specific DHCP option 43, a suitably configured DHCP server sends information about how to reach an LSR (Large Scale Rollout) server, among other things. The rollout agent of the LANCOM device processes this information, contacts the LSR server and, according to the rollout strategy, it retrieves its configuration, updates its firmware, or whatever is required.

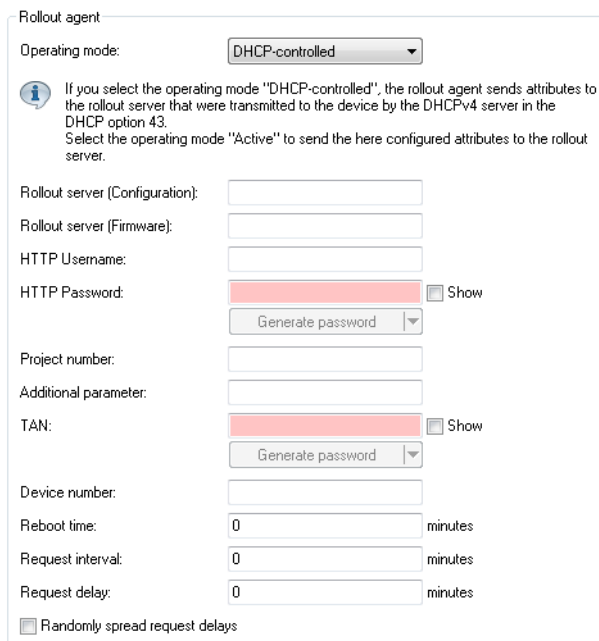
This function simplifies the rollout process as the devices no longer have to be preconfigured. This LSR information can also be compiled from variables, in which case it is possible to operate without a central rollout system (LSR).

The LSR server connects via HTTP, HTTPS or TFTP, in which case an SSL certificate needs to be stored on the LANCOM device to secure the connection.

It remains possible to configure a rollout agent in advance. In this case, the LSR information received by the LANCOM device is sure to contain the current address of the LSR server.


Configuration with LANconfig

The rollout agent is configured in LANconfig under **Management > Rollout Agent**.



Operation mode

If you select the operating mode "DHCP-controlled", the rollout agent sends the rollout server the attributes that the device received from the DHCP server by means of the vendor-specific DHCP option 43. In the "Active" operating mode, the device sends the attributes configured in this dialog. Setting the mode to "Off" disables the rollout agent.

 The "DHCP-controlled" operating mode does not overwrite manually configured attributes. This makes it possible to carry out a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

Rollout server (configuration)

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.



An entry can take the following form:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

Rollout server (firmware)

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.



An entry can take the following form:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

HTTP username

Set the user name used by the rollout agent to log on to the rollout server.

HTTP password

Set the user password used by the rollout agent to log on to the rollout server.

Project number

This entry specifies the rollout project number for the rollout agent.

Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

TAN

Use this entry to specify the rollout TAN.

Device number

Contains the device number of the device that is running the rollout agent.

Reboot time

Here you set the time at which the device should reboot after a rollout.

Request interval

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.



If the value is "0" the repeated attempt takes place in 1 minute.

Request delay

This entry contains the delay time in seconds for a rollout request.

Randomly spread request delays

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

2.2.2 Additions to the Setup menu

Rollout agent

This menu allows you to configure the settings for the rollout agent.

SNMP ID:

2.11.92

Telnet path:

Setup > Config

Operating

This entry determines how the rollout agent operates.

SNMP ID:

2.11.92.1

Telnet path:

Setup > Config > Rollout-Agent

Possible values:**No**

The rollout agent is disabled.

Yes

The rollout agent is enabled and transmits the rollout data that is configured in the device to the rollout server.

DHCP initiated

The rollout agent is enabled. It processes the information received from the DHCP server in the DHCP option 43.



The "DHCP-initiated" operating mode does not overwrite manually configured attributes. This makes it possible to carry out a comprehensive pre-configuration based on the latest contact information for the rollout server (address, login data) as communicated by the DHCP server.

Default:

DHCP initiated

Configuration server

Use this entry to specify the address of the rollout server that is responsible for rolling out the configuration.



An entry can take the following form:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

SNMP ID:

2.11.92.2

Telnet path:**Setup > Config > Rollout-Agent****Possible values:**

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

Default:*empty***Firmware server**

Use this entry to specify the address of the rollout server that is responsible for rolling out the firmware.



An entry can take the following form:

- IP address (HTTP, HTTPS, TFTP)
- FQDN

SNMP ID:

2.11.92.3

Telnet path:**Setup > Config > Rollout-Agent****Possible values:**

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

Default:*empty***User name**

Set the user name used by the rollout agent to log on to the rollout server.

SNMP ID:

2.11.92.4

Telnet path:**Setup > Config > Rollout-Agent****Possible values:**

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

Default:*empty*

Password

Set the user password used by the rollout agent to log on to the rollout server.

SNMP ID:

2.11.92.5

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

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

Default:

empty

Project number

This entry specifies the rollout project number for the rollout agent.

SNMP ID:

2.11.92.6

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

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

Default:

empty

Additional parameter

Use this entry to specify any additional parameters that the rollout agent should transfer to the rollout server.

SNMP ID:

2.11.92.7

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

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

Default:

empty

Reboot time

Here you set the time at which the device should reboot after a rollout.

SNMP ID:

2.11.92.8

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

Max. 10 characters from [0–9]

Default:

0

Request interval

If a configuration fails, the time in seconds you set here is the delay before a request for a configuration rollout is repeated.

SNMP ID:

2.11.92.9

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

Max. 10 characters from [0–9]

Default:

0

Special values:

0

The next attempt starts in 1 minute.

TAN

Use this entry to specify the rollout TAN.

SNMP ID:

2.11.92.10

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

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

Default:*empty***Device number**

Contains the device number of the device that is running the rollout agent.

SNMP ID:

2.11.92.11

Telnet path:**Setup > Config > Rollout-Agent****Possible values:**

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

Default:*empty***Request delay**

This entry contains the delay time in seconds for a rollout request.

SNMP ID:

2.11.92.12

Telnet path:**Setup > Config > Rollout-Agent****Possible values:**

Max. 10 characters from [0-9]

Default:

0

Request time random

With this entry, you specify that the request for a rollout takes place after a random delay. This setting prevents all of the devices involved in the rollout from requesting a configuration from the LSR server all at the same time.

SNMP ID:

2.11.92.13

Telnet path:**Setup > Config > Rollout-Agent**

Possible values:

No
Yes

Default:

No

Omit certificate check

Specifies whether a server certificate verification is carried out on HTTPS connections.

SNMP ID:

2.11.92.14

Telnet path:

Setup > Config > Rollout-Agent

Possible values:

No
A certificate check is carried out.
Yes
No certificate check is carried out.

Default:

No

3 WLAN

3.1 Adaptive RF Optimization



Improved WLAN throughput due to dynamic selection of the best WLAN channel by the access point in case of interference.

Choosing a WLAN channel specifies which part of the frequency band is used by an access point for its logical WLANs. To ensure the flawless operation of a WLAN within range of another access point, each of the access points should be using a separate channel—otherwise the WLANs have to share the medium. For this purpose, LANCOM access points use the feature Adaptive RF Optimization: The access point permanently scans the radio field for interfering signals. If a threshold is exceeded on the current WLAN channel (by means of the “wireless quality indicators”), the access point automatically switches to a qualitatively better channel. This intelligent feature enables the access point to dynamically adapt to an ever-changing radio field in order to maximize the WLAN’s stability.

In LANconfig you have the option to manually configure the different thresholds that are used as the basis for an automatic channel change.



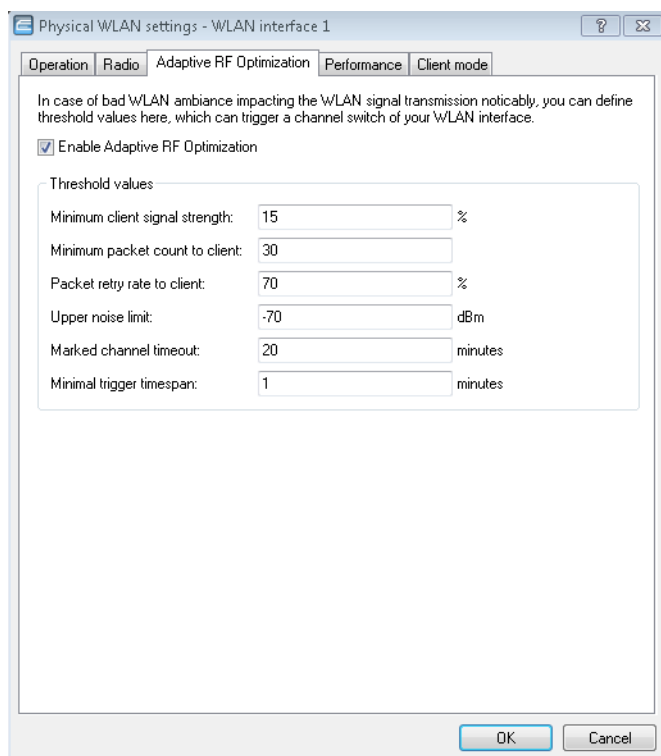
With the current LCOS version **Adaptive RF Optimization** is available to the following devices: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

3.1.1 Setting up Adaptive RF Optimization with LANconfig



In order to use LANconfig to configure the function Adaptive RF Optimization, it is necessary for the devices that you want to configure to offer the feature “Wireless Quality Indicators”. Further information about WQI is available in the reference manual.

To configure Adaptive RF Optimization, open LANconfig and go to **Wireless LAN > General**. In the “Interfaces” section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure and go to the tab **Adaptive RF Optimization**.



Enable Adaptive RF Optimization

To enable monitoring of the WLAN radio field via Adaptive RF Optimization, check the box **Enable Adaptive RF Optimization**.

You then configure the thresholds that trigger automatic channel changes.

Minimum client signal strength

Setting for the minimum client signal strength. Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change. The value is set in % with a default of 15.

Minimum packet count to client

Setting for the minimum number of packets sent to a client (TX). Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change (default value: 30).

Packet retry rate to client

Setting for the upper limit of packets that are resent to a client. If a client receives a proportion of resent packets that exceeds this percentage value, the device will consider this client the next time the need for a channel change is evaluated. The value is set in % with a default of 70.

Upper noise limit

Setting for the upper limit of acceptable noise on the channel. The value is set in dBm with a default of -70.

Marked channel timeout

If a channel is considered unusable, it will be marked/blocked for the length of time specified here. This value also blocks the channel change trigger in case all channels have been blocked. The value is set in minutes (default value: 20).

Minimal trigger timespan

Here you specify for how long a limit is exceeded continuously before an action is triggered. The timer is reset if no limits are exceeded for a period of 20 seconds. If a limit is exceeded for the entire time span, the current channel is blocked/marked. The value is set in minutes (default value: 1).



For this setting we recommend small single-digit values.

3.1.2 Additions to the Setup menu

Adaptive-RF-Optimization

Adaptive RF Optimization constantly monitors the WLAN environment and evaluates the quality of the network based on the "Wireless Quality Indicators". If the quality drops, the Adaptive RF Optimization triggers a change to a better suited channel.

SNMP ID:

2.23.20.23

Telnet path:

Setup > Interfaces > WLAN

Ifc

Shows the interface for the Adaptive RF Optimization.

SNMP ID:

2.23.20.23.1

Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

Operating

Activates or deactivates Adaptive RF Optimization for this interface.

SNMP ID:

2.23.20.23.2

Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

Possible values:

No
Yes

Default:

No

Min-Client-Phy-Signal

Setting for the minimum signal strength of clients.

SNMP ID:

2.23.20.23.3

Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

Possible values:

Max. 3 characters from [0-9]

Default:

15

Min-Client-Tx-Packets

Setting for the minimum number of packets sent to a client.

SNMP ID:

2.23.20.23.4

Telnet path:

Setup > Interfaces > WLAN > Adaptive-RF-Optimization

Possible values:

Max. 5 characters from [0-9]

Default:

30

Tx-Client-Retry-Ratio-Limit

In this field you specify how quickly a packet is resent to a client.

SNMP ID:

2.23.20.23.5

Telnet path:**Setup > Interfaces > WLAN > Adaptive-RF-Optimization****Possible values:**

Max. 3 characters from [0–9]

Default:

70

Noise-Limit

Setting for the upper limit of acceptable noise on the channel.

SNMP ID:

2.23.20.23.6

Telnet path:**Setup > Interfaces > WLAN > Adaptive-RF-Optimization****Possible values:**

Max. 6 characters from [0–9] –

Default:

-70

Marked-Channel-Timeout

When a channel is considered unusable it is marked/blocked for the time specified here.

SNMP ID:

2.23.20.23.7

Telnet path:**Setup > Interfaces > WLAN > Adaptive-RF-Optimization****Possible values:**

Max. 5 characters from [0–9]

Default:

20

Trigger-Timespan

The trigger timespan set here determines how long a limit is continuously exceeded before an action is triggered.

SNMP ID:

2.23.20.23.8

Telnet path:**Setup > Interfaces > WLAN > Adaptive-RF-Optimization****Possible values:**

Max. 5 characters from [0–9]

Default:

1

3.2 Airtime Fairness



By fairly sharing the WLAN transmission time between all of the active clients, the available bandwidth is used to maximum effect and WLAN performance is improved.

Especially in WLAN scenarios with a high client-density, the devices have to compete for the available bandwidth. Here, the AP offers transmission slots to each of the clients in turn—without any consideration for the necessary transmission times. Legacy clients end up slowing down faster clients, even though the faster ones could complete their data transmission more quickly. The feature “Airtime Fairness” ensures that the available bandwidth is used efficiently. To this end, the WLAN transmission time (“airtimes”) is fairly distributed between the active clients. The consequence: Thanks to all clients being provided with the same airtime, faster clients can achieve more data throughput in the same amount of time.

“Airtime” refers to the WLAN transmission time. Airtime Fairness provides WLAN transmission time to all of the active clients according to the mode configured for the Airtime Fairness. This, for example, stops older clients from slowing down more modern clients.



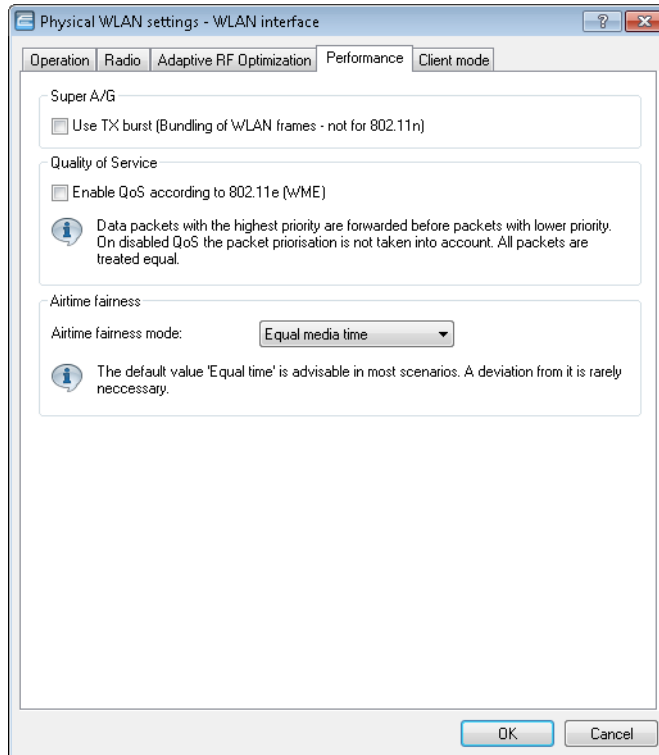
For devices with WLAN modules supporting the IEEE 802.11ac standard, the **Airtime Fairness** feature is automatically enabled in the WLAN module.



With the current LANCOM version **Airtime Fairness** is available to the following devices: L-151, L-3xx, L-4xx, L-8xx, LN-8xx, L-13xx, IAP-3xx, OAP-3xx, OAP-8xx.

3.2.1 Setting up Airtime Fairness with LANconfig

Go to **Wireless LAN > General**. In the **Interfaces** section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure, and go to the tab **Performance**.



In the section **Airtime fairness mode** you select the Airtime Fairness operating mode:

Round robin scheduling

Each client receives a time slot for transmission, one after the other.

Equal media time

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because they can transmit a greater amount of data to the access point in a given amount of time.



IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

802.11n preferred

This setting prefers clients using IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

Equal media volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down the other clients.



This setting is only recommended where it is necessary for all clients to receive the same throughput.

3.2.2 Additions to the Setup menu

Airtime-Fairness-Mode

Airtime Fairness is a feature that shares the available bandwidth fairly between all of the active clients. Especially useful in high-density environments, it results in an improvement to WLAN performance. **Airtime Fairness** is activated by default.

SNMP ID:

2.23.20.9.6

Telnet path:

Setup > Interfaces > WLAN > Performance

Possible values:

Round-Robin

Each client in turn receives a time slot for transmission.

Equal-Airtime

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because the access point can send more data to the client in the same amount of time.



IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

Pref.-11n-Airtime

This setting prefers clients that use IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent much faster to clients using IEEE 802.11n.

Equal-Volume

This setting distributes the airtime between the clients to ensure that all clients receive the same amount of throughput by the access point. However, slower clients will slow down all clients.



This setting is only recommended when it is necessary for all clients to receive the same throughput.

Default:

Equal-Airtime

3.3 Encrypted OKC via IAPP

As of LCOS version 9.18 RU1, it is also possible to use OKC (opportunistic key caching) in networks operating without a WLC.

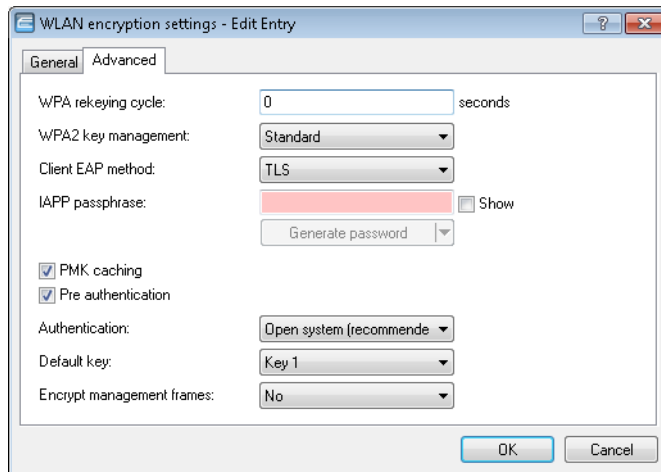
3.3.1 Encrypted OKC via IAPP

OKC (opportunistic key caching) enables WLAN clients to connect to APs without having to authenticate every time. If a client associates with an AP and authenticates successfully, this AP transmits the PMK (pairwise master key) to a WLC, which informs all of the other APs on the network. Consequently, the client is known to all of the APs. A client moving into signal range of a neighboring AP negotiates a new connection with it. This type of OKC requires a WLC, which coordinates the PMKs between the APs.

The IAPP (Inter Access Point Protocol) serves to exchange information between APs in a network, including information about the BSSIDs they operate and the WLAN clients authenticated with them. This makes it possible for a client to move between the areas of signal coverage of the various APs. Each AP queries all of the other APs for information about the new client, and informs them when the client associates with it. This communication allows the implementation of OKC directly between the APs, without the need for a WLC.

By setting an IAPP passphrase (PMK-IAPP secret) on an AP, it is possible to transfer the encrypted PMK (pairwise master key) to the other APs and store it there. This makes OKC available to all of the APs on the network, without the need for a WLC.

In LANconfig, the IAPP passphrase is entered under **Wireless LAN > 802.11i/WEP** and clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.



3.3.2 Additions to the Setup menu

PMK-IAPP-Secret

Networked APs exchange data about associated WLAN clients by means of the IAPP, which ensures that the WLAN clients roam securely. The mechanism is similar to the OKC used for WLC management, although here it works entirely without WLCs.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

SNMP ID:

2.23.20.3.20

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

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

Default:

empty

Special values:

empty

OKC via IAPP is disabled.

3.4 Fast roaming

As of LCOS version 9.18 RU1, fast roaming (IEEE 802.11r) is available also for networks that operate without a WLC.

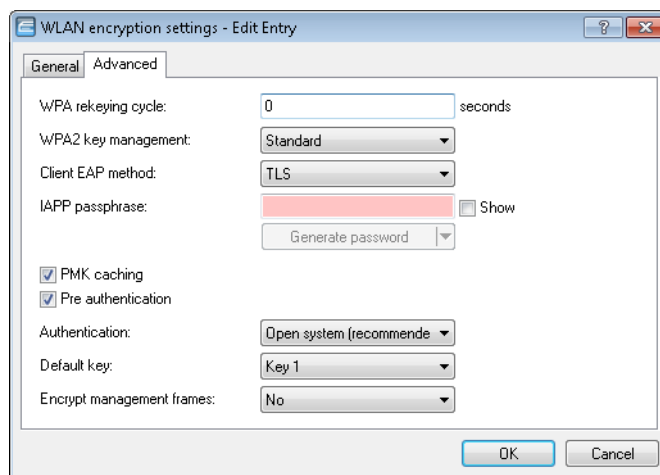
3.4.1 Fast roaming with IAPP

IEEE 802.11r reduces the time required for authentication and minimizes the interruption when a WLAN client moves from one AP to another. These interruptions typically last for several hundred milliseconds.

Fast roaming with the Inter Access Point Protocol (IAPP) enables you to operate IEEE 802.11r directly on your APs. Until now, a WLC was required for this purpose.

In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). APs that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between themselves and ensure uninterrupted connections.

In LANconfig, the IAPP passphrase is entered under **Wireless LAN > encryption** and clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.



ⓘ Please note the use of IEEE 802.11r requires **WPA2 key management** in the encryption settings to be set to "Fast roaming".

3.4.2 Additions to the Setup menu

PMK-IAPP-Secret

Networked APs exchange data about associated WLAN clients by means of the IAPP, which ensures that the WLAN clients roam securely. The mechanism is similar to the OKC used for WLC management, although here it works entirely without WLCs.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

SNMP ID:

2.23.20.3.20

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

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

Default:

empty

Special values:

empty

OKC via IAPP is disabled.

3.5 Wireless Intrusion Detection System (WIDS)

An Intrusion Detection System (IDS) recognizes attacks on a network and reports these attacks to a network management system. Especially in a professional environment, an IDS is essential for the detection and handling of potential attacks or interference.

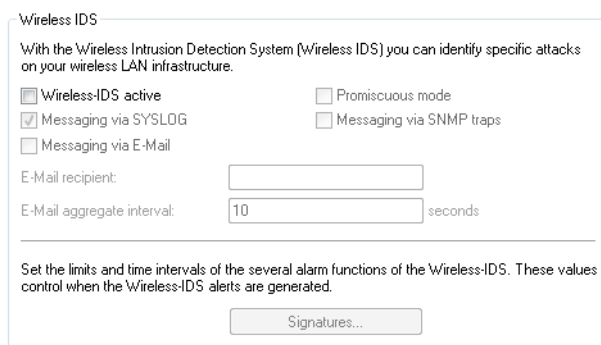
The Wireless Intrusion Detection System (WIDS) in LCOS devices monitors the different WLANs by using a wide range of specified thresholds. If a potential attack is detected, the system reports it immediately via e-mail, SYSLOG, or SNMP traps.

Attacks are detected by monitoring for known or similar patterns.

 Please note that detection based on pattern recognition (heuristics) can lead to false alarms ("false positives").

3.5.1 Setting up the Wireless Intrusion Detection System with LANconfig

To configure the Wireless Intrusion Detection System (WIDS) open LANconfig and go to **Wireless LAN > Security**.


Wireless-IDS active

Activates or deactivates the Wireless Intrusion Detection System.

Promiscuous mode

With the ("promiscuous mode") enabled, the AP additionally receives packets that were not directed at it, but to other network participants.

This mode is necessary to be able to detect the attacks listed below. However, the promiscuous mode affects the performance. For this reason, activating the promiscuous mode automatically causes frame aggregation to be switched off.

Messaging via SYSLOG

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level “INFO” and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

Messaging via SNMP traps

Activates or deactivates the WIDS messaging via SNMP traps.

Messaging via e-mail

Activates or deactivates the messaging via e-mail.



An SMTP account has to be configured in order to use messaging via e-mail.

E-mail recipient

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

E-mail aggregate interval

This setting sets the delay in seconds before a new e-mail is sent if the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

Signatures

Here you configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

Attack scenarios	Measuring interval
EAPOL start: 250 Packets	per interval of: 10 seconds
Broadcast probe: 1.500 Packets	per interval of: 10 seconds
Authentication request: 250 Packets	per interval of: 10 seconds
Deauthentication: 250 Packets	per interval of: 10 seconds
Broadcast deauthentication: 2 Packets	per interval of: 1 seconds
Association request: 250 Packets	per interval of: 10 seconds
Reassociation request: 250 Packets	per interval of: 10 seconds
Disassociation request: 250 Packets	per interval of: 10 seconds
Broadcast disassociate: 2 Packets	per interval of: 1 seconds
Out-of-window: 200 Packets	per interval of: 5 seconds
Block Ack after DelBA: 100 Packets	per interval of: 5 seconds
Null data flood: 500 Packets	per interval of: 5 seconds
Null data PS buffer overflow: 200 Packets	per interval of: 5 seconds
Multi stream data: 100 Packets	per interval of: 5 seconds
Premature EAPOL success: 0 Packets	per interval of: 1 seconds
Premature EAPOL failure: 0 Packets	per interval of: 1 seconds
PS poll TIM interval: 100 Packets	per interval of: 5 seconds
Listen interval difference: 5	

The following attack scenarios can be detected by configuring the thresholds and measuring intervals:

- EAPOL-Start
- Broadcast probe
- Authentication request
- Deauthentication request (*)
- Broadcast deauthentication
- Association request
- Reassociation request
- Disassociation request (*)
- Broadcast disassociate

- Out-of-window
- Block Ack after DelBA
- Null data flood
- Null data PS buffer overflow
- Multi stream data
- Premature EAPOL success (*)
- Premature EAPOL failure (*)
- PS poll TIM interval
- Listen interval difference

There are typical default values set for the different attack scenarios.



(*) These attacks are only detected if promiscuous mode is active.

3.5.2 Additions to the Setup menu

Wireless-IDS

In this directory, you configure the Wireless Intrusion Detection System (WIDS).

SNMP ID:

2.12.248

Telnet path:

Setup > WLAN

IDS-Operational

Activates or deactivates the Wireless Intrusion Detection System (WIDS).

SNMP ID:

2.12.248.9

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:**No**

The Wireless Intrusion Detection System is deactivated.

Yes

The Wireless Intrusion Detection System is activated.

Default:

No

Syslog-Operational

Activates or deactivates the messaging via SYSLOG.

The generated SYSLOG message has the severity level "INFO" and contains the timestamp, the interface, and the trigger (type of attack and passed threshold).

SNMP ID:

2.12.248.10

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:**No**

WIDS messaging via SYSLOG is disabled.

Yes

WIDS messaging via SYSLOG is enabled.

Default:

Yes

SNMPTraps-Operational

Activates or deactivates the WIDS messaging via SNMP traps.

SNMP ID:

2.12.248.11

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:**No**

Messaging via SNMP traps is disabled.

Yes

Messaging via SNMP traps is enabled.

Default:

No

E-mail

Activates or deactivates the messaging via e-mail.



An SMTP account has to be configured in order to use messaging via e-mail.

SNMP ID:

2.12.248.12

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:**No**

Messaging via e-mail is disabled.

Yes

Messaging via e-mail is enabled.

Default:

No

E-Mail-Receiver

The e-mail address of the recipient when messaging via e-mail is activated.

The field must contain a valid e-mail address.

SNMP ID:

2.12.248.13

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:

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

E-Mail-Aggregate-Interval

This setting sets the delay in seconds before a new e-mail is sent in case the WIDS is triggered again.

This prevents flooding by e-mail in case of extensive attacks.

SNMP ID:

2.12.248.14

Telnet path:

Setup > WLAN > Wireless-IDS

Possible values:

Max. 4 characters from [0–9]

Default:

10

Signatures

Here you configure the various thresholds and measuring intervals (packets per second) of the different WIDS alarm functions. These settings are used by the WIDS to determine if an attack is taking place.

SNMP ID:

2.12.248.50

Telnet path:

Setup > WLAN > Wireless-IDS

AssociateReqFlood

Here you configure the threshold for attacks of the type AssociateReqFlood.

SNMP ID:

2.12.248.50.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.1.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

Possible values:

Max. 4 characters from [0–9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.1.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AssociateReqFlood

Possible values:

Max. 4 characters from [0 – 9]

Default:

10

ReassociateReqFlood

Here you configure the threshold for attacks of the type ReassociateReqFlood.

SNMP ID:

2.12.248.50.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.2.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood

Possible values:

Max. 4 characters from [0 – 9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.2.2

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > ReassociateReqFlood****Possible values:**

Max. 4 characters from [0 – 9]

Default:

10

AuthenticateReqFlood

Here you configure the threshold for attacks of the type AuthenticateReqFlood.

SNMP ID:

2.12.248.50.3

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures****CounterLimit**

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.3.1

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood****Possible values:**

Max. 4 characters from [0 – 9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.3.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > AuthenticateReqFlood

Possible values:

Max. 4 characters from [0–9]

Default:

10

EAPOLStart

Here you configure the threshold for attacks of the type EAPOLStart.

SNMP ID:

2.12.248.50.4

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.4.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > EAPOLStart

Possible values:

Max. 4 characters from [0–9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.4.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > EAPOLStart

Possible values:

Max. 4 characters from [0 – 9]

Default:

10

ProbeBroadcast

Here you configure the threshold for attacks of the type ProbeBroadcast.

SNMP ID:

2.12.248.50.5

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.5.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

Possible values:

Max. 4 characters from [0 – 9]

Default:

1500

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.5.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > ProbeBroadcast

Possible values:

Max. 4 characters from [0 – 9]

Default:

10

DisassociateBroadcast

Here you configure the threshold for attacks of the type DisassociateBroadcast.

SNMP ID:

2.12.248.50.6

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures****CounterLimit**

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.6.1

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast****Possible values:**

Max. 4 characters from [0–9]

Default:

2

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.6.2

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > DisassociateBroadcast****Possible values:**

Max. 4 characters from [0–9]

Default:

1

DeauthenticateBroadcast

Here you configure the threshold for attacks of the type DeauthenticateBroadcast.

SNMP ID:

2.12.248.50.7

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.7.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

Possible values:

Max. 4 characters from [0–9]

Default:

2

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.7.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateBroadcast

Possible values:

Max. 4 characters from [0–9]

Default:

1

DisassociateReqFlood

Here you configure the threshold for attacks of the type DisassociateReqFlood.

SNMP ID:

2.12.248.50.8

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures****CounterLimit**

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.8.1

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood****Possible values:**

Max. 4 characters from [0–9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.8.2

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > DisassociateReqFlood****Possible values:**

Max. 4 characters from [0–9]

Default:

10

BlockAckOutOfWindow

Here you configure the threshold for attacks of the type BlockAckOutOfWindow.

SNMP ID:

2.12.248.50.9

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.9.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

Possible values:

Max. 4 characters from [0–9]

Default:

200

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.9.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckOutOfWindow

Possible values:

Max. 4 characters from [0–9]

Default:

5

BlockAckAfterDelBA

Here you configure the threshold for attacks of the type BlockAckAfterDelBA.

SNMP ID:

2.12.248.50.10

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.10.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

Possible values:

Max. 4 characters from [0 – 9]

Default:

100

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.10.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > BlockAckAfterDelBA

Possible values:

Max. 4 characters from [0 – 9]

Default:

5

NullDataFlood

Here you configure the threshold for attacks of the type NullDataFlood.

SNMP ID:

2.12.248.50.11

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.11.1

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > NullDataFlood****Possible values:**

Max. 4 characters from [0–9]

Default:

500

CounterInterval

Set the interval in seconds, in which the number of received packets of this type have to pass the set threshold before the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.11.2

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > NullDataFlood****Possible values:**

Max. 4 characters from [0–9]

Default:

5

NullDataPSBufferOverflow

Here you configure the threshold for attacks of the type NullDataPSBufferOverflow.

SNMP ID:

2.12.248.50.12

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures****CounterLimit**

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.12.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

Possible values:

Max. 4 characters from [0–9]

Default:

200

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.12.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > NullDataPSBufferOverflow

Possible values:

Max. 4 characters from [0–9]

Default:

5

PSPollTIMInterval

Here you configure the threshold for attacks of the type PSPollTIMInterval.

SNMP ID:

2.12.248.50.13

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.13.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

Possible values:

Max. 4 characters from [0–9]

Default:

100

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.13.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

Possible values:

Max. 4 characters from [0–9]

Default:

5

Interval-Diff**SNMP ID:**

2.12.248.50.13.3

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PSPollTIMInterval

Possible values:

Max. 4 characters from [0–9]

Default:

5

SMPSMultiStream

Here you configure the threshold for attacks of the type SMPSMultiStream.

SNMP ID:

2.12.248.50.14

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.14.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > SMPSPMultiStream

Possible values:

Max. 4 characters from [0–9]

Default:

100

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.14.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > SMPSPMultiStream

Possible values:

Max. 4 characters from [0–9]

Default:

5

DeauthenticateReqFlood

Here you configure the threshold for attacks of the type DeauthenticateReqFlood.

SNMP ID:

2.12.248.50.15

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.15.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

Possible values:

Max. 4 characters from [0–9]

Default:

250

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.15.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > DeauthenticateReqFlood

Possible values:

Max. 4 characters from [0–9]

Default:

10

PrematureEAPOLSuccess

Here you configure the threshold for attacks of the type PrematureEAPOLSuccess.

SNMP ID:

2.12.248.50.16

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

CounterLimit

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.16.1

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess****Possible values:**

Max. 4 characters from [0 – 9]

Default:

2

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.16.2

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLSuccess****Possible values:**

Max. 4 characters from [0 – 9]

Default:

1

PrematureEAPOLFailure

Here you configure the threshold for attacks of the type PrematureEAPOLFailure.

SNMP ID:

2.12.248.50.17

Telnet path:**Setup > WLAN > Wireless-IDS > Signatures****CounterLimit**

Set the threshold number of packets, beyond which the WIDS will notify of an attack.

SNMP ID:

2.12.248.50.17.1

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

Possible values:

Max. 4 characters from [0–9]

Default:

2

CounterInterval

Set the interval in seconds, within which the threshold set for the number of received packets of this type must be exceeded in order for WIDS to notify of an attack.

SNMP ID:

2.12.248.50.17.2

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures > PrematureEAPOLFailure

Possible values:

Max. 4 characters from [0–9]

Default:

1

Promiscuous-Mode

Activates or deactivates the promiscuous mode. This mode handles also packets that were not sent to the device itself. These packets are forwarded to LCOS to allow an analysis by the WIDS.

This mode can be used to detect the following attacks:

- PrematureEAPOLFailure
- PrematureEAPOLSuccess
- DeauthenticateReqFlood
- DisassociateReqFlood



Please note that the promiscuous mode has a significant impact on the performance. For example, frame aggregation is deactivated while it is in action. Only use this mode in case of a strong suspicion.

SNMP ID:

2.12.248.51

Telnet path:

Setup > WLAN > Wireless-IDS > Signatures

3 WLAN

Possible values:**No**

Promiscuous mode is disabled.

Yes

Promiscuous mode is enabled.

Default:

No

3.6 Status counters for failed WPA-PSK/IEEE 802.1X login attempts

As of LCOS version 9.18 RU1, you have the option to display the number of failed login attempts for WPA and IEEE 802.1X.

3.6.1 Status counters for WPA-PSK login attempts

An overview of the number of failed WPA-PSK login attempts is located in the LCOS menu tree under **Status > WLAN > Encryption**.

There is also an overview of successful login attempts, as well as the number of authorizations rejected due to an incorrect passphrase.

Encryption													
Interface	Encryption	Method	WPA Version	WPA1-Session-Keytypes	WPA2-Session-Keytypes	PMK Caching	Pre Authentication	OKC	Prot.-Mgmt-Frames	WPA2-Key-Management	WPA-PSK-Num-Success	WPA-PSK-Num-Failures	WPA-PSK-Num-Wrong-Passphrase
WLAN-1	Yes	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1.2	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1.3	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1.4	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1.5	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1.6	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0

Select an interface in the table (e.g. WLAN-1) to display the information for the selected interface.

Encryption	
Interface	WLAN-1
Encryption	Yes
Method	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Session-Keytypes	TKIP/AES
WPA2-Session-Keytypes	TKIP/AES
PMK-Caching	Yes
Pre-Authentication	Yes
OKC	No
Prot.-Mgmt-Frames	No
WPA2-Key-Management	Standard
WPA-PSK-Num-Success	0
WPA-PSK-Num-Failures	0
WPA-PSK-Num-Wrong-Passphrase	0

3.6.2 Status counters for IEEE 802.1X login attempts

A table showing the number of accepted and rejected connect requests for each logical interface is located in the LCOS menu tree under **Status > IEEE802.1x > Ports**.

The overview also indicates the number of times the authorization limit was reached for each interface.

Ports				
Port	Num-Accept	Num-Reject	Num-Reauth	Max-reached
LAN-1	0	0	0	
LAN-2	0	0	0	
LAN-3	0	0	0	
LAN-4	0	0	0	
WLAN-1	0	0	0	
P2P-1-1	0	0	0	
P2P-1-2	0	0	0	
P2P-1-3	0	0	0	
P2P-1-4	0	0	0	
P2P-1-5	0	0	0	
P2P-1-6	0	0	0	
P2P-1-7	0	0	0	
P2P-1-8	0	0	0	
P2P-1-9	0	0	0	
P2P-1-10	0	0	0	
P2P-1-11	0	0	0	
P2P-1-12	0	0	0	
P2P-1-13	0	0	0	
P2P-1-14	0	0	0	

3.6.3 Additions to the Status menu

WPA-PSK-Num-Wrong-Passphrase

Displays the number of WPA requests on this interface that were rejected due to an incorrect passphrase.

SNMP ID:

1.3.64.20

Telnet path:

Status > WLAN > Encryption

WPA-PSK-Num-Success

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.3.64.21

Telnet path:

Status > WLAN > Encryption

WPA-PSK-Num-Failures

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.3.64.22

Telnet path:**Status > WLAN > Encryption****Ports**

This table provides an overview of the accepted or rejected connection requests for each logical interface.

SNMP ID:

1.46.3

Telnet path:**Status > IEEE802.1x****Port**

Displays the name of the interface.

SNMP ID:

1.46.3.1

Telnet path:**Status > IEEE802.1x > Ports****Num-accept**

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.46.3.2

Telnet path:**Status > IEEE802.1x > Ports****Num-reject**

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.46.3.3

Telnet path:

Status > IEEE802.1x > Ports

Num-ReauthMax-reached

SNMP ID:

1.46.3.4

Telnet path:

Status > IEEE802.1x > Ports

3.7 Adaptive Transmission Power

As of LCOS version 9.18 RU1, the failure of any APs on the network can be automatically compensated for by increasing the transmission power of the other APs.

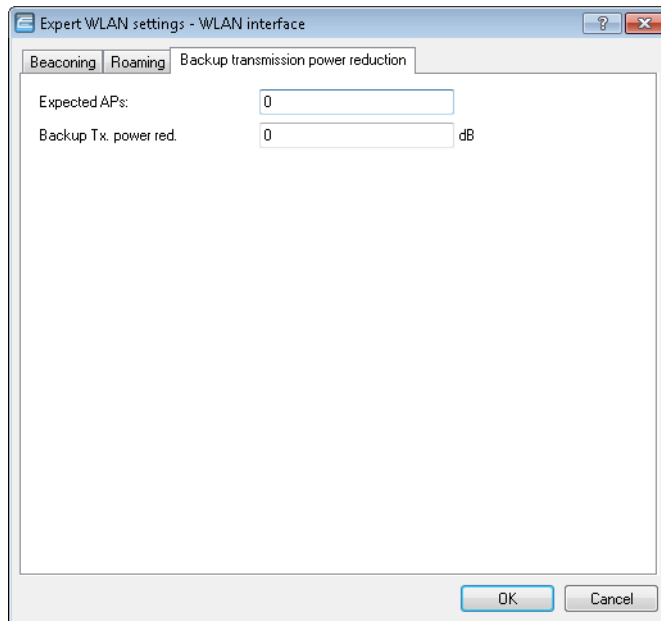
3.7.1 Configuring Adaptive Transmission Power with LANconfig

Dynamic transmission power adaptation is an essential feature for WLAN environments with professional backup scenarios. If an AP fails, the remaining access points automatically increase their transmission power to ensure full WLAN coverage at all times.

To do this, specify how many APs operate within a broadcast domain. So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs becomes equal to the expected number of devices. The other APs return their transmission power to the default value.

To configure this in LANconfig, go to **Wireless LAN > General**. In the "Extended settings" section, click the button **Expert WLAN settings** and, if your AP has multiple WLAN interfaces, select the appropriate one. Go to the **Backup transmission power reduction** tab and enter the number of expected APs and the power reduction.



Expected APs

Specify how many APs operate within a broadcast domain.

Backup TX power red.

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.



The default transmission power reduction is configured under **Wireless LAN > General** by clicking the button **Physical WLAN settings** (selecting the WLAN interface, if necessary) and accessing the **Radio** tab.

3.7.2 Additions to the Setup menu

Redundancy settings

In this directory, you configure the dynamic adjustment of transmission power in the event of the failure of an AP a cluster of several APs.

SNMP ID:

2.23.20.24

Telnet path:

Setup > Interfaces > WLAN

Ifc

The interface that this entry refers to.

SNMP ID:

2.23.20.24.1

Telnet path:**Setup > Interfaces > WLAN > Redundancy-Settings****Other APs expected**

Use this item to specify the number of other APs that are located in the AP cluster.

So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs is equal to the number of expected devices. The other APs return their transmission power to the default value.

SNMP ID:

2.23.20.24.2

Telnet path:**Setup > Interfaces > WLAN > Redundancy-Settings****Possible values:**

Max. 5 characters from [0–9]

Backup transmission power reduction

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

SNMP ID:

2.23.20.24.3

Telnet path:**Setup > Interfaces > WLAN > Redundancy-Settings****Possible values:**

Max. 3 characters from [0–9]

3.8 Improved start-up conditions for WLAN RADIUS accounting

Normally, the WLAN stack sends a RADIUS "accounting start" message as soon as the WLAN client is connected. Often the WLAN client has no IP address at this time, most likely because one has not yet been issued by the DHCP server. Consequently the "Framed-IP-Address" attribute in the RADIUS accounting message may lack meaningful content.

As of LCOS version 9.18 RU1, the accounting start message is optionally generated only after the client has received a valid IP address. In this case the RADIUS accounting server always receives a valid framed IP address.

3.8.1 Configuring start-up conditions for RADIUS accounting with LANconfig

In LANconfig, go to the view **Wireless LAN > General > Logical WLAN settings**. On the tab "Network", enable the check box **RADIUS accounting activated**.

You can now set the accounting start condition with the drop-down menu. The following settings are available.

Connected

Accounting starts when the WLAN client takes on the status "Connected". This is the default setting.

Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6).

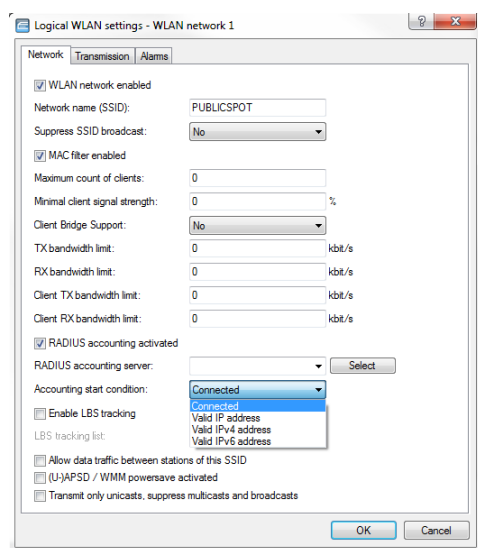
Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address.

Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address.

⚠️ APIPA addresses (169.254.1.0 – 169.254.254.255) are not recognized as valid IP addresses.

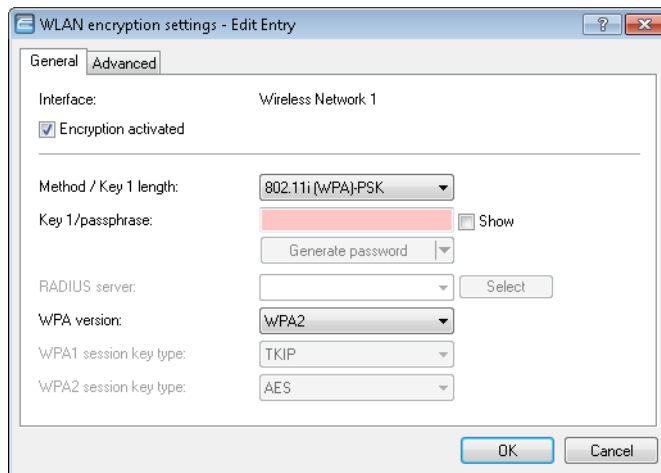


3.8.2 Configuring start-up conditions for RADIUS accounting with WEBconfig

In the LCOS menu tree, navigate to the view **Setup > Interfaces > WLAN > Network**. You can now set the accounting start condition with the drop-down menu.

3.9 Selecting a RADIUS server profile for 802.1X authentication

As of LCOS version 9.18 RU1, you have the option to specify a RADIUS server profile when you operate the IEEE 802.1X standard for authentication.



RADIUS server

If under **Method/Key 1 length** you select an authentication method based on the IEEE 802.1X standard, you specify the profile of a RADIUS server here.

3.9.1 Additions to the Setup menu

RADIUS profile

If you are operating an authentication method based on the IEEE 802.1X standard, you specify the profile of a RADIUS server here.

SNMP ID:

2.23.20.3.21

Telnet path:

Setup > Interfaces > WLAN > Encryption

Possible values:

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

Default:

empty

3.10 Configurable data rates per WLAN module

As of LCOS version 9.18 RU1, it is possible to configure the data rates for each WLAN module separately.

The following LANCOM devices support this option:

- L-151
- L-3xx
- L-4xx
- L-822
- LN-830
- L-13xx
- IAP-xxx
- OAP-xxx
- All E-series devices

The data rate currently being used is displayed in the status tree for the WLAN client and in LANmonitor.

3.10.1 Configurable data rates per WLAN module

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

! In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates “announced” by the AP to the client for its communication with the AP (RX).

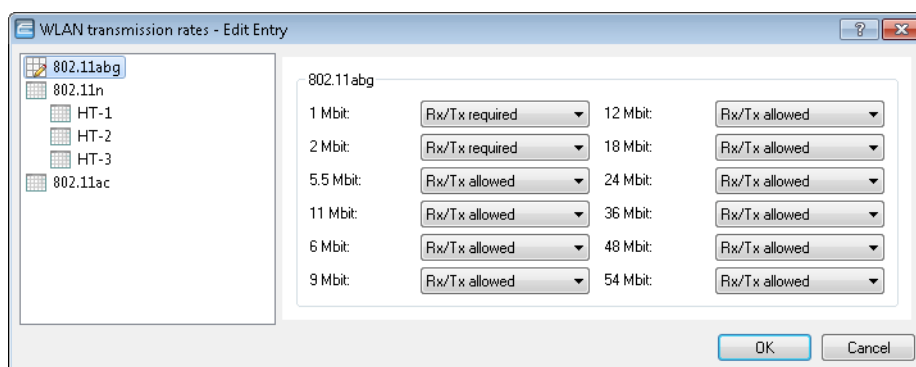
This rate adaptation specifies a minimum and a maximum data rate, and it also allows you to disable certain data rates between these limits.

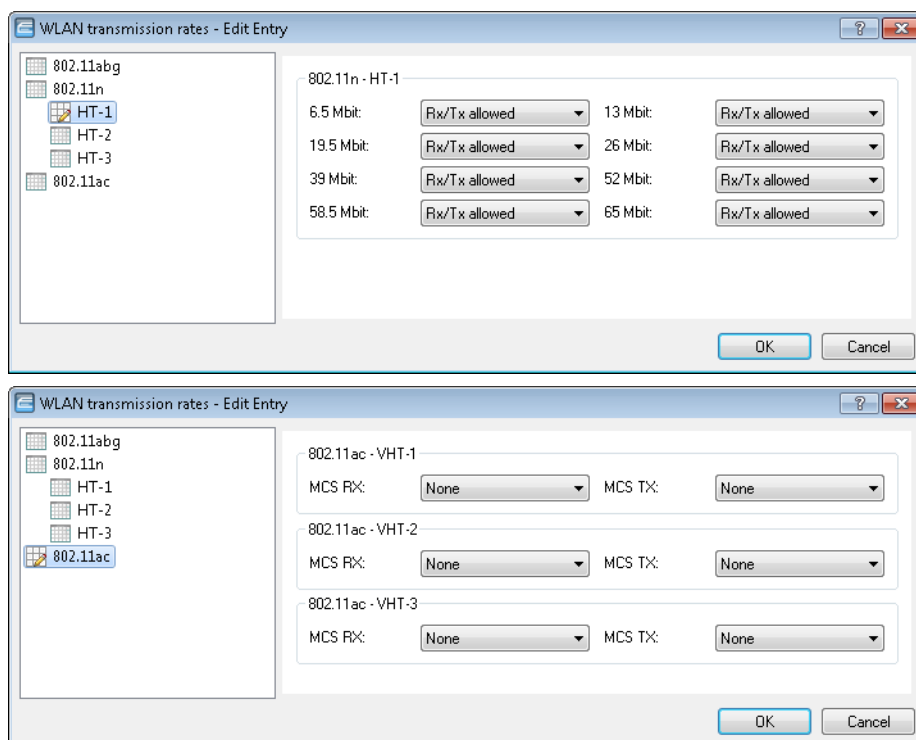
i The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

Configuring the data rates with LANconfig

To configure the data rates with LANconfig, switch to the view **Wireless LAN > General** and, in the **Extended settings** section, open the dialog **WLAN transmission rates**. LANconfig lists the settings for all of the available interfaces. To modify the settings for an interface, select the corresponding entry and click on **Edit**.

On the left you select the standard that you want to configure.





The configuration can be modified for each of the standards separately

- 802.11abg
- 802.11n
 - HT-1
 - HT-2
 - HT-3
- 802.11ac
 - VHT-1
 - VHT-2
 - VHT-3

Depending on the standard, the following settings are available for each transmission rate and each SSID or P2P link:

Rx/Tx required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx allowed

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx allowed

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Deactivated

The AP does not announce this rate and does not use it to communicate with the client.

MCS-9/8/7

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.


None

With 802.11ac modules, the respective stream option is disabled for the corresponding data direction.

3.10.2 Additions to the Setup menu


Rate selection

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

 In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates “announced” by the AP to the client for its communication with the AP (RX).

This rate adaptation specifies a minimum and a maximum data rate, and it also allows certain data rates between these limits to be disabled. This can save airtime under certain circumstances.

 The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

In this directory you configure these data rates.

SNMP ID:

2.23.20.25

Telnet path:

Setup > Interfaces > WLAN

1M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.1

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

2M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.2

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

Ifc

This entry shows which interface is being configured.

SNMP ID:

2.23.20.25.3

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

5.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.4

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

11M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.6

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

6M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.8

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection**

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

9M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.9

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

12M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.10

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

18M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.11

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

24M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.12

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

36M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.13

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

48M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.14

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

54M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.15

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-6.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.28

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-13M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.29

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-19.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.30

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection**

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-26M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.31

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.32

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-52M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.33

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-58.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.34

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-65M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.35

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-13M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.36

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-26M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.37

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.38

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-52M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.39

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-78M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.40

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-104M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.41

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-117M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.142

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-130M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.43

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-19.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.44

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.45

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-58.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.46

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-78M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.47

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-117M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.48

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-156M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.49

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection****Possible values:****No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-175.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.50

Telnet path:**Setup > Interfaces > WLAN > Rate-Selection**

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-195M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.51

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:**No**

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

VHT-1-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.105

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-1-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.106

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-2-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.115

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-2-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.116

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-3-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.125

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-3-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.



In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.126

Telnet path:

Setup > Interfaces > WLAN > Rate-Selection

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

4 WLAN management

4.1 Automatically switch off IAPP if a CAPWAP tunnel exists

As of LCOS version 9.18 RU1, a WLC disables IAPP on the managed APs as soon as a CAPWAP management tunnel exists between the APs and the WLC.

5 LANCOM Location Based Services (LBS)

5.1 Dynamic and persistent tracking lists for WLAN clients

As of LCOS version 9.18 RU1, it is also possible to configure the LBS tracking lists with LANconfig.

On the WLC, the LBS tracking list is configured under **WLAN controller > Profiles > Logical WLAN networks**.

Enable LBS tracking

This option specifies whether the LBS server is permitted to track the client information.



This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

On the AP, the LBS tracking list is configured under **Wireless LAN > General > Logical WLAN settings** on the **Network** tab.

Enable LBS tracking

This option specifies whether the LBS server is permitted to track the client information.



This option configures the tracking of all clients in an SSID. In the Public Spot module you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

5.1.1 Using the LBS tracking lists of Public Spot users

APs and WLCs feature the option to add associated Public Spot users to lists, and to register these users at an LBS (location-based service) server.

You configure this function for APs and WLCs in LANconfig under **Public Spot > Users** in the **LBS tracking** section.

Enable LBS tracking

Here you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

LBS tracking list

Name of the LBS tracking list sent by the AP or WLC to the LBS server.

5.1.2 Additions to the Setup menu**LBS-Tracking**

Here you determine whether the LBS server is allowed to track the users who are logged on to the Public Spot.

SNMP ID:

2.24.38

Telnet path:

Setup > Public-Spot-Module

Possible values:

No
Yes

Default:

No

LBS tracking list

Name of the LBS tracking list

SNMP ID:

2.24.39

Telnet path:

Setup > Public-Spot-Module

Possible values:

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

Default:

empty

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

SNMP ID:

2.37.1.1.47

Telnet path:**Setup > WLAN-Management > AP-Configuration****Possible values:****Name** from **Setup > WLAN-Management > AP-Configuration > LBS-Tracking**Max. 16 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;=>?[\]^_.`**Default:***empty*

LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

SNMP ID:

2.23.20.1.25

Telnet path:**Setup > Interfaces > WLAN > Network****Possible values:****No**

LBS tracking is disabled.

Yes

LBS tracking is enabled.

LBS tracking list

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the AP transfers the specified list name, the MAC address of the client, and its own MAC address to the LBS server.

SNMP ID:

2.23.20.1.26

Telnet path:**Setup > Interfaces > WLAN > Network****Possible values:****Name** from **Setup > WLAN > Network > LBS-Tracking**Max. 16 characters from `[A-Z][0-9]@{ }~!$%&'()+-,:;=>?[\]^_.`**Default:***empty*

6 RADIUS

6.1 User-definable attributes in the RADIUS client

Until now, all LANCOM devices have used the device name as the NAS identifier.

As of LCOS version 9.18 RU1, the NAS ID can be freely configured in LANconfig.

In LANconfig, you configure the attributes under **Communication > RADIUS** in the sections **Authentication via RADIUS for PPP and clip** and **Tunnel authentication via RADIUS for L2TP**.

Authentication via RADIUS for PPP and CLIP

RADIUS server: Protocols:

Address:

Server port:

Source address (optional):

Attribute values:

Secret: ☐ Show

PPP operation:

PPP authentication protocols:
☒ PAP ☒ CHAP ☒ MS-CHAP ☒ MS-CHAPv2

Tunnel authentication via RADIUS for L2TP

RADIUS server: Protocols:

Address:

Port:

Source address (optional):

Attribute values:

Secret: ☐ Show

Password: ☐ Show

Attribute values

LCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can be abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device, the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks ("`<Value>`") allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

6.2 Automatic clean-up of access information on the RADIUS server

As of LCOS version 9.18 RU1, the function "Auto-Cleanup-Accounting-Totals" is enabled by default.

6.2.1 Additions to the Setup menu

Auto-Cleanup-Accounting-Totals

Closed accounting sessions are deleted if the function "RADIUS cleanup user table" has removed the related RADIUS account.

SNMP ID:

2.25.10.18

Telnet path:

Setup > RADIUS > Server

Possible values:

No

Accounting information is not automatically deleted.

Yes

Accounting information is deleted automatically.

Default:

Yes

6.3 Vendor-specific RADIUS attribute "LCS-Routing-Tag"

As of LCOS version 9.18 RU1, the RADIUS client supports the vendor-specific RADIUS attribute "LCS-Routing-Tag" for PPTP, L2TP and PPPoE.

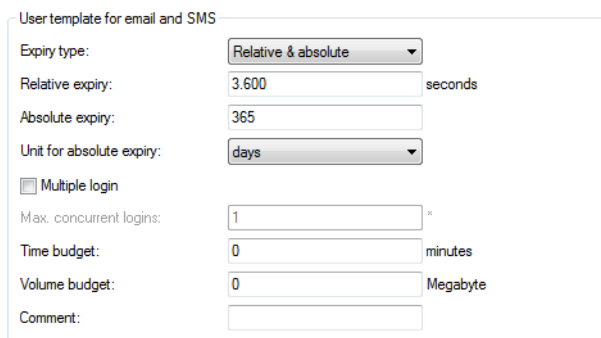
7 Public Spot

7.1 Shorter units for absolute expiry

As of LCOS version 9.18 RU1, Public Spot vouchers can be set with shorter units of time (days, hours, minutes). This is especially useful for scenarios with a high customer frequency in combination with short linger times.

7.1.1 Configuring shorter units with LANconfig

Shorter expiry times for Public Spots are configured in LANconfig under **Public Spot > Wizard**. In the "User template for e-mail and SMS" section, use the drop down menu to select the unit for the absolute expiry. Adjust the value for the absolute expiry if necessary.



The screenshot shows the 'User template for email and SMS' configuration window in LANconfig. It contains the following fields and settings:

- Expiry type:** A dropdown menu set to 'Relative & absolute'.
- Relative expiry:** A text input field containing '3.600' with a unit dropdown set to 'seconds'.
- Absolute expiry:** A text input field containing '365'.
- Unit for absolute expiry:** A dropdown menu set to 'days'.
- Multiple login:** A checkbox that is currently unchecked.
- Max. concurrent logins:** A text input field containing '1' with a '*' symbol to its right.
- Time budget:** A text input field containing '0' with a unit dropdown set to 'minutes'.
- Volume budget:** A text input field containing '0' with a unit dropdown set to 'Megabyte'.
- Comment:** An empty text input field.

7.2 Circuit ID as a Public Spot URL-redirect variable

As of LCOS version 9.18 RU1, the redirect variable "%d" enables you to display different welcome pages on authenticated clients, depending on their location.

7.2.1 Using the URL redirect variable

Enter the URL parameter '%d' as the circuit ID, for example `http://ipaddress/?circuit=%d&nas=%i`. The Public Spot module replaces this variable with the circuit ID that is detected in the client's DHCP request.

This requires "DHCP snooping" to be configured on the AP in such a way that the AP can query the circuit ID in the Public Spot station table of the WLC.

In this way it is possible for the Public Spot welcome page displayed on the clients to be customized by location.

7.3 Create Public Spot user on a remote Public Spot Gateway

As of LCOS version 9.18 RU1, you have the option of using the web-API to create a Public Spot user on a remote Public Spot-Gateway.

7.3.1 Create Public Spot user on a remote Public Spot Gateway

With Smart Ticket operating, each user is given a Public Spot account on the RADIUS server of the local Public Spot gateway.

However, where multiple Public Spot gateways operate with a single Gateway charging the user accounts on its RADIUS server, Smart Ticket causes the Public Spot account to be created on the central RADIUS server. To implement this, the remote Public Spot gateway needs to be specified in the LCOS menu tree under **Setup > Public Spot module > Authentication modules**.

 If no remote Public Spot gateway is specified, Public Spot user accounts are created on the local Public Spot gateway.

7.3.2 Additions to the Setup menu

Radius server

This menu specifies the settings used when creating Public Spot user accounts on the RADIUS server of a remote Public Spot gateway.

SNMP ID:

2.24.41.5

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules

Provider

Use this entry to specify the RADIUS server profile, which is located in the Public Spot provider table and references the RADIUS server of the remote Public Spot gateway.

SNMP ID:

2.24.41.5.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Modules > Radius-Server

Possible values:

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

Default:

empty

Name

Use this entry to specify which administrator account is used for creating user accounts on the remote Public Spot gateway.

SNMP ID:

2.24.41.5.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > Radius-Server****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`**Default:***empty***Password**

Use this entry to enter the password for the administrator account specified above.

SNMP ID:

2.24.41.5.3

Telnet path:**Setup > Public-Spot-Module > Authentication-Modules > Radius-Server****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]#@{ }~!$%&'()*+,-./:;<=>?[\]^_`~`**Default:***empty*

7.4 PMS template: Accept GTC

Depending on the configuration, authentication at a Public Spot optionally depends upon the acceptance of the general terms and conditions of use (GTC). In some combinations of login options (e.g. via stored reservation data or SMS authentication) the confirmation of the GTC was not clearly structured until now.

As of LCOS version 9.18 RU1, the appearance of the login page when using a combination of login methods has been redesigned.

7.5 Hiding fields in the setup wizard "Manage Public Spot Account"

As of LCOS version 9.18 RU1 you have the option of permanently hiding table columns in the wizard "Manage Public Spot Account".

7.5.1 Hiding fields in WEBconfig

In the setup wizard "Manage Public Spot Account", the **Show/hide column** button enables you to display or conceal columns of the table. These changes are only temporary. Hidden columns are shown again after a page refresh or in a new session.

If you want to permanently hide specific fields, use the LCOS menu tree and navigate to the view **Setup > Public Spot module > Manage user wizard**. All of the fields are displayed by default. If you hide certain fields, for example to

conceal the time budget, they will stay hidden in the wizard itself and also in the drop-down menu behind the button **Show/hide column** after reloading the page.



In order to delete authenticated Public Spot users, the columns "Calling station ID mask" and "Called station ID mask" need to be visible in the wizard. Unauthenticated users can be deleted even if these two columns are hidden.

Please note that hidden fields are not printed out when you press the **Print** button. On the other hand, exporting a CSV file includes all of the data. The **Save as CSV** button can optionally be hidden. To do this, use the LCOS menu tree to navigate to the view **Setup > Public Spot module > Add User Wizard > Hide CSV export**. Select "Yes" and save your entry.

Additions to the Setup menu

Show expiry type

This entry gives you the option to hide the "Expiry type" column in the Setup Wizard.

SNMP ID:

2.24.44.12

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:

Yes

The Setup Wizard shows the "Expiry type" column.

No

The Setup Wizard hides the "Expiry type" column.

Default:

Yes

Show abs. expiry

This entry gives you the option to hide the "Absolute expiry" column in the Setup Wizard.

SNMP ID:

2.24.44.13

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:

Yes

The Setup Wizard shows the "Absolute expiry" column.

No

The Setup Wizard hides the "Absolute expiry" column.

Default:

Yes

Show rel. expiry

This entry gives you the option to hide the "Relative expiry" column in the Setup Wizard.

SNMP ID:

2.24.44.14

Telnet path:**Setup > Public-Spot-Module > Manage-User-Wizard****Possible values:****Yes**

The Setup Wizard shows the "Relative expiry" column.

No

The Setup Wizard hides the "Relative expiry" column.

Default:

Yes

Show time budget

This entry gives you the option to hide the "Time budget" column in the Setup Wizard.

SNMP ID:

2.24.44.15

Telnet path:**Setup > Public-Spot-Module > Manage-User-Wizard****Possible values:****Yes**

The Setup Wizard shows the "Time budget" column.

No

The Setup Wizard hides the "Time budget" column.

Default:

Yes

Show volume budget

This entry gives you the option to hide the "Volume budget MByte" column in the Setup Wizard.

SNMP ID:

2.24.44.16

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Volume budget MByte" column.

No

The Setup Wizard hides the "Volume budget MByte" column.

Default:

Yes

Show case sensitive

This entry gives you the option to hide the "Case sensitive" column in the Setup Wizard.

SNMP ID:

2.24.44.17

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Case sensitive" column.

No

The Setup Wizard hides the "Case sensitive" column.

Default:

Yes

Show active

This entry gives you the option to hide the "Show active" column in the Setup Wizard.

SNMP ID:

2.24.44.18

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Show active" column.

No

The Setup Wizard hides the "Show active" column.

Default:

Yes

Show TX limit

This entry gives you the option to hide the "TX limit" (max. transmission bandwidth) column in the Setup Wizard.

SNMP ID:

2.24.44.19

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "TX limit" column.

No

The Setup Wizard hides the "TX limit" column.

Default:

Yes

Show RX limit

This entry gives you the option to hide the "RX limit" (max. receiving bandwidth) column in the Setup Wizard.

SNMP ID:

2.24.44.20

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "RX limit" column.

No

The Setup Wizard hides the "RX limit" column.

Default:

Yes

Show calling station

This entry gives you the option to hide the "Show calling station" column in the Setup Wizard.

SNMP ID:

2.24.44.21

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Show calling station" column.

No

The Setup Wizard hides the "Show calling station" column.

Default:

Yes

Show called station

This entry gives you the option to hide the "Show called station" column in the Setup Wizard.

SNMP ID:

2.24.44.22

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Show called station" column.

No

The Setup Wizard hides the "Show called station" column.

Default:

Yes

Show online time

This entry gives you the option to hide the "Online time" column in the Setup Wizard.

SNMP ID:

2.24.44.23

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Online time" column.

No

The Setup Wizard hides the "Online time" column.

Default:

Yes

Show traffic

This entry gives you the option to hide the "Traffic (Rx / Tx Kbyte)" column in the Setup Wizard.

SNMP ID:

2.24.44.24

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "Traffic (Rx / Tx Kbyte)" column.

No

The Setup Wizard hides the "Traffic (Rx / Tx Kbyte)" column.

Default:

Yes

Show status column

This entry gives you the option to hide the "Status" column in the Setup Wizard.

SNMP ID:

2.24.44.25

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:

Yes

The Setup Wizard shows the "Status" column.

No

The Setup Wizard hides the "Status" column.

Default:

Yes

Show MAC address

This entry gives you the option to hide the "MAC address" column in the Setup Wizard.

SNMP ID:

2.24.44.26

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:

Yes

The Setup Wizard shows the "MAC address" column.

No

The Setup Wizard hides the "MAC address" column.

Default:

Yes

Show IP address

This entry gives you the option to hide the "IP address" column in the Setup Wizard.

SNMP ID:

2.24.44.27

Telnet path:

Setup > Public-Spot-Module > Manage-User-Wizard

Possible values:**Yes**

The Setup Wizard shows the "IP address" column.

No

The Setup Wizard hides the "IP address" column.

Default:

Yes

7.6 Redirect for HTTPS connections switchable

To minimize the load on Public Spot gateways, LCOS version 9.18 RU1 introduced the option for HTTPS connections from unauthenticated clients to be redirected.

7.6.1 Redirect for HTTPS connections

If an unauthenticated client attempts to access an HTTPS website via an interface operated by the Public Spot, the connection request is redirected to the Public Spot gateway itself, which then presents the login page to the user. (This is also the case with HTTP). Usually, the user's browser displays a certificate warning, because the name or IP of the requested website is different from that of the Public Spot. To prevent this and the increased load on the Public Spot from the HTTPS/TLS connections, this setting is used to prevent HTTPS connections from being established for unauthenticated clients.

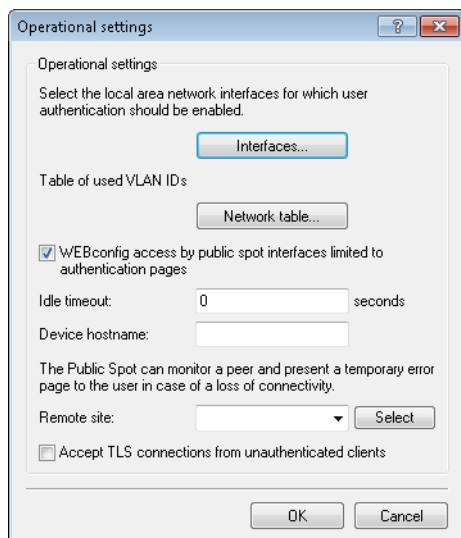


Once the client is authenticated, redirection is stopped and the client can establish any HTTP or HTTPS connection.

Modern clients carry out a "captive portal detection" via HTTP. The client attempts to access a certain URL via HTTP to check for the presence of a login page (from the Public Spot or other solutions). This mechanism is not affected by turning off the HTTPS redirect, since detection is usually via HTTP.

However, if unauthenticated WLAN clients should not perform connect requests over HTTP, this ineffective HTTPS redirect would place unnecessary load on the Public Spot gateway. For this reason it is possible to disable this HTTPS redirect. In this case, the user's browser displays a blank page.

In LANconfig, the HTTPS redirect is configured under **Public Spot > Server > Operational settings**.



To enable the HTTPS redirect, activate the option **Accept TLS connections from unauthenticated clients**. This option is disabled by default.

7.6.2 Additions to the Setup menu

Redirect TLS connections

Use this option to determine whether the Public Spot redirects HTTPS connections for unauthenticated clients. With this option disabled, unauthenticated clients are unable to establish HTTPS connections.

SNMP ID:

2.24.51

Telnet path:

Setup > Public-Spot-Module

Possible values:

No

The Public Spot does not perform HTTPS redirects for unauthenticated WLAN clients.

Yes

The Public Spot performs HTTPS redirects for unauthenticated WLAN clients.

Default:

No

7.7 Printout of bandwidth profile on the voucher

As of LCOS version 9.18 RU1, the voucher printout optionally shows the user-specific bandwidth profile. It is entered into the voucher template with this new template identifier:

BANDWIDTHPROFNAME**Valid for:**<pbelem>

This identifier contains the bandwidth profile that the user is associated with.



This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

RXBANDWIDTH**Valid for:**<pbelem>

This identifier contains the maximum reception bandwidth of the bandwidth profile.



This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

TXBANDWIDTH**Valid for:**<pbelem>

This identifier contains the maximum transmission bandwidth of the bandwidth profile.



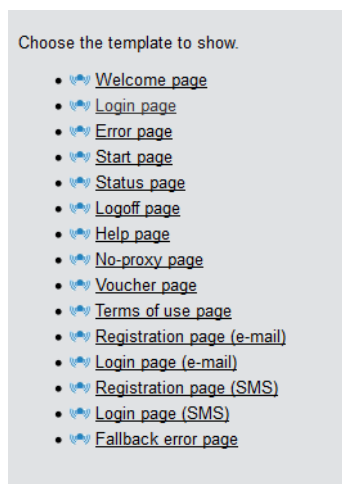
This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

7.8 Template preview

As of LCOS version 9.18 RU1 you have the option to preview the uploaded Public Spot templates.

7.8.1 Template preview in WEBconfig

You can view the changes to the Public Spot templates in WEBconfig by switching to the view **Extras > Public Spot template preview**.



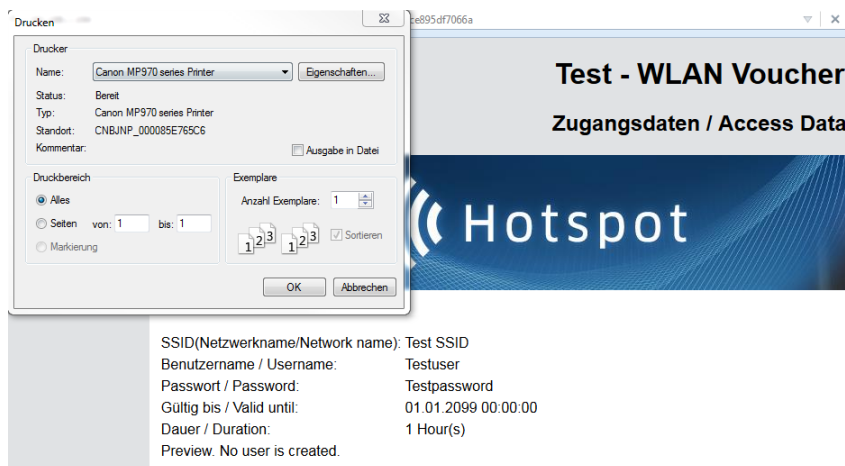
Select a template to display from the list.



The selected template is displayed in the same browser window. Use the "Back" function of your browser to return to WEBconfig.

Some templates contain JavaScript code. This code is executed when the template is invoked. For example, the "Voucher page" template contains code that starts a printout when the page is displayed.

This page contains test data. However, no user is created at this point. This allows you to test the template and print it out.



! If a template does not exist or cannot be found, an error message is displayed by WEBconfig.

7.9 Logging DNS requests and responses to external SYSLOG servers

As of LCOS version 9.18 RU1, it is possible to log the DNS requests and responses for the domains that are invoked by clients.

7.9.1 Logging DNS requests and responses to external SYSLOG servers

The DNS server in LANCOM devices resolves the DNS queries from clients. SYSLOG provides an overview of the clients, the names they requested, and the responses they received.

! It is not possible to use the router/AP's own internal SYSLOG. For this reason it is necessary to employ an external SYSLOG server.

DNS logging is configured in LANconfig under **IPv4 > DNS** in the section **SYSLOG**.

SYSLOG

DNS replies to clients can be logged to an external SYSLOG server.

☒ Log DNS resolutions to an external SYSLOG server

Server address:

Log the DNS resolutions on an external SYSLOG server

Select this option to enable the DNS logging.

i This option is independent of the setting in the SYSLOG module. Even if the SYSLOG module is disabled (setting under **Log & Trace > General** in the section **SYSLOG**), DNS logging is carried out nevertheless.

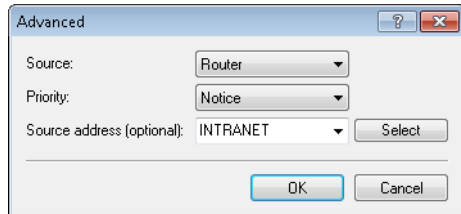
The corresponding SYSLOG message is structured as follows:

```
PACKET_INFO: DNS for <IP address>, TID {Hostname}: Resource-Record
```

Server address

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

The settings behind the button **Advanced** influence the content of SYSLOG messages.

**Source**

Contains the log source as displayed in the SYSLOG messages.

Priority

Contains the log level as displayed in the SYSLOG messages.

Source address (optional)

Contains the source address that is shown in the SYSLOG messages.

7.9.2 Additions to the Setup menu

Syslog

This directory is used to configure the SYSLOG output of DNS requests and responses for the domains that are invoked by clients.

SNMP ID:

2.17.20

Telnet path:

Setup > DNS

Log DNS resolutions

Enables or disables the logging of DNS requests and responses.



This option is independent of the setting in the SYSLOG module. DNS logging is still carried out even if the SYSLOG module is disabled (setting under **Setup > SYSLOG > Operating** set to "No").

The corresponding SYSLOG message is structured as follows:

```
PACKET_INFO: DNS for <IP address>, TID {Hostname}: Resource-Record
```

SNMP ID:

2.17.20.1

Telnet path:

Setup > DNS > Syslog

Possible values:**No**

Disables the logging of DNS requests.

Yes

Enables the logging of DNS requests.

Default:

No

Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.



In general the IP addresses 127.0.0.1 and ::1 are rejected, so as to force the use of an external server.

SNMP ID:

2.17.20.2

Telnet path:

Setup > DNS > Syslog

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-: %`

Log source

Contains the log source as displayed in the SYSLOG messages.

SNMP ID:

2.17.20.3

Telnet path:

Setup > DNS > Syslog

Possible values:

System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

Router

Log level

Contains the log level as displayed in the SYSLOG messages.

SNMP ID:

2.17.20.4

Telnet path:

Setup > DNS > Syslog

Possible values:

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Default:

Notice

Loopback-Addr.

Source address shown in the SYSLOG messages.

SNMP ID:

2.17.20.5

Telnet path:

Setup > DNS > Syslog

Possible values:

Max. 16 characters from `[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

LB0 to LBF for the 16 loopback addresses

Any valid IP address

Facility

The mapping of sources to specific facilities.

SNMP ID:

2.22.3.2

Telnet path:

Setup > SYSLOG > Facility-Mapper

Possible values:

**KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7**

IP address

The mapping of the IP address to specific facilities.

SNMP ID:

2.22.2.7

Telnet path:**Setup > SYSLOG > SYSLOG table****Possible values:**Max. 64 characters from `[A-Z][a-z][0-9].-: %`

7.10 Protection against brute force attacks

Starting with version 9.18 RU1, LCOS provides protection against brute-force attacks on the Public Spot.

7.10.1 Protection against brute force attacks

Brute force attacks are the most common type of attack on networks. This method of attack tries out a variety of potential passwords in the shortest possible time, until the right one is found. One form of protection against brute-force attacks is to react to one or more successive failed attempts by delaying the time until the entry is allowed to be attempted again.

Configure the protection against brute-force attacks in LANconfig under **Public Spot > Server** in the section **Brute force protection**.

Brute force protection	
Lock after:	<input type="text" value="10"/> failed attempts
Lock duration:	<input type="text" value="60"/> minutes

Lock after

Specify how many unsuccessful attempts are permitted before the entry lock takes effect.

Lock duration

Specify for how long the entry lock is to apply.

You can use the console to display the current status of the brute-force protection with the command `show pbbruteprotector`:

show pbbruteprotector

Shows all of the MAC addresses that are associated with the Public Spot.

show pbbruteprotector [MAC address [MAC address [...]]

Specifying one or more space-separated MAC addresses shows the status of all of the respective MAC addresses.



The MAC address is specified in the format `11 : 22 : 33 : 44 : 55 : 66`, `11-22-33-44-55-66` or `112233445566`.

7.10.2 Additions to the Setup menu

Brute force protection

This menu contains the settings for the brute-force protection used by the Public Spot.

SNMP ID:

2.24.49

Telnet path:**Setup > Public-Spot-Module****Max. login tries**

Specify how many unsuccessful attempts are permitted before the login block takes effect.

SNMP ID:

2.24.49.1

Telnet path:**Setup > Public-Spot-Module > Brute-Force-Protection****Possible values:**

Max. 3 characters from [0–9]

Default:

10

Blocking time in minutes

Specify how long the login block of the brute-force protection applies.

SNMP ID:

2.24.49.2

Telnet path:**Setup > Public-Spot-Module > Brute-Force-Protection****Possible values:**

Max. 5 characters from [0–9]

Default:

60

Unblocking check in seconds

Specify the interval after which the AP checks for the expiry of a login block for a MAC address.

SNMP ID:

2.24.49.3

Telnet path:**Setup > Public-Spot-Module > Brute-Force-Protection****Possible values:**

Max. 5 characters from [0-9]

Default:

60

Unblock

Use this action to remove the login block on a MAC address. Enter the parameters as one or more space-separated MAC addresses.



The MAC address is specified in the format 11 : 22 : 33 : 44 : 55 : 66, 11-22-33-44-55-66 or 112233445566.

SNMP ID:

2.24.49.4

Telnet path:**Setup > Public-Spot-Module > Brute-Force-Protection**

8 Routing and WAN connections

8.1 Route monitor

As of LCOS version 9.18 RU1, a route monitor checks the network connections to a specified prefix. This prefix is learned, for example as the result of a dynamic routing protocol such as BGP.

In case of a faulty connection, the route monitor opens a backup connection, if required.

8.1.1 Route monitor

The route monitor observes the connections to the networks of different providers and establishes a backup connection in case of failure. The monitoring makes use of a trigger prefix, which providers supply in their routing protocol, for example with the Border Gateway Protocol (BGP). As soon as a route to a provider's network becomes unavailable, the route monitor declares the relevant trigger prefix to be invalid for its network and opens a backup connection to the provider's network.

In LANconfig, the route monitor is configured under **Communication > Call management**.

Activate the check box **Route monitor active**. Now click the button **Route monitor table**.

Add a new entry to the table and enable the **Active** check box to enable this backup connection.

Set the following parameters:

Remote site

Contains the name of the backup remote station.

Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

Routing-Tag

Contains the routing tag of the prefix being monitored.

Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

Comment

Contains a comment on this entry.

8.1.2 Additions to the Setup menu

Route monitor

In this directory, you configure the route monitor.

SNMP ID:

2.93.2

Telnet path:

Setup > Routing-protocols

Monitor table

In this table, you configure the route monitor.

SNMP ID:

2.93.2.1

Telnet path:

Setup > Routing-protocols > Route-monitor

Backup peer

Contains the name of the backup remote station.

SNMP ID:

2.93.2.1.1

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:**Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-;/:<=>?[\]^_.`**Default:***empty***Prefix**

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

SNMP ID:

2.93.2.1.2

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:**Max. 43 characters from `[A-F][a-f][0-9]:./`**Default:***empty***Rtg-Tag**

Contains the routing tag of the prefix being monitored.

SNMP ID:

2.93.2.1.3

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:**Max. 5 characters from `[0-9]`**Default:**

0

Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

SNMP ID:

2.93.2.1.4

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:**

Max. 10 characters from [0–9]

Default:

20

Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

SNMP ID:

2.93.2.1.5

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:**

Max. 10 characters from [0–9]

Default:

0

Special values:**0**

No delay: The device immediately closes the connection to the backup peer when the prefix arrives.

Active

Specifies whether this backup connection is enabled.

SNMP ID:

2.93.2.1.6

Telnet path:**Setup > Routing-protocols > Route-monitor > Monitor-table****Possible values:****Yes**

The backup connection is enabled.

No

The backup connection is disabled.

Default:

No

Comment

Comment on this entry.

SNMP ID:

2.93.2.1.7

Telnet path:

Setup > Routing-protocols > Route-monitor > Monitor-table

Possible values:

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

Default:

empty

Operating

This action is used to enable or disable the route monitor.

SNMP ID:

2.93.2.2

Telnet path:

Setup > Routing-protocols > Route-monitor

Possible values:**No**

The route monitor is disabled.

Yes

The route monitor is enabled.

Default:

No

8.2 DiffServ field enabled by default

As of LCOS version 9.18 RU1, the Routing Method in the LCOS menu tree under **Setup > IP router > Routing method** observes the DiffServ field by default. Consequently, the routing method DiffServ is enabled by default.

8.2.1 Additions to the Setup menu

Routing method

Controls the analysis of ToS or DiffServ fields.

SNMP ID:

2.8.7.1

Telnet path:

Setup > IP-Router > Routing-Method

Possible values:

Normal

The TOS/DiffServ field is ignored.

Type of service

The TOS/DiffServ field is regarded as a TOS field; the bits "low delay" and "high reliability" will be evaluated.

DiffServ

The TOS/DiffServ field is regarded as a DiffServ field and evaluated as follows.

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

Default:

DiffServ

9 Other services

A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Office communications with LANCAPI
- Time server

9.1 IPv6 support for (S)NTP client and server

LCOS version 9.18 RU1 supports IPv6 for the (S)NTP client and server.