



Addendum LCOS 8.82

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Contents

1 Addendum to LCOS version 8.82.....	4
2 Routing and WAN connections.....	5
2.1 DNS forwarding configurable per ARF context.....	5
2.1.1 Advanced Routing and Forwarding (ARF).....	5
2.1.2 Additions to the Setup menu.....	7
2.2 Source tags for firewall rules.....	8
2.2.1 Additions to the Setup menu.....	8
3 VPN.....	9
3.1 Hash function SHA2-256 selectable via LANconfig.....	9
3.1.1 An overview of LANCOM VPN.....	9
3.1.2 Additions to the Setup menu.....	9
4 RADIUS.....	11
4.1 Input length for RADIUS forwarding destinations.....	11
4.1.1 Additions to the Setup menu.....	11
4.2 Bandwidth allocation by RADIUS.....	12
4.2.1 Extensions to the RADIUS server.....	12
4.2.2 Additions to the Status menu.....	14
5 WLAN management.....	15
5.1 Band steering via WLAN controller.....	15
5.1.1 Enhancements to LANconfig.....	15
5.1.2 Additions to the Setup menu.....	18
6 WLAN.....	20
6.1 Advanced ARP handling.....	20
6.1.1 Additions to the Status menu.....	20
6.2 Multicast and broadcasts in cells can be switched off.....	23
6.2.1 Additions to the Setup menu.....	23
6.2.2 Enhancements to LANconfig.....	23
6.3 IEEE 802.11u and Hotspot 2.0.....	26
6.3.1 Hotspot operators and service providers.....	27
6.3.2 Functional description.....	27
6.3.3 Recommended general settings.....	28
6.3.4 Enhancements to LANconfig.....	29
6.3.5 Additions to the Setup menu.....	40
7 Public Spot.....	61
7.1 Template variables.....	61
7.2 Customizing the standard pages.....	61
7.2.1 Customized text on the login page.....	61
7.2.2 Custom header images for variable screen widths.....	62
7.2.3 Additions to the Setup menu.....	64
7.3 Independent user registration - simple Login.....	64

7.3.1 Independent user authentication (Smart Ticket).....	64
7.3.2 Enhancements to LANconfig.....	65
7.3.3 Additions to the Setup menu.....	67
7.4 Bandwidth profile.....	69
7.4.1 Enhancements to LANconfig.....	69
7.4.2 Additions to the Setup menu.....	70
7.5 Dynamic VLAN assignment via RADIUS.....	71
7.5.1 Enhancements to LANconfig.....	71
7.5.2 Additions to the Setup menu.....	72
7.6 Automatic re-login.....	73
7.6.1 Additions to the Setup menu.....	74
7.6.2 Additions to the Status menu.....	76
7.7 Login via WISPr.....	76
7.7.1 Automatic authentication via WISPr.....	76
7.7.2 Enhancements to LANconfig.....	78
7.7.3 Additions to the Setup menu.....	79
7.8 PMS interface.....	81
7.8.1 Interface for property management systems.....	82
7.8.2 Functional description.....	83
7.8.3 Enhancements to LANconfig.....	84
7.8.4 Additions to the Status menu.....	86
7.8.5 Additions to the Setup menu.....	87
8 LCMS.....	97
8.1 SSH configuration protocol in LANconfig.....	97
8.1.1 Enhancements to LANconfig.....	97
9 IPv6.....	104
9.1 Reconfigure function of the DHCPv6 server.....	104
9.1.1 Enhancements to LANconfig.....	104
9.1.2 Additions to the Setup menu.....	109
9.1.3 Additions to the Status menu.....	110
10 Diagnosis.....	111
10.1 SYSLOG: Configuration of the retention period for system events.....	111
10.1.1 Additions to the Setup menu.....	111
10.1.2 Enhancements to LANconfig.....	111
10.2 SYSLOG: Extension of log entries of the internal SYSLOG server.....	112
10.3 SYSLOG: Extended status display of the login to the cellular network.....	112
10.3.1 Extended status display of the login to the cellular network.....	113
10.3.2 Additions to the Status menu.....	114

1 Addendum to LCOS version 8.82

This document describes the changes and enhancements in LCOS Version 8.82 since the previous version.

2 Routing and WAN connections

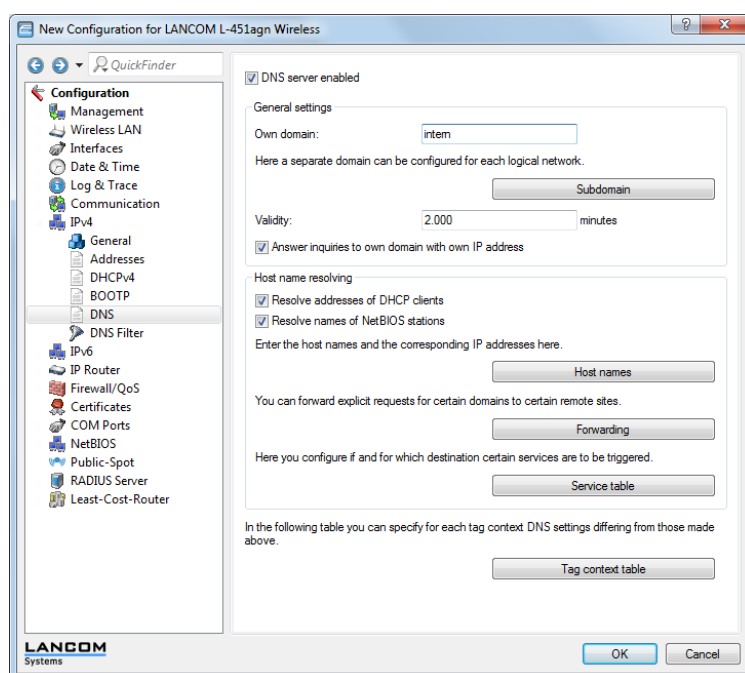
2.1 DNS forwarding configurable per ARF context

As of LCOS version 8.82 multiple independent forwarding definitions (especially general wildcard definitions with "**") are possible for DNS forwarding by identifying them with unique routing tags. Depending on the routing context of the requesting client, the router considers only the forwarding entries that are identified accordingly and the general entries marked with "0".

2.1.1 Advanced Routing and Forwarding (ARF)

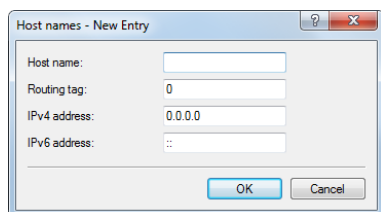
Routing tags for DNS forwarding

For DNS forwarding, multiple independent forwarding definitions (especially general wildcard definitions with "**") are possible for DNS forwarding by identifying them with unique routing tags. Depending on the routing context of the requesting client, the router considers only the forwarding entries that are identified accordingly and the general entries marked with "0".



Host names

The item **Configuration > IPv4 > DNS > Host names** is used to define the tag context and IP number used by the device to resolve the station names.



Host names - New Entry

Host name:

Routing tag:

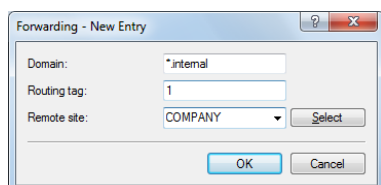
IPv4 address:

IPv6 address:

OK Cancel

DNS forwarding

The item **Configuration > IPv4 > DNS > Forwarding** is used to set the routing tags for the forwarding rules, so ensuring they only apply when the correct routing tags are used.



Forwarding - New Entry

Domain:

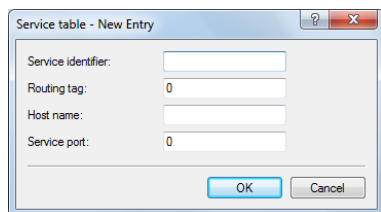
Routing tag:

Remote site:

OK Cancel

Service table

The item **Configuration > IPv4 > DNS > Service table** is used to assign routing tags to the services, so ensuring that they are only available when the correct routing tags are used.



Service table - New Entry

Service identifier:

Routing tag:

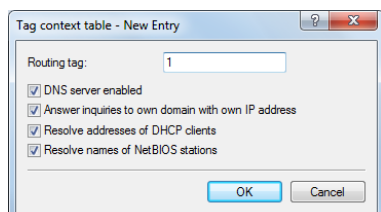
Host name:

Service port:

OK Cancel

Tag context table

It is possible to define tag contexts in LANconfig under **Configuration > IPv4 > DNS > Tag context table**, which override the global settings of the DNS server for specific interface and routing tags (routing context):



Tag context table - New Entry

Routing tag:

☒ DNS server enabled

☒ Answer inquiries to own domain with own IP address

☒ Resolve addresses of DHCP clients

☒ Resolve names of NetBIOS stations

OK Cancel

If an entry for a tag context exists, then only the DNS settings in this table apply for this context. However, if there is no entry in this table, then the global settings of the DNS server apply.

The following options are possible for each tag context:

- **Routing tag:** Unique interface or routing tag in the range of 1 to 65535, the subsequent settings will override the global settings of the DNS server.
- **DNS server enabled:** Enables the DNS server of the device.

- **Answer inquiries to own domain with own IP address:** If enabled, DNS requests relating to the router's own domain will be answered with the router's IP address.
- **Resolve addresses of DHCP clients:** Enables resolution of station names that have requested an IP address through DHCP.
- **Resolve names of NetBIOS stations:** Enables resolution of station names that are known to the NetBIOS router.

2.1.2 Additions to the Setup menu

Routing tag

When resolving a station name, the device uses the routing tag to set the tag context for that station.

SNMP ID:

2.17.5.4

Telnet path:

Setup > DNS > DNS-List

Possible values:

0 to 65535

Default:

0

Routing tag

The routing tag determines which filters apply in each tag context.

SNMP ID:

2.17.6.6

Telnet path:

Setup > DNS > Filter-List

Possible values:

0 to 65535

Default:

0

Routing tag

The routing tag makes it possible to specify multiple forwarding definitions that are independent of each other (especially general wildcard definitions with "*"). Depending on the routing context of the requesting client, the router considers only the forwarding entries that are identified accordingly and the general entries marked with "0".

SNMP ID:

2.17.9.3

Telnet path:

Setup > DNS > DNS-Destinations

Possible values:

0 to 65535

Default:

0

Routing tag

The routing tag determines whether and how the router should resolve specific service requests within the current tag context.

SNMP ID:

2.17.10.4

Telnet path:

Setup > DNS > Service-Location-List

Possible values:

0 to 65535

Default:

0

2.2 Source tags for firewall rules

2.2.1 Additions to the Setup menu

Source tag

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received. This can be used to restrict firewall rules to certain ARF contexts.

SNMP ID:

2.8.10.2.15

Telnet path:

Setup > IP-Router > Firewall > Rules

Possible values:

0 - 65535

Comment

- 65535: The firewall rule is applied if the expected interface- or routing tag is 0.
- 1 - 65534: The firewall rule is applied if the expected interface- or routing tag is 1...65534.
- 0: Wildcard. The firewall rule is applied to all ARF contexts (the expected interface- or routing tag is 0...65535).

Default:

0

3 VPN

3.1 Hash function SHA2-256 selectable via LANconfig

As of LCOS version 8.82, you can also select the hash algorithm SHA-2-256 for IKE and IPSec proposals over LANconfig for devices that are equipped appropriately.

3.1.1 An overview of LANCOM VPN

Functions of LANCOM VPN

This section lists all of the functions and properties of LANCOM VPN. Experts in the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the LANCOM VPN, this information is not required.

- VPN according to IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- IKE Main and Aggressive mode
- LANCOM Dynamic VPN: Public IP addresses can be static or dynamic (establishing a connection with remote sites using dynamic IP addresses requires ISDN)
- IPSec protocols ESP, AH and IPCOMP in transport and Tunnel mode
- Hash algorithms:
 - HMAC-MD5-96, hash length 128 bits
 - HMAC-SHA-1-96, hash length 160 bits
 - HMAC-SHA-2-256, hash length 256 bits
- Symmetrical encryption methods
 - AES, key lengths of 128, 192 and 256 bits
 - Triple DES, Key length 168 bits
 - Blowfish, key length 128 - 448 bits
 - CAST, key length 128 bits
 - DES, key length 56 bits
- Compression with "Deflate" (ZLIB) and LZS
- IKE config mode
- IKE with preshared keys
- IKE with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with a key length of 768 bits, 1024 bits, 1536 bits and 2048 bits (well known groups 1, 2, 5 und 14)
- Key management according to ISAKMP

3.1.2 Additions to the Setup menu

IKE authentication algorithm

Hash algorithm for the encryption

SNMP ID:

2.19.4.11.4

Telnet path:

Setup > VPN > Proposals > IKE

Possible values:

MD5

SHA1

SHA2-256

Default:

MD5

ESP authentication algorithm

ESP authentication method for this proposal

SNMP ID:

2.19.4.12.5

Telnet path:

Setup > VPN > Proposals > IPSEC

Possible values:

No authentication

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

No authentication

AH authentication algorithm

AH authentication method for this proposal

SNMP ID:

2.19.4.12.6

Telnet path:

Setup > VPN > Proposals > IPSEC

Possible values:

No authentication

HMAC-MD5

HMAC-SHA1

HMAC-SHA2-256

Default:

No authentication

4 RADIUS

4.1 Input length for RADIUS forwarding destinations

As of LCOS version 8.82, realms can be up to 64 characters long, in order to use roaming providers with long realms.

4.1.1 Additions to the Setup menu

Realm

String with which the RADIUS server identifies the forwarding destination.

SNMP ID:

2.25.10.3.1

Telnet path:

Setup > RADIUS > Server > Forward-Server

Possible values:

Max. 64 characters

Default:

Blank

Backup

Alternative routing server that the RADIUS server forwards requests to when the first routing server is not reachable.

SNMP ID:

2.25.10.3.5

Telnet path:

Setup > RADIUS > Server > Forward-Server

Possible values:

Max. 64 characters

Default:

Blank

Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

SNMP ID:

2.25.10.5

Telnet path:

Setup > RADIUS > Server

Possible values:

Max. 64 characters

4 RADIUS

Default:

Blank

Empty realm

This realm is used when the specified username does not contain a realm.

SNMP ID:

2.25.10.6

Telnet path:**Setup > RADIUS > Server****Possible values:**

Max. 64 characters

Default:

Blank

4.2 Bandwidth allocation by RADIUS

As of LCOS version 8.82, the LANCOM RADIUS server can assign each registered client a bandwidth limitation regardless of the interface used. Up until now, that was only possible for Public Spot scenarios if the Public Spot gateway and the associated WLAN interface were both enabled on the same device.

4.2.1 Extensions to the RADIUS server

RADIUS user

You can enter up to 64 users in the user database that the RADIUS server can authenticate without needing other databases. This user table uses the RADIUS server for local requests, also for requests with usernames without a realm.

- **Name:** Enter the name of the user
- **Please note that the username is case-sensitive:** When enabled, the RADIUS server distinguishes between uppercase and lowercase. "User12345" and "user12345" are therefore two different users.
- **Password:** User password.

- **VLAN ID:** ID of the logical subnet
- **Comment:** Additional information about the user
- **Service type:** The service type is a special attribute of the RADIUS protocol, which the NAS (Network Access Server) transmits with the authentication request. The request will only receive a positive response if the requested service type fits the service type of the user account. Possible values include:
 - `Any`: The service type can be any type.
 - `Framed`: For checking WLAN MAC addresses via RADIUS or IEEE 802.1x.
 - `Login`: For Public-Spot logins.
 - `Authentication only`: For RADIUS authentication of dialup peers via PPP.



Please note that, depending on the device, the number of entries can be limited with the service type `Any` or `Login`. If your device, for example, is able to manage a total of 64 Public Spot users, the LANconfig rejects them after 64. User account with the service type `Any/Login` requires the creation of additional user accounts with these service types.

- **Protocol restriction:** This option limits the selection of authentication methods allowed for the user. Possible values include:
 - `PAP`
 - `CHAP`
 - `MSCHAP`
 - `MSCHAPv2`
 - `EAP`
- **Passphrase:** Associated WPA passphrase of the registered user
- **TX bandwidth limit:** Bandwidth limitation for sending data
- **RX bandwidth limit:** Bandwidth limitation for receiving data



The bandwidth limitation for sending and receiving applies regardless of the interface used (LAN and WLAN).

- **Calling station:** This mask limits the validity of the entry to certain IDs transmitted by the calling station (WLAN client). When authenticating via 802.1x the calling station's MAC address is transmitted in ASCII format (capital letters only) with a hyphen separating pairs of characters (for example, "00-10-A4-23-19-C0").
- **Called station:** This mask limits the validity of the entry to specified IDs as transmitted by the called station (BSSID and SSID of the access point). When authenticating via 802.1x the called station's MAC address (BSSID) is transmitted in ASCII format (capital letters only) with a hyphen separating pairs of characters. The SSID is appended using a colon as a separator (e.g., "00-10-A4-23-19-C0:AP1").
- **Expiry type:** This option specifies the type of the validity period of the user account. Possible values include:
 - `Relative & absolute:`
 - `Relative`
 - `Absolute`
 - `Never`
- **Relative expiry:** Validity period in seconds from the initial successful login
- **Absolute expiry:** Validity period in hours, minutes and seconds from a certain date
- **Multiple login:** Activates the option for the client to register more than once
- **Maximum number:** Maximum number of concurrent logins by the client
- **Time budget:** Specifies the time in seconds available to the client.
- **Volume budget:** Specifies the data volume available to the client.

4.2.2 Additions to the Status menu

Station table

This table contains the bandwidth allocations for the clients registered on the RADIUS server, regardless of the interface that the clients are connected to.

SNMP ID:

1.5.90

Telnet path:

Status > LAN

Interface

Interface to which the client is connected.

MAC address

MAC address of the client

Tx limit

Bandwidth limitation for the reception of data.

Rx limit

Bandwidth limitation for sending data.

VLAN ID

VLAN ID of the network over which the client communicates.

5 WLAN management

5.1 Band steering via WLAN controller

As of LCOS version 8.82, WLAN controllers can manage settings for band steering for the access points in the radio profiles.

5.1.1 Enhancements to LANconfig

Configuration

Most of the parameters for configuring the LANCOM WLAN controller correspond with those of the access points. For this reason, this section does not explicitly describe all of the WLAN parameters, but only those aspects necessary for operating the WLAN controller.

Profiles

The profiles area is used to define the logical WLAN networks, physical WLAN parameters, and the WLAN profiles which combine these two elements.

Logical WLAN networks

Here the logical WLAN networks are set for assignment to the access points. The following parameters can be defined for each logical WLAN network:

LANconfig: **WLAN controller > Profiles > Logical WLAN networks**

WEBconfig: **LCOS Menu Tree > Setup > WLAN-Management > AP-Configuration > Network profiles**

- **Network name (SSID)**

Name of the logical WLAN network under which the settings are saved. This name is only used for internal administration of logical networks.

■ **Inheritance**

Selection of a logical WLAN network defined earlier and from which the settings are to be inherited.

■ **SSID connect to**

Service Set Identifier – the name under which the logical WLAN network is offered to the WLAN clients.

■ **VLAN-ID**

VLAN ID for this logical WLAN network



Please note that to use VLAN IDs in a logical WLAN network, you must set up a management VLAN ID (see physical WLAN parameters).

■ **AP standalone time**

The time in minutes that a managed-mode access point continues to operate in its current configuration.

The configuration is provided to the access point by the WLAN controller and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN controller be interrupted, the access point will continue to operate with the configuration stored in flash for the time period entered here. The access point can also continue to work with this flash configuration after a local power outage.

If there is still no connection to the WLAN controller after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLAN controller is available again, the configuration is transmitted again from the WLAN controller to the access point.

This option enables an access point to continue operating even if the connection to the WLAN controller is temporarily interrupted. Furthermore this represents an effective measure against theft as all security-related configuration parameters are automatically deleted after this time has expired.



If the access point establishes a backup connection to a secondary WLAN controller, then the countdown to the expiry of standalone operation is halted. The access point and its WLAN networks remain active as long as it has a connection to a WLAN controller.



Please note that the configuration in flash memory is deleted only after expiry of the time for standalone operation, and not when the power is lost!

■ **Minimum client signal strength**

This entry determines the threshold, in percentage, for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, since the list does not contain any access points that would offer a weak connection at the client's current position.



All other WLAN network parameters correspond to those for the standard configuration of access points.

Physical WLAN parameters

Here the physical WLAN parameters are set for assignment to the access points. The following parameters can be defined for each set of physical WLAN parameters:

LANconfig: **WLAN Controller > Profiles > Physical WLAN parameters**

WEBconfig: **LCOS Menu Tree > Setup > WLAN management > AP configuration > Radio profiles**

■ Name

Unique name for this combination of physical WLAN parameters.

■ Inheritance

Selection of a physical WLAN parameter set defined earlier and from which the settings are to be inherited.

■ Country

The country in which the access points are to be operated. This information is used to define country-specific settings such as the permitted channels, etc.

■ Automatic channel selection

By default, the access points can use all of the channels permitted in the country of operation. To restrict the selection to certain channels, these can be entered here as a comma-separated list. It is also possible to specify ranges or lists (e.g. '1,6,11').

■ Management VLAN-ID

The VLAN ID of the management network that is to manage the access points.

! The Management VLAN ID **must** be set to a value not equal to zero in order for VLANs to be used over the WLAN networks. This also applies when the management network itself is not to be tagged with VLAN IDs (Mgmt-VLANID=1).

! VLAN activation only applies to WLAN networks which are connected by means of these physical WLAN parameters.

■ Band steering activated

This entry determines whether the access point should enable band steering. In this case, a dual-port access point can forward a WLAN client to a preferred frequency band.

! All other physical WLAN parameters correspond to those for the standard configuration of access points.

! To successfully acquire a profile, HTTP access to the WLAN controller from the local network must be allowed.

5.1.2 Additions to the Setup menu

Report seen clients

This entry determines whether the access point should report clients detected in the WLAN network.

SNMP ID:

2.37.1.2.20

Telnet path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:

Yes

No

Default:

Yes

Client steering

This entry determines whether the access point should enable band steering.

SNMP ID:

2.37.1.2.21

Telnet path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:

Yes

No

Default:

No

Preferred band

This entry determines the frequency band that the access point preferably should direct the WLAN client.

SNMP ID:

2.37.1.2.22

Telnet path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:

5GHz

2.4GHz

Default:

5GHz

Probe request ageout in seconds

This entry determines the length of time in seconds that the access point should store a WLAN client's connection. When this time expires, the access point deletes the entry from the table.



This value should be set to a low value if you are using clients in the WLAN that frequently switch from dual-band to single-band mode.

SNMP ID:

2.37.1.2.23

Telnet path:

Setup > WLAN-Management > AP-Configuration > Radioprofiles

Possible values:

max. 10 characters from 0 to 9

Special values:

0: The access point immediately considers seen probe requests as invalid.

Default:

120

Minimum client strength

This entry determines the threshold, in percentage, for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, since the list does not contain any access points that would offer a weak connection at the client's current position.

SNMP ID:

2.37.1.1.36

Telnet path:

Setup > WLAN-Management > AP-Configuration > Network-Profiles

Possible values:

max. 3 characters from 0 to 9

Default:

0

6 WLAN

6.1 Advanced ARP handling

As of LCOS version 8.82, access points can store more than one IP address per WLAN client.

6.1.1 Additions to the Status menu

ARP handling

This menu displays both IPv4 and IPv6 information about the WLAN clients detected in the WLAN cell.



The access point can store multiple IP addresses per WLAN client in these tables, especially in IPv6 networks. If there are several IP addresses for each WLAN client, the entry in the WLAN station table (**Setup > WLAN > Station-Table**) points to the most recently identified IP address.

SNMP ID:

1.3.62

Telnet path:

Status > WLAN

ARP Table

This table contains IPv4 information about the WLAN clients detected in the WLAN cell.

SNMP ID:

1.3.62.1

Telnet path:

Status > WLAN > ARP-Handling

Address

Contains the stored IPv4 address of the WLAN client.

MAC address

Contains the associated MAC address of the WLAN client.

Interface

Contains the SSID with which the WLAN client is connected.

VLAN ID

Contains the VLAN ID on which the WLAN client is connected.

Age

Contains the time, in seconds, since the access point last identified the WLAN client.



The access point only deletes entries in this table if it no longer detects the corresponding WLAN client in the WLAN cell.



In this table, it is possible that the access point stores multiple IP addresses for a WLAN client (or several WLAN clients with the same IP address), in order to identify, for example, address conflicts.

ND table

This table contains IPv6 information about the WLAN clients detected in the WLAN cell.

SNMP ID:

1.3.62.2

Telnet path:

Status > WLAN > ARP-Handling

Address

Contains the stored IPv6 address of the WLAN client.

MAC address

Contains the associated MAC address of the WLAN client.

Interface

Contains the SSID with which the WLAN client is connected.

VLAN ID

Contains the VLAN ID on which the WLAN client is connected.

Age

Contains the time, in seconds, since the access point last identified the WLAN client.



The access point only deletes entries in this table if it no longer detects the corresponding WLAN client in the WLAN cell.



In this table, it is possible that the access point stores multiple IP addresses for a WLAN client (or several WLAN clients with the same IP address), in order to identify, for example, address conflicts.

ARP requests answered

This entry shows the number of ARP requests that the access point successfully and directly answered without the request having been previously sent to the WLAN cell.

SNMP ID:

1.3.62.11

Telnet path:

Status > WLAN > ARP-Handling

ARP requests not answered

This entry indicates the number of ARP requests not directly answered by the access point. Instead, the access point had to forward this request to the WLAN cell first.

SNMP ID:

1.3.62.12

Telnet path:

Status > WLAN > ARP-Handling

ARP requests rejected

This entry shows the number of ARP requests rejected by the access point. Reasons for this may include:

- The access point has already answered this request over a different interface.
- The access point has classified this request as an unnecessary ARP check.
- The request does not match the VLAN override of the WLAN client.

SNMP ID:

1.3.62.13

Telnet path:

Status > WLAN > ARP-Handling

ND searches answered

This entry shows the number of ND requests that the access point successfully and directly answered without the request having been previously sent to the WLAN cell.

SNMP ID:

1.3.62.14

Telnet path:

Status > WLAN > ARP-Handling

ND searches not answered

This entry indicates the number of ND requests not directly answered by the access point. Instead, the access point had to forward this request to the WLAN cell first.

SNMP ID:

1.3.62.15

Telnet path:

Status > WLAN > ARP-Handling

ND searches rejected

This entry shows the number of ND requests rejected by the access point. Reasons for this may include:

- The access point has already answered this request over a different interface.
- The access point has classified this request as a DAD query (Duplicate Address Detection).
- The request does not match the VLAN override of the WLAN client.

SNMP ID:

1.3.62.16

Telnet path:

Status > WLAN > ARP-Handling

Delete values

This action deletes all stored values in the ARP or ND tables.

SNMP ID:

1.3.62.99

Telnet path:

Status > WLAN > ARP-Handling

6.2 Multicast and broadcasts in cells can be switched off

According to the HotSpot 2.0 specification, as of LCOS version 8.82 it is possible to switch off multicasts and broadcasts in cells.

6.2.1 Additions to the Setup menu

Transmit only unicasts

Multicast and broadcast transmissions within a WLAN cell cause a load on the bandwidth of the cell, especially since the WLAN clients often do not know how to handle these transmissions. The access point already intercepts a large part of the multicast and broadcast transmissions in the cell with ARP spoofing. With the restriction to unicast transmissions it filters out unnecessary IPv4 broadcasts from the requests, such as Bonjour or NetBIOS.

The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

SNMP ID:

2.23.20.1.19

Telnet path:

Telnet path: Setup > Interfaces > WLAN > Network

Possible values:

Yes

No

Default:

No

6.2.2 Enhancements to LANconfig

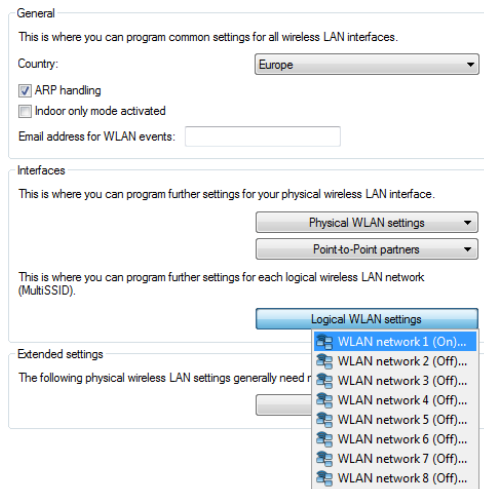
Configuration of WLAN parameters

The settings for the cellular networks are made at various points in the configuration:

- Some parameters concern the physical WLAN interfaces. Some LANCOM models have just one WLAN interface (single radio access point), and others have a second WLAN module integrated (dual radio access point). The settings for the physical WLAN interfaces apply to all of the logical cellular networks supported by this module. These parameters include, for example, the transmission power of the antenna and the operating mode of the WLAN module (access point or client).
- Other parameters are only related to the Logical cellular networks, which are supported by a physical interface. These include, for example, the SSID or the activation of encryption, such as 802.11i with AES.
- A third group of parameters affect the wireless network operation, but are not significant only to WLANs. These include, for example, the protocol filter in the LAN bridge.

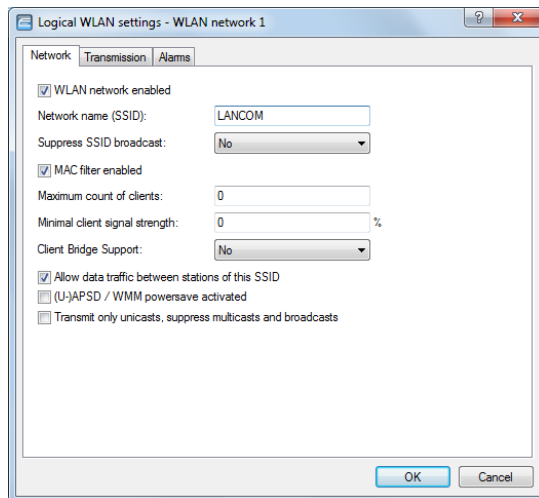
The logical WLAN interfaces

Every physical WLAN interface can support up to eight different logical cellular networks (Multi-SSID). Parameters can be defined specifically for each of these networks, without the need of additional access points.



Network settings

LANconfig:Wireless LAN > General > Logical WLAN settings > Network



■ WLAN network enabled

This switch enables or disables the corresponding logical WLAN.

■ Network name (SSID)

Specify a unique SSID (the network name) for each of the required logical wireless LANs. Only network cards that have the same SSID can register with this wireless network.

■ Suppress SSID broadcast

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option **Suppress SSID broadcast** provides the following settings:

- **No:** The access point publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes:** The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID.
- **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond.

! Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

■ **MAC filter enabled**

The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (**Wireless LAN > Stations > Stations**). The **MAC filter enabled** switch allows you to switch off the use of the MAC filter list for individual logical networks.

! Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The access point always consults the MAC filter list for registrations with an individual passphrase, even if this option is deactivated here.

■ **Maximum number of clients**

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

■ **Minimum client signal strength**

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

■ **Client-bridge support**

Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ().

! The client-bridge mode operates between two LANCOM devices only.

■ **Allow traffic between stations of this SSID**

Check this option if all stations logged on to this SSID are to be able to communicate with one another.

■ **(U)APSD / WMM Power Save activated**

Enable this option to signal stations that the power saving function (U)APSD ([Un]scheduled Automatic Power Save Delivery) is supported.

(U)APSD is established in the 802.11e standard, and helps VoWLAN devices to increase their battery life. The related devices switch to power saving mode after login on a (U)APSD-capable access point. If the access point receives data packets for the related devices thereafter, it temporarily stores the data and waits until the VoWLAN device is available again. It then forwards the data. Afterwards, (U)APSD increases the latency time of the radio module, whereby it ultimately consumes less power. The individual rest periods may be so short that a VoWLAN device can still use the power saving function in the call state itself. However, the relevant devices must also support (U)APSD.

WMM (Wi-Fi Multimedia) Power Save is a power saving function of the Wi-Fi Alliance and is based on U-APSD. Certain LANCOM access points are WMM® Power Save CERTIFIED by the Wi-Fi Alliance.

- **Only transmit unicasts, suppress broadcast and multicasts**

Multicast and broadcast transmissions within a WLAN cell cause a load on the bandwidth of the cell, especially since the WLAN clients often do not know how to handle these transmissions. The access point already intercepts a large part of the multicast and broadcast transmissions in the cell with ARP spoofing. With the restriction to unicast transmissions it filters out unnecessary IPv4 broadcasts from the requests, such as Bonjour or NetBIOS.

The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

6.3 IEEE 802.11u and Hotspot 2.0

As of LCOS 8.82, your device supports WLAN connections according to the IEEE 802.11u standard and—based on that—the Hotspot 2.0 specification. Using 802.11u you have the option to implement automatic authorization and authentication of your users on a local WLAN network (for example, within your company) or a Public Spot network. The prerequisite for this is that the relevant stations (smartphones, tablet PCs, notebooks, etc.) also support connections for 802.11u and Hotspot 2.0. In detail, the following functions are offered:

- **Automatic network selection**

In a 802.11u-enabled environment, the user does not have to manually detect and select an SSID. Instead, the client independently searches for and selects a suitable Wi-Fi network by automatically requesting and evaluating the operator and network data of all 802.11u-enabled access points that are in range. A previous login to the access point is not required.

Hotspot 2.0 stations also have the ability to retrieve information about the services available in a Wi-Fi network. If specific services that are relevant for a user (e.g., connections via HTTP, VPN or VoIP) are not available for a Wi-Fi network, any networks that do not meet the criteria are excluded from further searches. This ensures that users are always connected to the optimal network.

- **Automatic authentication and authorization**

In 802.11u-enabled environments, the station automatically carries out the user's login if the necessary credentials are available. Authentication can be done, for example, using a SIM card, a username and password, or a digital certificate. Repetitive manual input of the credentials by the user in a login screen is no longer necessary. After successful authentication, the user can immediately use the desired services.

- **Seamless handover**

Connections according to 802.11u and in conjunction with 802.21 facilitate the uninterrupted exchange of data connections between different network types. This enables users to switch their stations seamlessly from a cellular network to a WLAN network as soon as they get within range of a Hotspot 2.0 zone—and vice versa. The same is true for the transfer between two different operators if, for example, the user goes from one homogeneous network to another during a bus trip.

- **Automatic roaming**

Connections as per 802.11u facilitate roaming between different operator networks. If a user is in range of a Hotspot 2.0 zone of an operator for which he does not have any credentials, his station still has the option to switch to its home network. Authentication at a third-party Hotspot 2.0 zone is handled by the operator's roaming partner, which then allows the user to access the third-party Wi-Fi network. This is interesting not only in areas where there are only single network operators with access points, it is also especially attractive for people traveling abroad.

Example: For example, a user who is in transit in the city with his 802.11u-enabled smartphone (station) can enable the WLAN feature to browse the Internet. The station then starts trying to find all available Wi-Fi networks in the area. If any of the access points offer 802.11u, the station selects the one network that best fits the required service based on the operator and network information that was previously obtained, for example, from a hotspot offering Internet access from its own cellular network company. In this case, the subsequent authentication can be performed automatically via the SIM card so that the user does not need to intervene at any time during the process. The encryption method selected for the connection – e.g., WPA2 – is unaffected.

In summary, connections according to 802.11u and with Hotspot 2.0 enabled combine the security features and performance of classic Wi-Fi hotspots with the flexibility and simplicity of data cellular network connections. At the same time, they relieve the cellular networks by redistributing data traffic (and possibly also telephony) to the network connections and frequency bands offered by access points.

6.3.1 Hotspot operators and service providers

The Hotspot 2.0 specification of the Wi-Fi Alliance differentiates between hotspot operators and hotspot service providers: A **hotspot operator** only operates one Wi-Fi network, while a **hotspot service provider** (SP) provides the connection for the user to the Internet or a cellular network. Of course, it is possible for an operator to also be an SP. However, in all other cases, a hotspot operator requires the corresponding roaming agreements with an SP or a group of multiple SPs (called a roaming consortium). Only when an operator has made these agreements are the various roaming partners' customers able to authenticate with the hotspot operator. Each service provider operates its own AAA infrastructure. A hotspot communicates this list of possible roaming partners and the name of the hotspot operator using ANQP (see functional description).

6.3.2 Functional description

The **802.11u** standard is the base standard of IEEE. This standard essentially expands access points or hotspots with the ability to broadcast so-called **ANQP data packets** (Advanced Message Queuing Protocol) in its broadcast signals. ANQP is a query/response protocol that a device can use to request a range of information about the hotspot. This includes both meta-data, such as information about the owner and the venue, as well as information on the underlying network, such as information on operator domains, roaming partners, authentication methods, forwarding addresses, etc. All 802.11u-enabled devices in range have the ability to request these data packets without a prior login to the access point in order to select a network based on the network information.

The Wi-Fi Alliance has added further ANQP elements to the standard, and markets this specification as **Hotspot 2.0**. This Hotspot 2.0 function merely adds additional elements to the standard, which the device can use as criteria for selecting its network. These criteria include, for example, information about the services and WAN metrics available at the hotspot. The associated certification program is called Pass Points™. Certain LANCOM access points are Passpoint™ CERTIFIED by the Wi-Fi Alliance.

The ANQP data packets are the central information element of the 802.11u standard. However, to signal the support for 802.11u and to transmit data packets, further elements are required for the operation of 802.11u:

- The signaling of 802.11u support in the beacons and probes of a hotspot are done by the element known as the **Interworking element**. In this element, the initial basic network information—such as the network classification, Internet availability (Internet bit) and the OI of the roaming consortium and/or of the operator—are already included. At the same time, it is used by 802.11-enabled devices as an initial screening criterion when detecting a network.
- ANQP data packets are transferred within the so-called GAS containers. **GAS** stands for Generic Advertisement Service, and is the name of generic containers that allow a device to request additional internal and external information for the network selection from the hotspot, in addition to the information in the beacons. The GAS containers are transmitted on layer 2 by what are referred to as public action frames.

Login by an 802.11u-enabled client at a Hotspot 2.0

The following functional description schematically illustrates the selection and login process of an 802.11u-enabled device at a Hotspot 2.0.

Login via username/password or digital certificate

1. The hotspots reply with an ANQP response, which contains, among other things, the name of the hotspot operator and a list of NAI realms, which list all available roaming partners (service provider, abbreviated SP).
2. The device loads the locally stored credentials from the WLAN profiles or installed certificates that were set up by the user, and compares the local realms with the NAI realm lists obtained in (2).
 - a. If the device successfully finds one, it knows that it can be authenticated successfully on the relevant Wi-Fi network.

- b. If the device successfully finds more than one, the selection of a Wi-Fi network is made based on the user's preference list. This list defines the preferred order of operators in conjunction with the potential roaming partners. In this case, the device compares the operator names listed under (2) with the list, and selects the operator with the highest priority.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate SP. The access point then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for authentication. The authentication is performed using the authentication method determined by the SP. The authentication via username/password uses EAP-TTLS, and authentication via digital certificate uses EAP-TLS.

Login via (U)SIM

1. In contrast to the login via username/password or digital certificate, a device with a (U)SIM does not request the list of NAI realms in its ANQP requests, but rather the 3GPP Cellular Network Information. The ANQP responses contain the cellular network information list of all cellular network providers for which the access point offers authentication.
2. The device loads the parameters for the cellular network from its local (U)SIM card, and compares it with the data retrieved from the cellular network information lists. The list comparison and selection of a preferred provider network is performed analogous to the login via username/password or digital certificate.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate cellular network company. The hotspot then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for the authentication. The presence of a (U)SIM card changes the possible authentication method for the device to EAP-SIM or EAP-AKA.
4. The AAA system verifies the credentials for authentication via the interface MAP (Mobile Application Part) at the HLR server (Home Location Register) of the cellular network company.

If authentication is successful, the device gets access to the WLAN network either via hotspot (credentials for the operator's network are available) or automatic roaming (credentials for the operator's network are not available).

If there are multiple authentication options available for the device (e.g., SIM card and username/password), it has the option of using the preferred EAP authentication method and, therefore, the preferred credentials based on the NAI realm or cellular network information list.

6.3.3 Recommended general settings

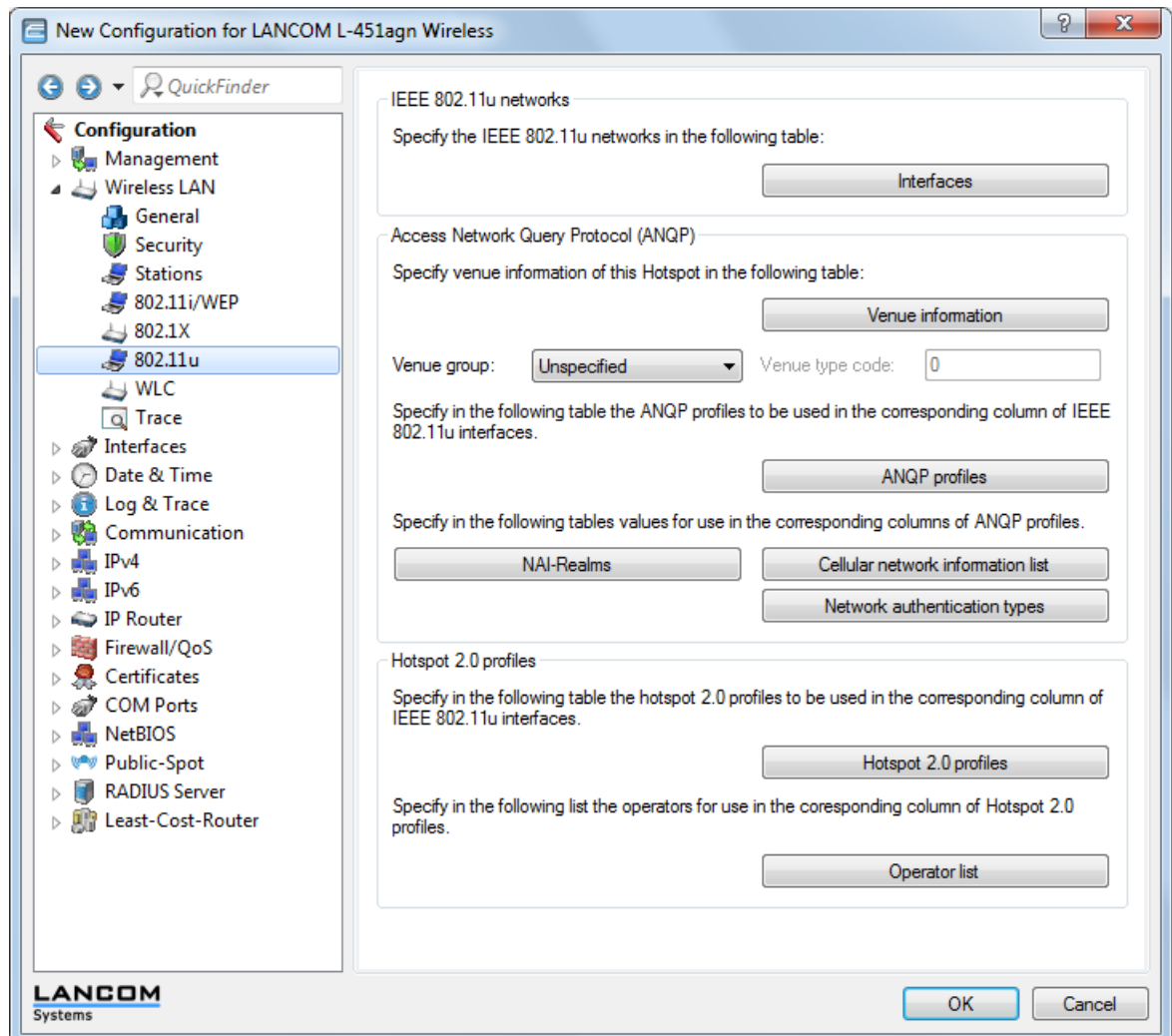
The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- WPA2-Enterprise Security (802.1x) enabled
- Authentication using EAP with the corresponding variant:
 - EAP-SIM/EAP-AKA for authentication with SIM / USIM card
 - EAP-TLS for authentication with a digital certificate
 - EAP-TTLS for authentication with a username and password
- Enabled and properly configured ARP proxy
- Disabled multicasts and broadcast in cellular networks (new in LCOS 8.82)
- Non-approved data traffic between the cellular network devices (Layer 2 traffic inspection and filtering). The corresponding settings can be found in LANconfig under **Wireless LAN > Security**.
- Enabled and implemented firewall on the access router, which provides Internet access

6.3.4 Enhancements to LANconfig

Configuration menu for IEEE 802.11u / Hotspot 2.0

You can find the configuration menu for IEEE 802.11u and Hotspot 2.0 under **Configuration > Wireless LAN > IEEE 802.11u**.



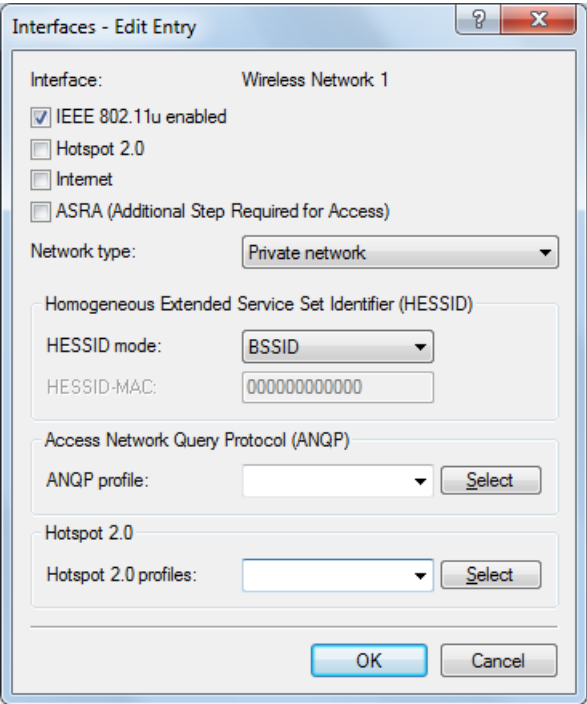
The device offers the ability to individually enable or disable and configure the support the IEEE 802.11u standard as well as the Hotspot 2.0 functionality for each logical WLAN interface using the button **Interfaces**.

Some of the parameters that need to be configured are located in so-called "profiles". Using profiles, you can group different rows in lists, which you only have to reference from the other windows. Essentially, these are profiles for ANQP data packets and Hotspot 2.0. The relationships between the profile lists is as follows:

```
-- Interfaces
|-- ANQP-Profiles
|   |-- NAI-Realms
|   |-- Cellular-Network-Information-List
|   |-- Network-Authentication-Types
|-- Hotspot 2.0 Profiles
|   |-- Operator-List
```

Activating interfaces

The table **Interfaces** is the highest administrative level for 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.



In order to edit the entries in the table **Interfaces**, click on the button **Edit....** The entries in the edit window have the following meaning:

- **Interface:** Name of the logical WLAN interface that you are currently editing.
- **IEEE 802.11u enabled:** Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11-enabled devices as the first filtering criteria for network detection.
- **Hotspot 2.0:** Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.
- **Internet:** Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.




Using this function you only communicate the availability of an Internet connection. You configure the corresponding regulations on the firewall, irrespective of this option.

- **ASRA - Additional steps for access required:** Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.



Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

- **Network type:** Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface. Based on the setting made here, the user has the option to limit network detection of their devices to specific network types. Possible values include:
 - **Private network:** Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.
 - **Private with guest access:** Similar to **Private network**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.
 - **Chargeable public network:** Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.
 - **Free public network:** Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.
 - **Personal device network:** In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.
 - **Emergency services only network:** Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.
 - **Test or experimental:** Describes networks that are set up for testing purposes or are still in the setup stage.
 - **Wildcard:** Placeholder for previously undefined network types.
 - **HESSID mode:** Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT". Possible values for the HESSID mode include:
 - **BSSID:** Select this item to set the BSSID of the device as the HESSID for your homogeneous ESS.
 - **User:** Select this item to manually assign a HESSID.
 - **None:** Select this item in order to not assign any homogeneous ESS and to isolate it from the device network.
 - **HESSID-MAC:** If you selected the setting **user** for the **HESSID mode**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., 008041AEFD7E for the MAC address 00:80:41:ae:fd:7e.
-
-  If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces
- **ANQP profile:** Select an ANQP profile from the list. You create ANQP profiles in the configuration menu using the button of the same name.
 - **Hotspot 2.0 profiles:** Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

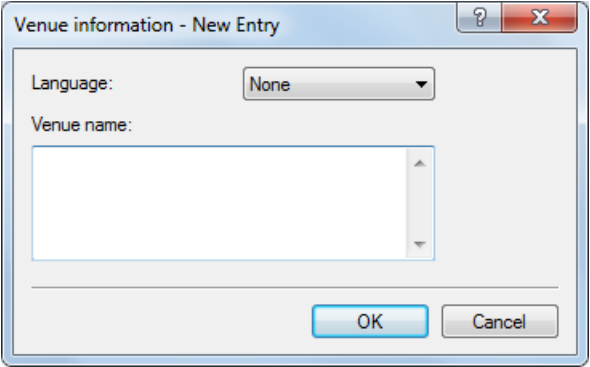
Configuring ANQP data packets

Venue information and group

Using the table **Venue information** and the following dialogs **Venue group** and **Venue type code**, you manage the information about the access point's location.

In the event of a manual search, additional details on the **Venue information** help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

You can place your device in a predefined category using the **Venue group** and **Venue type code** – as opposed to the user-defined location information.



In order to edit the entries in the table **Venue information**, click on the button **Add....** The entries in the edit window have the following meaning:

- **Language:** You have the ability to specify custom information for the location of the access point for each language. The location name that matches your user's language will then be displayed. If a language is not available for a user, its station chooses one based, for example, on the default language.
- **Venue name:** Enter a short description of the location of your device for the selected language, for example:

Ice Café Valencia
123 Street
City, State 12345

The **Venue group** describes the environment where you operate the access point. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

Using the **Venue type code**, you have the option to specify the details for the venue group. These values are also specified by the standard. The possible type codes can be found in the following table.

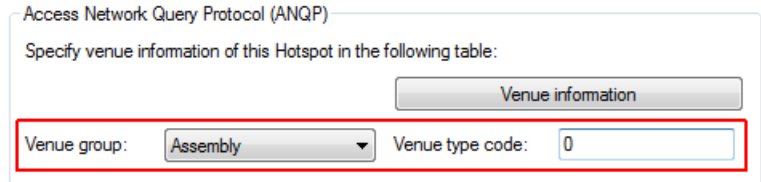


Table 1: Overview of possible values for venue groups and types

Venue group	Code = Venue type code
Unspecified	
Assembly	<ul style="list-style-type: none">■ 0 = unspecified assembly■ 1 = stage■ 2 = stadium■ 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station)■ 4 = amphitheater■ 5 = amusement park■ 6 = place of worship■ 7 = convention center■ 8 = library■ 9 = museum■ 10 = restaurant■ 11 = theater

Venue group	Code = Venue type code
	<ul style="list-style-type: none"> ■ 12 = bar ■ 13 = café ■ 14 = zoo, aquarium ■ 15 = emergency control center
Business	<ul style="list-style-type: none"> ■ 0 = unspecified business ■ 1 = doctor's office ■ 2 = bank ■ 3 = fire station ■ 4 = police station ■ 6 = post office ■ 7 = office ■ 8 = research facility ■ 9 = law firm
Educational:	<ul style="list-style-type: none"> ■ 0 = unspecified education ■ 1 = primary school ■ 2 = secondary school ■ 3 = college
Factory and industry	<ul style="list-style-type: none"> ■ 0 = unspecified factory and industry ■ 1 = factory
Institutional	<ul style="list-style-type: none"> ■ 0 = unspecified institution ■ 1 = hospital ■ 2 = long-term care facility (e.g., nursing home, hospice) ■ 3 = rehabilitation clinic ■ 4 = organizational association ■ 5 = prison
Commerce	<ul style="list-style-type: none"> ■ 0 = unspecified commerce ■ 1 = retail store ■ 2 = food store ■ 3 = auto repair shop ■ 4 = shopping center ■ 5 = gas station
Halls of residence	<ul style="list-style-type: none"> ■ 0 = unspecified residence hall ■ 1 = private residence ■ 2 = hotel or motel ■ 3 = student housing ■ 4 = guesthouse
Warehouse	<ul style="list-style-type: none"> ■ 0 = unspecified warehouse
Utility and miscellaneous	<ul style="list-style-type: none"> ■ 0 = unspecified service and miscellaneous
Vehicular	<ul style="list-style-type: none"> ■ 0 = unspecified vehicle ■ 1 = passenger or transport vehicles ■ 2 = aircraft ■ 3 = bus ■ 4 = ferry ■ 5 = ship or boat ■ 6 = train ■ 7 = motorcycle
Outdoor	<ul style="list-style-type: none"> ■ 0 = unspecified outdoor

Venue group	Code = Venue type code
	<ul style="list-style-type: none"> ■ 1 = municipal Wi-Fi network (wireless mesh network) ■ 2 = city park ■ 3 = rest area ■ 4 = traffic control ■ 5 = bus stop ■ 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. **ANQP profiles** offers you the ability to group certain ANQP elements and to independently assign logical WLAN interfaces in the table **Interfaces**. These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.

In order to edit the entries in the table **ANQP profiles**, click on the button **Add....** The entries in the edit window have the following meaning:

- **Name:** Assign a name for the ANQP 2.0 profile here. This name will appear later in the interfaces table in the selection for ANQP profiles.
- **Beacon OUI:** Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.

! This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

- **Additional OUI:** Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.
- **Domain name list:** Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org, provx-mobile.com, wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., `providerX.org`, this domain is also assigned to access points with the domain name `wi-fi.providerX.org`. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.
- **NAI realm list:** Select an NAI realm profile from the list. You specify profiles for NAI realms in the configuration menu by clicking the button **NAI realms**.
- **Cellular list:** Select the cellular network identity from the list. You set the identities for cellular networks – similar to profiles – in the configuration menu using the button **Cellular network information list**.
- **Network authentication type list:** Select an authentication profile from the list. You specify profiles for network authentication in the configuration menu by clicking the button **Network authentication types**.

Additionally, using the telnet console or setup menu, you have the option to also display the type of available IP addresses, which they can obtain from the network after a successful authentication. You can access the relevant parameters **IPv4-Addr-Type** and **IPv6-Addr-Type** via the telnet path **Setup > IEEE802.11u > ANQP-General**.

NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.

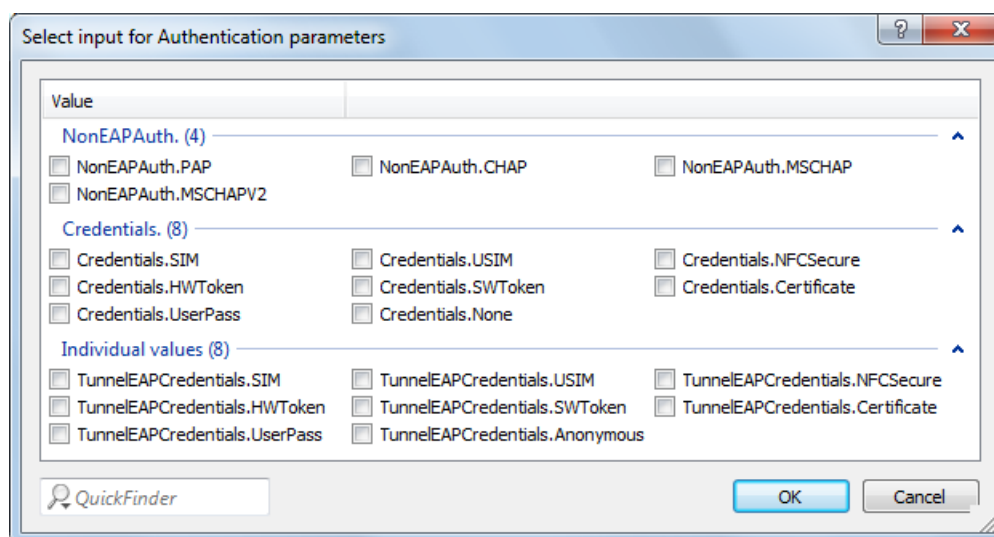
The image shows a dialog box titled "NAI-Realms - New Entry". It has a standard Windows-style title bar with a question mark icon and a close button (X). The dialog contains several input fields: "Name:" with a text box, "Network Access Identifier (NAI)" with a text box, "NAI-Realm:" with a text box, "EAP method:" with a dropdown menu currently showing "None", and "Authentication parameters:" with a text box and a "Select" button next to it. At the bottom of the dialog are "OK" and "Cancel" buttons.

In order to edit the entries in the table **NAI realms**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **Name:** Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. This name will appear later in the ANQP profile in the selection for **NAI realm list**.
- **NAI realm:** Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest case, is `<username>@<realm>`, for `user746@providerX.org`, and therefore the corresponding realm is `providerX.org`.
- **EAP method:** Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication method. Possible values include:

- **EAP-TLS:** Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate that the user has to install.
- **EAP-SIM:** Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.
- **EAP-TTLS:** Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI realm is performed using a username and password. For security reasons, the connection is tunneled for this method.
- **EAP-AKA:** Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.
- **None:** Select this setting when the relevant NAI realm does not require authentication.

■ **Authentication parameters:**



In the window that opens when you click the **Select** button, select the appropriate authentication parameters for the EAP method, such as EAP-TTLS `NonEAPAuth.MSCHAPV2`, `Credential.UserPass` or for EAP-TLS `Credentials.Certificate`. Possible values include:

Table 2: Overview of possible authentication parameters

Parameters	Sub-parameters	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWTOKEN*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate

Parameters	Sub-parameters	Comment
TunnelEAPCredentials.*	UserPass	Username and password
	None	No credentials required
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Cellular network information list

Using this table you manage the identity lists for cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.

In order to edit the entries in the table **Cellular network information list**, click on the button **Add....** The entries in the edit window have the following meaning:

- **Name:** Assign a name for the cellular network identity, such as an abbreviation of the network operator in combination with the cellular network standard used. This name will appear later in the ANQP profile in the selection for **Cellular list**.
- **Country code (MCC):** Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., 262 for Germany.
- **Network code (MNC):** Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Network authentication types

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

! Please remember to set the ASRA bit in the **Interfaces** table if you set up an additional authentication step.

In order to edit the entries in the table **Network authentication types**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **Name:** Assign a name for the table entry, for example, *Accept Terms & Conditions*. This name will appear later in the ANQP profile in the selection for **Network auth. type list**.
- **Authentication type:** Choose the context from the list, which applies before forwarding. Possible values include:
 - *Accept terms & conditions:* An additional authentication step is set up that requires the user to accept the terms of use.
 - *Online enrollment:* An additional authentication step is set up that requires the user to register online first.
 - *HTTP redirection:* An additional authentication step is set up to which the user is forwarded via HTTP.
 - *DNS redirection:* An additional authentication step is set up to which the user is forwarded via DNS.
- **Redirect URL:** Enter the address to which the device forwards stations for additional authentication.

Configuring Hotspot 2.0

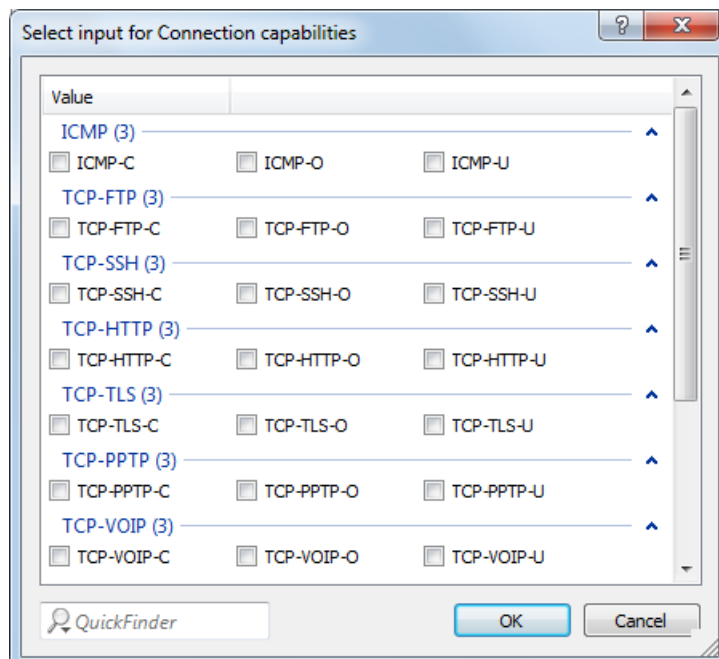
Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offers you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign logical WLAN interfaces in the table **Interfaces**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.

In order to edit the entries in the table **Hotspot 2.0 profiles**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **Name:** Assign a name for the Hotspot 2.0 profile here. This name will appear later in the interfaces table in the selection for the Hotspot 2.0 profile.
- **Operator name list:** Select the profile of a hotspot operator from the list. You specify profiles for hotspot operators in the configuration menu by clicking the **Operator list**.

■ Connection capabilities:



Click the **Select** button and enter the connection capabilities for each service in the window that opens. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown". Possible status values for each of these services are "closed" (–C), "Open" (–O) or "unknown" (–U):

- ICMP: Specify whether to allow the exchange of information and error messages via ICMP.
- TCP–FTP: Specify whether to allow file transfers via FTP.
- TCP–SSH: Specify whether to allow encrypted connections via SSH.
- TCP–HTTP: Specify whether to allow Internet connections via HTTP/HTTPS.
- TCP–TLS: Specify whether to allow encrypted connections via TLS.
- TCP–PPTP: Specify whether to allow the tunneling of VPN connections via PPTP.
- TCP–VOIP: Specify whether to allow Internet telephony via VoIP (TCP).
- UDP–IPSEC–500: Specify whether to allow IPsec via UDP and port 500.
- UDP–VOIP: Specify whether to allow Internet telephony via VoIP (UDP).
- UDP–IPSEC–4500: Specify whether to allow IPsec via UDP and port 4500.
- ESP: Specify whether to allow ESP (Encapsulating Security Payload) for IPsec.

If you do not know if a service is available and its ports are open or closed on your network, or you consciously do not want to make any entry for the status, select a –U setting.

ⓘ Using this dialog, you do not define permissions! The stations only use the entries to determine whether to join a network via your device. You configure specific access permissions for your network with other device functions, such as the firewall/QoS.

- **Operating class:** Enter the code for the global operating class of the access point. Using the operating class, you inform a station on which frequency bands and channels your access point is available. Example:

- 81: Operation at 2.4 GHz with channels 1-13
- 116: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at standards.ieee.org.

Operator list

Using this table you manage the plain text name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.

In order to edit the entries in the table **Operator list**, click on the button **Add....** The entries in the edit window have the following meaning:

- **Name:** Assign a name for the entry, such as an index number or combination of operator-name and language.
- **Language:** Select a language for the hotspot operator from the list.
- **Operator name:** Enter the plain text name of the hotspot operator.

6.3.5 Additions to the Setup menu

IEEE802.11u

The tables and parameters in this menu are used to make all settings for connections according to IEEE 802.11u and Hotspot 2.0.

SNMP ID:

2.71

Telnet path:

Setup

ANQP general

The general settings for ANQP are made in this menu.

SNMP ID:

2.71.6

Telnet path:

Setup > IEEE802.11u

IPv4 address type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv4.

SNMP ID:

2.71.6.5

Telnet path:**Setup > IEEE802.11u > ANQP-General****Possible values:****Not-Available**

IPv4 address type is not available.

Public-Addr-Available

Public IPv4 address is available.

Port-Restr-Addr-Avail

Port-restricted IPv4 address is available.

Single-Nat-Priv-Addr-Avail

Private, single NAT-masked IPv4 address is available.

Double-Nat-Priv-Addr-Avail

Private, double NAT-masked IPv4 address is available.

Port-Restr-Single-Nat-Addr-Avail

Port-restricted IPv4 address and single NAT-masked IPv4 address is available.

Port-Restr-Double-Nat-Addr-Avail

Port-restricted IPv4 address and double NAT-masked IPv4 address is available.

Availability-not-known

The availability of an IPv4 address type is unknown.

Default:

Single-Nat-Priv-Addr-Avail

IPv6 address type

Using this entry you inform an IEEE802.11u-capable station whether the address it receives after successful authentication on the operator's Hotspot is of type IPv6.

SNMP ID:

2.71.6.6

Telnet path:**Setup > IEEE802.11u > ANQP-General****Possible values:****Not-Available**

IPv6 address type is not available.

Available

IPv6 address type is available.

Availability-not-known

The availability of an IPv6 address type is unknown.

Default:

Not-Available

Venue group

The venue group describes the environment where you set up the access point. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

SNMP ID:

2.71.6.1

Telnet path:**Setup > IEEE802.11u > ANQP-General****Possible values:**

- Unspecified: Unspecified
- Assembly: Assembly
- Business: Business
- Educational: Educational:
- Factory-and-Industry: Factory and industry
- Institutional: Institutional
- Mercantile: Commerce
- Residential: Residence hall
- Storage: Warehouse
- Utility-and-Miscellaneous: Utility and miscellaneous
- Vehicular: Vehicle
- Outdoor: Outdoor

Default:

Unspecified

Venue type

Using the location type code (venue type), you have the option to specify details for the location group. These values are also specified by the standard. The possible type codes can be found in the following table.

SNMP ID:

2.71.6.2

Telnet path:**Setup > IEEE802.11u > ANQP-General****Possible values:****Table 3: Overview of possible values for venue groups and types**

Venue group	Code = Venue type code
Unspecified	
Assembly	<ul style="list-style-type: none"> ■ 0 = unspecified assembly ■ 1 = stage ■ 2 = stadium ■ 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) ■ 4 = amphitheater ■ 5 = amusement park ■ 6 = place of worship ■ 7 = convention center ■ 8 = library ■ 9 = museum ■ 10 = restaurant ■ 11 = theater ■ 12 = bar ■ 13 = café

Venue group	Code = Venue type code
	<ul style="list-style-type: none"> 14 = zoo, aquarium 15 = emergency control center
Business	<ul style="list-style-type: none"> 0 = unspecified business 1 = doctor's office 2 = bank 3 = fire station 4 = police station 6 = post office 7 = office 8 = research facility 9 = law firm
Educational:	<ul style="list-style-type: none"> 0 = unspecified education 1 = primary school 2 = secondary school 3 = college
Factory and industry	<ul style="list-style-type: none"> 0 = unspecified factory and industry 1 = factory
Institutional	<ul style="list-style-type: none"> 0 = unspecified institution 1 = hospital 2 = long-term care facility (e.g., nursing home, hospice) 3 = rehabilitation clinic 4 = organizational association 5 = prison
Commerce	<ul style="list-style-type: none"> 0 = unspecified commerce 1 = retail store 2 = food store 3 = auto repair shop 4 = shopping center 5 = gas station
Halls of residence	<ul style="list-style-type: none"> 0 = unspecified residence hall 1 = private residence 2 = hotel or motel 3 = student housing 4 = guesthouse
Warehouse	<ul style="list-style-type: none"> 0 = unspecified warehouse
Utility and miscellaneous	<ul style="list-style-type: none"> 0 = unspecified service and miscellaneous
Vehicular	<ul style="list-style-type: none"> 0 = unspecified vehicle 1 = passenger or transport vehicles 2 = aircraft 3 = bus 4 = ferry 5 = ship or boat 6 = train 7 = motorcycle
Outdoor	<ul style="list-style-type: none"> 0 = unspecified outdoor 1 = municipal Wi-Fi network (wireless mesh network) 2 = city park

Venue group	Code = Venue type code
	<ul style="list-style-type: none"> ■ 3 = rest area ■ 4 = traffic control ■ 5 = bus stop ■ 6 = kiosk

Default:

0

Hotspot2.0

The general settings for Hotspot 2.0 are made in this menu.

SNMP ID:

2.71.7

Telnet path:**Setup > IEEE802.11u****Connection capability**

This table contains a fixed list of connection capabilities. Possible status values for each of these services are "closed" (-C), "Open" (-O) or "unknown" (-U):

SNMP ID:

2.71.7.2

Telnet path:**Setup > IEEE802.11u > Hotspot2.0****Hotspot2.0**

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** allow you to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign logical WLAN interfaces in the table **Setup > Interfaces > WLAN > IEEE802.11u** under **HS20-Profile**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.

SNMP ID:

2.71.7.9

Telnet path:**Setup > IEEE802.11u > Hotspot2.0****Name**

Assign a name for the Hotspot 2.0 profile here. You specify this name later in the table **Setup > Interfaces > WLAN > IEEE802.11u** under **HS20-Profile**.

SNMP ID:

2.71.7.9.1

Telnet path:**Setup > IEEE802.11u > Hotspot2.0 > Hotspot2.0****Possible values:**

String, max. 32 characters

Default:

Operator name

Enter a valid profile for hotspot operators in this field.

SNMP ID:

2.71.7.9.2

Telnet path:

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

Possible values:

Name from table **Setup > IEEE802.11u > Hotspot2.0 > Operator-List**, max. 65 characters

Default:

Connection capabilities

Enter one or more valid entries for the connection capabilities in this field. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown".

SNMP ID:

2.71.7.9.3

Telnet path:

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

Possible values:

Name from table **Setup > IEEE802.11u > Hotspot2.0 > Connectivity-Capability**, max. 252 characters
Multiple names can be provided in a comma-separated list.

Default:

Operating class

Enter the code for the global operating class of the access point. Using the operating class, you inform a station on which frequency bands and channels your access point is available. Example:

- 81: Operation at 2.4 GHz with channels 1-13
- 116: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at standards.ieee.org.

SNMP ID:

2.71.7.9.4

Telnet path:

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

Possible values:

Operating class code, max. 32 characters

Default:

Operator list

Using this table you manage the plain text name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.

SNMP ID:

2.71.7.1

Telnet path:**Setup > IEEE802.11u > Hotspot2.0****Name**

Assign a name for the entry, such as an index number or combination of operator-name and language.

SNMP ID:

2.71.7.1.1

Telnet path:**Setup > IEEE802.11u > Hotspot2.0 > Operator-List****Possible values:**

String, max. 32 characters

Default:**Language**

Select a language for the hotspot operator from the list.

SNMP ID:

2.71.7.1.4

Telnet path:**Setup > IEEE802.11u > Hotspot2.0 > Operator-List****Possible values:**

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

Default:

None

Operator name

Enter the plain text name of the hotspot operator.

SNMP ID:

2.71.7.1.2

Telnet path:**Setup > IEEE802.11u > Hotspot2.0 > Operator-List****Possible values:**

String, max. 252 characters

Default:

Blank

Uplink speed

Using this entry you can enter the nominal value for the maximum transmission bandwidth (uplink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

SNMP ID:

2.71.7.8

Telnet path:**Setup > IEEE802.11u > Hotspot2.0****Possible values:**

0 to 4294967295, in kbps

Default:

0

Link status

Using this entry, you specify the connectivity status of your device to the Internet.

SNMP ID:

2.71.7.4

Telnet path:**Setup > IEEE802.11u > Hotspot2.0****Possible values:**

- **Auto:** The device determines the status value for this parameter automatically
- **Link-Up:** The connection to the Internet is established.
- **Link-Down:** The connection to the Internet is interrupted.
- **Link-Test:** The connection to the Internet is being established or is being checked.

Default:

Auto

Downlink speed

Using this entry, you enter the nominal value for the maximum receiving bandwidth (downlink) that is available to a client logged in to your hotspot. The bandwidth itself can be defined using the Public Spot module.

SNMP ID:

2.71.7.7

Telnet path:**Setup > IEEE802.11u > Hotspot2.0**

Possible values:

0 to 4294967295, in Kbit/s

Default:

0

Authentication parameter

This table contains a fixed list of possible authentication parameters for the NAI realm.

Table 4: Overview of possible authentication parameters

Parameters	Sub-parameters	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWTOKEN*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password
TunnelEAPCredentials.*	None	No credentials required
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWTOKEN*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

SNMP ID:

2.71.8

Telnet path:

Setup > IEEE802.11u

Cellular network information list

Using this table, you manage the profile lists for the cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.

In the setup menu you assign an IEEE802.11u profile to a list using this table **Setup > IEEE802.11u > IEEE802.11u**.

SNMP ID:

2.71.4

Telnet path:

Setup > IEEE802.11u

Name

Assign a name for the cellular network profile, such as an abbreviation of the network operator in combination with the cellular network standard used. You specify this name later in the table **Setup > IEEE802.11u > IEEE802.11u** under **Cellular-List**.

SNMP ID:

2.71.4.1

Telnet path:

Setup > IEEE802.11u > Cellular-Network-Information-List

Possible values:

String, max. 32 characters

Default:

Country code

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., 262 for Germany.

SNMP ID:

2.71.4.2

Telnet path:

Setup > IEEE802.11u > Cellular-Network-Information-List

Possible values:

String, max. 3 characters

Default:

Network code

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

SNMP ID:

2.71.4.3

Telnet path:

Setup > IEEE802.11u > Cellular-Network-Information-List

Possible values:

String, max. 3 characters

Default:**ANQP profiles**

Using this table you manage the profile lists for IEEE802.11u or ANQP. IEEE802.11u profiles give you the ability to group certain ANQP elements and to independently assign them to logical WLAN interfaces in the table **Setup > Interfaces > WLAN > IEEE802.11u** under **IEEE802.11u-Profile**. These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.

SNMP ID:

2.71.1

Telnet path:**Setup > IEEE802.11u****Name**

Assign a name for the IEEE802.11 profile here. You specify this name later in the table **Setup > Interfaces > WLAN > IEEE802.11u** under **IEEE802.11u-Profile**.

SNMP ID:

2.71.1.1

Telnet path:**Setup > IEEE802.11u > ANQP-Profiles****Possible values:**

String, max. 32 characters

Default:**Include in beacon OUI**

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.



This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional-OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

SNMP ID:

2.71.1.2

Telnet path:**Setup > IEEE802.11u > ANQP-Profiles****Possible values:**

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

Default:**Additional OUI**

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as 00105E, 00017D, 00501A.

SNMP ID:

2.71.1.3

Telnet path:

Setup > IEEE802.11u > ANQP-Profiles

Possible values:

OI, max. 65 characters. Multiple OIs can be provided in a comma-separated list.

Default:**Domain list**

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org`, `provx-mobile.com`, `wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., `providerX.org`, this domain is also assigned to access points with the domain name `wi-fi.providerX.org`. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

SNMP ID:

2.71.1.4

Telnet path:

Setup > IEEE802.11u > ANQP-Profiles

Possible values:

String, max. 65 characters Multiple domains can be provided in a comma-separated list.

Default:**NAI realm list**

Enter a valid NAI realm profile in this field.

SNMP ID:

2.71.1.5

Telnet path:

Setup > IEEE802.11u > ANQP-Profiles

Possible values:

Name from table **Setup > IEEE802.11u > NAI-Realms**, max. 65 characters

Default:**Cellular list**

Enter a valid cellular network profile in this field.

SNMP ID:

2.71.1.6

Telnet path:**Setup > IEEE802.11u > ANQP-Profiles****Possible values:****Name** from table **Setup > IEEE802.11u > Cellular-Network-Information-List**, max. 65 characters**Default:****Network authentication type list**

Enter one or more valid authentication parameters in this field.

SNMP ID:

2.71.1.7

Telnet path:**Setup > IEEE802.11u > ANQP-Profiles****Possible values:****Name** from table **Setup > IEEE802.11u > Network-Authentication-Type**, max. 65 characters Multiple names can be provided in a comma-separated list.**Default:****NAI realms**

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.

In the setup menu you assign an IEEE802.11u profile to a list using this table **Setup > IEEE802.11u > IEEE802.11u**.

SNMP ID:

2.71.9

Telnet path:**Setup > IEEE802.11u****Name**

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. You specify this name later in the table **Setup > IEEE802.11u > IEEE802.11u** under **NAI-Realm-List**.

SNMP ID:

2.71.9.1

Telnet path:**Setup > IEEE802.11u > NAI-Realms****Possible values:**

String, max. 32 characters

Default:**NAI realm**

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest

case, is <username>@<realm>, for user746@providerX.org, and therefore the corresponding realm is providerX.org.

SNMP ID:

2.71.9.2

Telnet path:

Setup > IEEE802.11u > NAI-Realms

Possible values:

String, max. 32 characters

Default:

EAP method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication procedure

SNMP ID:

2.71.9.3

Telnet path:

Setup > IEEE802.11u > NAI-Realms

Possible values:

- None: Select this setting when the relevant NAI realm does not require authentication.
- EAP-TLS: Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate installed by the user.
- EAP-SIM: Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.
- EAP-TTLS: Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.
- EAP-AKA: Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

Default:

None

Authentication parameter

In this field, enter the appropriate authentication parameters for the EAP method using a comma-separated list, e.g., for EAP-TTLS NonEAPAuth.MSCHAPV2,Credential.UserPass or for EAP-TLS Credentials.Certificate.

SNMP ID:

2.71.9.4

Telnet path:

Setup > IEEE802.11u > NAI-Realms

Possible values:

Name from table **Auth.-parameter**, max. 65 characters. Multiple names are separated by commas.

Default:**Network authentication type**

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

SNMP ID:

2.71.5

Telnet path:**Setup > IEEE802.11u****Name**

Assign a name for the table entry, e.g., `Accept Terms and Conditions`.

SNMP ID:

2.71.5.3

Telnet path:**Setup > IEEE802.11u > Network-Authentication-Type****Possible values:**

String, max. 32 characters

Default:**Network authentication type**

Choose the context from the list, which applies before forwarding.

SNMP ID:

2.71.5.1

Telnet path:**Setup > IEEE802.11u > Network-Authentication-Type****Possible values:**

- `Accept-Terms-Cond`: An additional authentication step is set up that requires the user to accept the terms of use.
- `Online-Enrollment`: An additional authentication step is set up that requires the user to register online first.
- `Http-Redirection`: An additional authentication step is set up to which the user is forwarded via HTTP.
- `DNS-Redirection`: An additional authentication step is set up to which the user is forwarded via DNS.

Default:`Accept-Terms-Cond`**Redirect URL**

Enter the address to which the device forwards stations for additional authentication.

SNMP ID:

2.71.5.2

Telnet path:

Setup > IEEE802.11u > Network-Authentication-Type

Possible values:

URL, max. 65 characters

Default:**Venue name**

In this table, enter general information about the location of the access point.

In the event of a manual search, additional details on the location information help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

SNMP ID:

2.71.3

Telnet path:

Setup > IEEE802.11u

Name

Enter a name for the list entry in the table, such as a language pair description or an index number.

SNMP ID:

2.71.3.1

Telnet path:

Setup > IEEE802.11u > Venue-Name

Possible values:

String, max. 32 characters

Default:

Blank

Language

Select the language in which you store information about the location.

SNMP ID:

2.71.3.3

Telnet path:

Setup > IEEE802.11u > Venue-Name

Possible values:

None

English

Deutsch

Chinese

Spanish

French

Italian

6 WLAN

Russian

Dutch

Turkish

Portuguese

Polish

Czech

Arabian

Default:

None

Venue name

Enter a short description of the location of your device for the selected language.

SNMP ID:

2.71.3.2

Telnet path:

Setup > IEEE802.11u > Venue-Name

Possible values:

String, max. 252 characters

Default:

Blank

IEEE802.11u

The table **IEEE802.11u** is the highest administrative level for 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.

SNMP ID:

2.23.10.16

Telnet path:

Setup > Interfaces > WLAN

Ifc

Name of the logical WLAN interface that you are currently editing.

SNMP ID:

2.23.10.16.1

Telnet path:

Setup > Interfaces > WLAN > IEEE802.11u

Operating

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11-enabled devices as the first filtering criteria for network detection.

SNMP ID:

2.23.10.16.2

Telnet path:**Setup > Interfaces > WLAN > IEEE802.11u****Possible values:**

Yes

No

Default:

No

Hotspot2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.



The prerequisite for this function is that support for connections according to IEEE 802.11u is enabled.

SNMP ID:

2.23.10.16.3

Telnet path:**Setup > Interfaces > WLAN > IEEE802.11u****Possible values:**

Yes

No

Default:

No

Internet

Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

SNMP ID:

2.23.10.16.4

Telnet path:**Setup > Interfaces > WLAN > IEEE802.11u****Possible values:**

Yes

No

Default:

No

Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface.

SNMP ID:

2.23.10.16.5

Telnet path:**Setup > Interfaces > WLAN > IEEE802.11u****Possible values:**

- **Private**: Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.
- **Private-GuestAcc**: Similar to **Private**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.
- **Public-Charge**: Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.
- **Public-Free**: Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.
- **Personal-Dev**: In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.
- **Emergency**: Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.
- **Experimental**: Describes networks that are set up for testing purposes or are still in the setup stage.
- **Wildcard**: Placeholder for previously undefined network types.

Default:

Private

Asra

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.



Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

SNMP ID:

2.23.10.16.6

Telnet path:**Setup > Interfaces > WLAN > IEEE802.11u****Possible values:**

Yes

No

Default:

No

HESSID

Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point (its BSSID) serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because

different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT".

SNMP ID:

2.23.10.16.7

Telnet path:

Setup > Interfaces > WLAN > IEEE802.11u

Possible values:

BSSID

user

None

Default:

BSSID

HESSID MAC

If you selected the setting `user` for the **HESSID-Mode**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., `008041AEFD7E` for the MAC address `00:80:41:ae:fd:7e`.



If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

SNMP ID:

2.23.10.16.8

Telnet path:

Setup > Interfaces > WLAN > IEEE802.11u

Possible values:

MAC address in capital letters and without separators

Default:

000000000000

ANQP profile

Select an ANQP or 802.11u profile from the list. Generate 802.11u profiles in the setup menu using the table **Setup > IEEE802.11u > ANQP-Profile**.

SNMP ID:

2.23.10.16.10

Telnet path:

Setup > Interfaces > WLAN > IEEE802.11u

Possible values:

Name from table **Setup > IEEE802.11u > ANQP-Profile**, max. 32 characters

Default:

HS20 profile

Select a Hotspot-2.0 or HS20 profile from the list. Generate HS20 profiles in the setup menu using the table **Setup > IEEE802.11u > IEEE802.11u**.

6 WLAN

SNMP ID:

2.23.10.16.13

Telnet path:

Setup > Interfaces > WLAN > IEEE802.11u

Possible values:

Name from table **Setup > IEEE802.11u > Hotspot2.0**, max. 32 characters

Default:

7 Public Spot

7.1 Template variables

A Public Spot gives you the option to include variables in the URL to be sent to the templates, i.e. to control the web pages displayed to a user. This can be used to implement login pages based on the SSID or VLAN-ID, or to display additional connection information to the user on the login page.

The following variables are available:

%i

Placeholder for the **NAS port ID**. In this context, "NAS" stands for "Network Access Server". This variable contains the interface of the device that the client used to login. For a WLC or router without WLAN this corresponds to a physical interface, such as `LAN-1`, or, for a standalone access point, it is the SSID.

%s

Placeholder for the **SSID**. If the device being used is an access point, this variable contains the SSID, e.g., `PUBLICSPOT`.

%v

Placeholder for **Source VLAN**. If the requesting client is assigned to a VLAN, this variable contains the source VLAN ID.

In order to use variables in a template, you set the **Request-Type** for each page under **Public-Spot-Module > Page-Table** and extend the **Page-Address (URL)**, where your custom templates are located, by the individual parameters. In the following URLs the variable `%i` is replaced with `LAN-1` as described in the sample above:

Example: `http://192.168.1.1/welcome.php?nas=%i`

Example: `http://192.168.1.1/%i_welcome.html`

7.2 Customizing the standard pages

As an alternative to installing complete user-defined Web pages, the device provides the option of customizing the pre-installed default pages to a certain extent. This includes for example the input of a login text that is displayed to your users in the registration form, or replacing the header image (logo). In this way, you can quickly deploy a customized Public Spot without having to deal in-depth with the subject of the Web page authoring.

7.2.1 Customized text on the login page

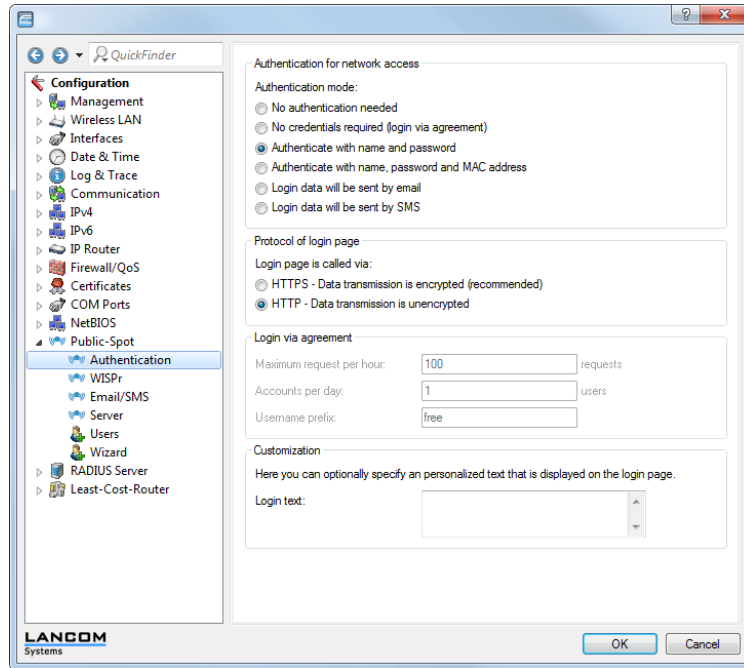
The Public Spot module gives you the option to specify customized text, which appears on the login page inside the box of the registration form. Do this by executing the following steps.

1. In LANconfig, open the configuration dialog for the device.
2. Navigate to the dialog **Public Spot > Authentication** and enter the text that you want your Public Spot users to see in the **Customization** section. You can enter an HTML string with max. 254 characters composed of:

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

LANconfig automatically transforms umlauts. To enter umlauts, you must use their HTML equivalents (e.g. ü ; for ü). You can also use HTML tags to structure and format the text. Example:

Herzlich Willkommen!
<i>Bitte füllen Sie das Formular aus.</i>)



3. Click on **OK** to load the login text into the device.

Once the configuration has been written successfully, the new login text appears the next time the Public Spot page is called.

7.2.2 Custom header images for variable screen widths

A component of the pre-installed pages in the device is a header image (logo), which is displayed to your users above the login form for the Public Spot. You can change this header image as you please, for example to reflect the application environment or your corporate design. There is no need for an external Web server; you can simply upload the image directly into the device via the file management in WEBconfig or the configuration management in LANconfig.

A special feature of the header image is that it is available in the device as two possible variants: One version is for large screens or browser windows with a horizontal resolution exceeding 800 px (normal monitors, laptops, tablet PCs, etc.),

and one is a small picture for screens with a lower horizontal resolution (PDAs, mobile phones, etc.). This allows you to provide header images for different target groups and to provide them a login page that is appropriate for their device.

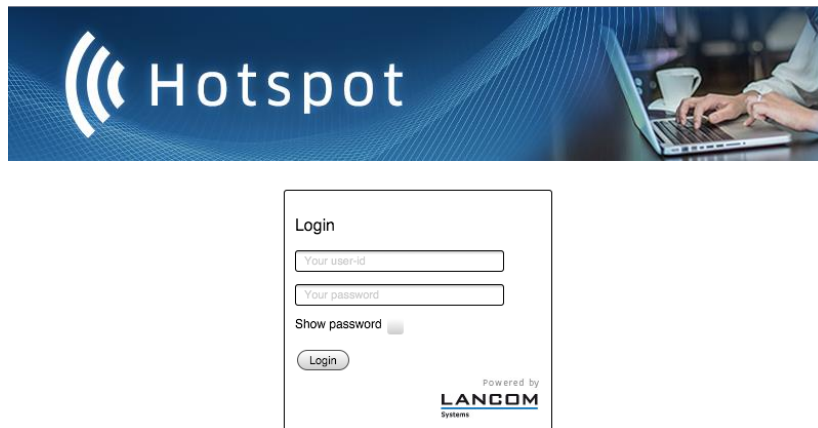


Figure 1: Login page for large screens

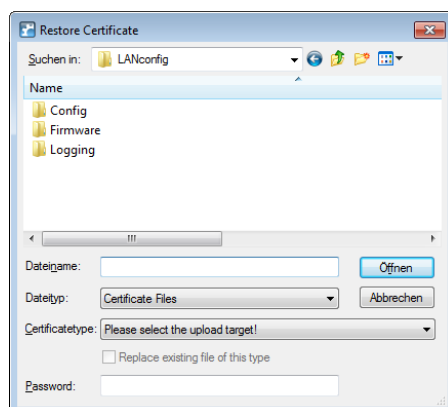


Figure 2: Login page for small screens

The available resolutions are set by the CSS file of the device. The pre-installed default graphics allow for 800x150 px for the large screen and 258x52 px for the small screen. The file type must be either JPG, GIF, or PNG.

To upload a new header image to the device either as a large or small version, follow the steps below.


1. Start LANconfig and highlight the device.
2. In the menu bar, click on **Device > Configuration management > Upload certificate or file**. The **Upload certificate** dialog opens.



3. Set the **File type** to **All files** and select the **Certificate type** that you want to upload.
 - **Public Spot - Header image of pages:** Certificate type for large screens
 - **Public Spot - Header image box:** Certificate type for small screens

4. Choose your custom header image and click on Open. LANconfig then starts the file upload.

After uploading successfully, the new header image appears the next time the Public Spot page is called.

 You can check that the large and small header images are displayed by your Public Spot by setting your browser window width to >800 px and then reducing the width of the window. The CSS technology automatically switches between the large and small pictures.

7.2.3 Additions to the Setup menu

Login-Text

The setting allows you to specify a custom text that the device inserts into the box on the login form of the Public Spot module's authentication page. To type umlauts, you should use their HTML equivalents (such as `ü` ; for `ü`), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

```
Herzlich Willkommen!<br/><i>Bitte füllen Sie das Formular aus.</i>)
```

SNMP ID:

2.24.33

Telnet path:

Setup > Public-Spot-Module

Possible values:

Any string, max. 254 characters from

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

Default:

7.3 Independent user registration - simple Login

As an alternative to independent user login via e-mail or SMS (text message), you have the ability to automatically perform login and authentication by Public Spot users using a RADIUS server once the user accepts the terms of use for the WLAN network.

7.3.1 Independent user authentication (Smart Ticket)

Devices operating a Public Spot provide users with time-limited access to wireless networks. Until now an administrator account was necessary to create a login on a device with the Public Spot. For employees at a hotel reception desk, for example, you can set up an administrator account that only has the function rights to create Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests for access to the wireless network.

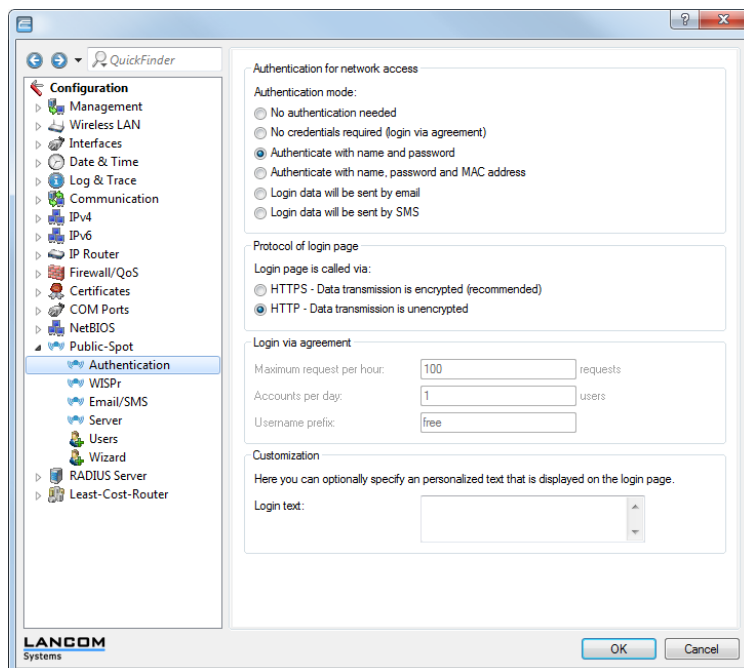
However, the easy voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network from the homepage of the Public Spot, and send it to themselves by e-mail or SMS (text message). In order to send e-mail, an SMTP account must be fully set up in the device settings. To send SMS/text messages the device uses an external SMS provider, which can charge fees to the Public-Spot operator or user, if desired.

Alternatively, the device gives you the ability to handle the login for Public Spot users transparently using a RADIUS server. In this case, the user login is preceded by checking the terms of use, whereby the user must first consent to the terms of use stored on the device before automatically receiving access to the Public Spot (one-click login). The creation of credentials by the user via e-mail or SMS does not apply for this authentication method.

7.3.2 Enhancements to LANconfig

Overview of authentication modes

In this window, specify the settings for authentication to the network.



The following authentication modes are available:

- **No authentication required**

Users get free access to the Public Spot, authentication is not required.

! Do not use this setting if your device has unlimited access to the Internet.

- **No credentials required (login after agreement)**

Users get free access to the Public Spot after they accept the operator's terms of use (one-click login). With a RADIUS server, login is completely transparent for the user. The prerequisite is that you have set up an individual welcome page with its own terms of use: In this case, the Public Spot initially forwards a user to the welcome page, where he must agree to the terms of use. After confirmation, the device automatically creates a user account according to the default values in the **Add user wizard** (under **Public-Spot > Wizard**) and provides access to the connected network.

Under **Login after agreement** you specify the framework conditions for the creation of free user accounts by the RADIUS server:

- **Maximum requests per hour:** Specify how many users per hour can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.
- **Accounts per day:** Specify how many accounts a user may create per day. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot for the rest of the day.
- **Username prefix:** Enter a prefix which can be used to identify the user in the RADIUS user table that the device created automatically after confirmation of the terms of use.

! To load a custom welcome page (htm, html) on the device, use the upload function under **Device > Configuration management > Upload certificate or file** and reference this file under **Public-Spot > Server > Page-Table > Welcome** in the field **Page address (URL)** with

file://pbspot_template_welcome. Templates for a welcome page and detailed information for uploading your own templates is available on the Internet in the LANCOM Support Knowledge Base under [Implementing your own websites](#).



The terms featured on the Welcome screen are not to be confused with the terms-of-use page itself. The **Terms of use page** is a special page that is displayed only after a separate activation in connection with notification by e-mail/SMS.



If no welcome page is set up, the device displays an error message when accessing the Public Spot.

■ Authenticate with name and password

Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher.

■ Authenticate with name, password and MAC address

Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher. For this login mode, the MAC address of the client must also match the one stored in the user list by the administrator.

■ Login data will be sent by e-mail

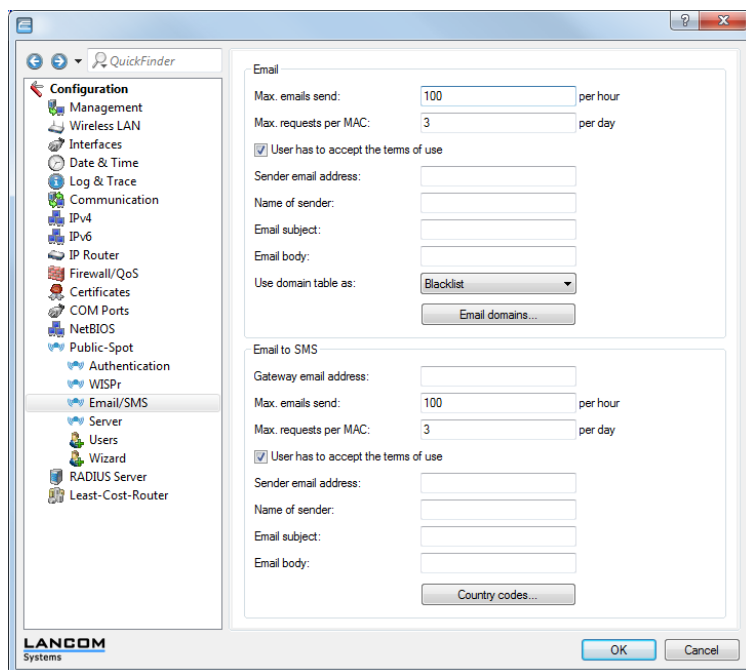
Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent via e-mail. No action by an administrator is necessary.

■ Login data will be sent by SMS (text message)

Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent by SMS (text message). No action by an administrator is necessary.

Configuring e-mail/SMS authentication

You define the settings for sending the login credentials via e-mail or SMS in the dialog **Public Spot > E-mail/SMS**.



You have following configuration options:

- **Max. e-mails send:** Here, enter the maximum number of e-mails that the Public Spot module may send per hour to users authenticating via e-mail. Lower the value to reduce the number of new users per hour.
- **Max. requests per MAC:** Specify how many different sets of credentials the device can provide to a MAC address within one day.
- **User has to accept the terms of use:** If you select this option, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering via e-mail/SMS.



Remember to upload a page with terms and conditions onto the device before you enable this option. Otherwise, the device will only show the user a placeholder instead of the terms and conditions.

- **Sender e-mail address:** Enter the e-mail address that your e-mail contains as the return address, e.g. `support@providerX.org`.
- **Name of sender:** Specify the name shown to your users as the sender of the e-mail, e.g. `Provider X`. If you leave this field blank, the device automatically enters the default text as described in the following section.
- **E-mail subject:** Type the subject line for the e-mail. If you leave this field blank, the device automatically enters the default text as described in the following section.
- **E-mail body:** Type the message text for the e-mail. You can use the following variables:

\$PSpotPasswd

Placeholder for user-specific password for the Public Spot access.

\$PSpotLogoutLink

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL enables Public Spot users to log off from the Public Spot. This may be useful if the session window (which also contains this link) that is normally displayed after a successful login is blocked by the browser or closed by the user.

If you leave this field blank, the device automatically enters the default text as described in the following section.

- **Use domain table as:** Specify whether the device uses the table **E-mail domains** as a blacklist or whitelist. This definition sets which e-mail addresses or domains may be entered by your Public Spot users in order to register.
 - **Blacklist:** Registration is permitted on all e-mail domains except those in this table.
 - **Whitelist:** Registration is possible only via the e-mail domains that are present in this table.
- **Gateway e-mail address:** Here you enter the IP address or the hostname of the gateway server, which converts the e-mail into SMS. If the provider expects to find the mobile phone number in the local part of the e-mail, you can use the variable `$PSpotUserMobileNo`.
- **Country codes:** In this table, enter the country codes accepted by the device. Country codes can be entered directly or with a prefixed double-zero, for example for Germany 49 or 0049.



This table acts as a whitelist. You **must** define country codes in order for the login data to be delivered.

7.3.3 Additions to the Setup menu

Authentication mode

Your device supports different types of authentication for network access with a Public Spot. To start with, you can specify whether a user needs to log in at all. The Public Spot stores the credentials in the user table. If you choose to use a registration procedure, you have two options:

- Login is performed with either a username and password, or additionally with the physical or MAC address. In this case, the administrator communicates the access credentials to the users by means of a printout.
- The login is performed using the username and password, which the user generates themselves. Access credentials can be automatically sent to users that login for first time either by e-mail or SMS (text message).
- The login is automatically performed via a RADIUS server after the user has accepted the terms of use on the welcome page that the administrator set up. The access credentials remain hidden from the user, and the user does not need

them. The creation of a user account on the RADIUS server is only for the internal administration of the associated users.

SNMP ID:

2.24.1

Telnet path:**Setup > Public-Spot-Module > Authentication-Mode****Possible values:**

None

User+password

MAC+user+password

E-mail

E-mail2SMS

Login via agreement

Default:

None

Authentication modules

In this menu option you define individual parameters for using the network login, and you specify how and with what parameters the authentication is performed and the login data is transmitted.

SNMP ID:

2.24.41

Telnet path:**Setup > Public-Spot-Module > Authentication-Module****Login after consent agreement**

In this menu, you specify the settings for automatic login and authentication via RADIUS.

SNMP ID:

2.24.41.4

Telnet path:**Setup > Public-Spot-Module > Authentication-Module****User accounts per day**

This entry displays the number of accounts that a user can create on one day for the designated login mode. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot on the specified day.

SNMP ID:

2.24.41.4.2

Telnet path:**Setup > Public-Spot-Module > Authentication-Module > Login-via-Agreement****Possible values:**

0 to 65535

Default:

1

Username prefix

This entry contains the prefix which is added to the automatically generated Public Spot username, when it is automatically generated by the device in the login mode "No Authentication" (automatic login and authentication).

SNMP ID:

2.24.41.4.3

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > Login-via-Agreement

Possible values:

String, max. 10 characters

Default:

free

Maximum requests per hour

This entry indicates the maximum number of users per hour, which can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.

SNMP ID:

2.24.41.4.1

Telnet path:

Setup > Public-Spot-Module > Authentication-Module > Login-via-Agreement

Possible values:

0 to 65535

Default:

100

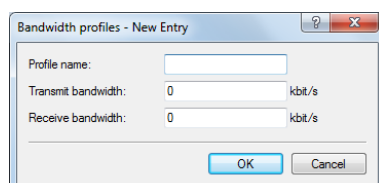
7.4 Bandwidth profile

As of LCOS 8.82 you have the option of setting up bandwidth profiles for Public Spot users.

7.4.1 Enhancements to LANconfig

Manage bandwidth profiles

Using the window **Public-Spot > Wizard > Bandwidth profiles**, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Create Public Spot account** in WEBconfig.



In order to edit the entries in the table **Bandwidth profiles**, click on the button **Add....** The entries in the edit window have the following meaning:

- **Profile name:** Enter the name for the bandwidth profile here.
- **TX bandwidth:** Enter the maximum uplink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value 1024.
- **RX bandwidth:** Enter the maximum downlink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value 1024.

Assigning bandwidth profiles

The following steps describe how you assign the available bandwidth profiles to a Public Spot user.

1. Open WEBconfig.
2. Start the add user wizard under **Setup Wizards > Create Public Spot account**.
3. Assign the new user an appropriate profile from the selection list **Bandwidth profile**.

The screenshot shows the 'Create Public Spot account' wizard. The 'Bandwidth profile' dropdown menu is highlighted with a red box, showing the following options: Visitor, Visitor, Standard (selected), and Premium.

When creating a new user, the RADIUS server automatically assigns the upper and lower boundaries of the bandwidth profile (not the bandwidth profile per se) to the associated account.

7.4.2 Additions to the Setup menu

Bandwidth profiles

In this table you manage individual bandwidth profiles. Using a bandwidth profile you have the option to selectively restrict the bandwidth (uplink and downlink) that is available to Public Spot users when their accounts are created.

SNMP ID:

2.24.19.17

Telnet path:

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

Profile name

Enter the name for the bandwidth profile here.

SNMP ID:

2.24.19.17.1

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard > Bandwidth-Profile

Possible values:

String, max. 255 characters

Default:**TX bandwidth**

Enter the maximum uplink bandwidth (in bps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value 1024.

SNMP ID:

2.24.19.17.2

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard > Bandwidth-Profile

Possible values:

0 to 4294967295

Default:

0

RX bandwidth

Enter the maximum uplink bandwidth (in bps), which should be available to Public Spot users. To limit the bandwidth, for example, to 1 Mbps, enter the value 1024.

SNMP ID:

2.24.19.17.3

Telnet path:

Setup > Public-Spot-Module > Add-User-Wizard > Bandwidth-Profile

Possible values:

0 to 4294967295

Default:

0

7.5 Dynamic VLAN assignment via RADIUS

As of LCOS 8.82 you have the ability to assign an individual VLAN ID to individual Public Spot users at login. Based on this ID you can, for example, set additional permissions and rules via the firewall, which are valid for the different users.

7.5.1 Enhancements to LANconfig

Assigning users to individual VLANs

Regardless of the assignment of a VLAN ID for the entire Public Spot module, the device offers you the option of separately assigning individual VLAN IDs for individual Public Spot users. This ID is automatically assigned by the RADIUS server to your users after successful authentication. In this way it is possible, for example, to classify different Public Spot users in separate networks with different access rights and access options without having them login to separate SSIDs or requiring you to publicize the availability of various networks (e.g., networks for different customer types). The relevant rules can be realized via the firewall by specifying the VLAN ID of the respective user/the relevant user groups as the source tag.

! An enabled VLAN module is a prerequisite for the functions described above.

- Open the **User table** in the dialog **RADIUS server General** and click **Add...** to create a new user.
- Assign an individual VLAN ID to the new user with the input field **VLAN-ID**. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value 0 disables the assignment of an individual VLAN ID.

! For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for the clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server as low as possible under **IPv4 > DHCPv4**. Possible values (in minutes) include, for example:

- **Maximum lease time:**2
- **Default lease time:**1

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using an external DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

! By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

7.5.2 Additions to the Setup menu

VLAN ID

Using this input field you assign the user an individual VLAN ID. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value 0 disables the assignment of an individual VLAN ID.

! For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for clients to be transferred to the new network as quickly as possible, it is

necessary to set the lease time of the DHCP server – in the setup menu **Setup > DHCP** – as short as possible. Possible values (in minutes) include, for example:

- **Max.-Validity-Minutes:** 2
- **Default-Validity-Minutes:** 1

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using a different DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.



By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

SNMP ID:

2.24.42.8

Telnet path:

Setup > RADIUS > Server > Users

Possible values:

0 to 4094

Default:

4

7.6 Automatic re-login

Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) It is similar for mobile LAN clients (e.g., notebooks) which have to be disconnected from the network for a short time for a change of location (e.g., for changes from a lecture hall to a library in a college). In all of these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

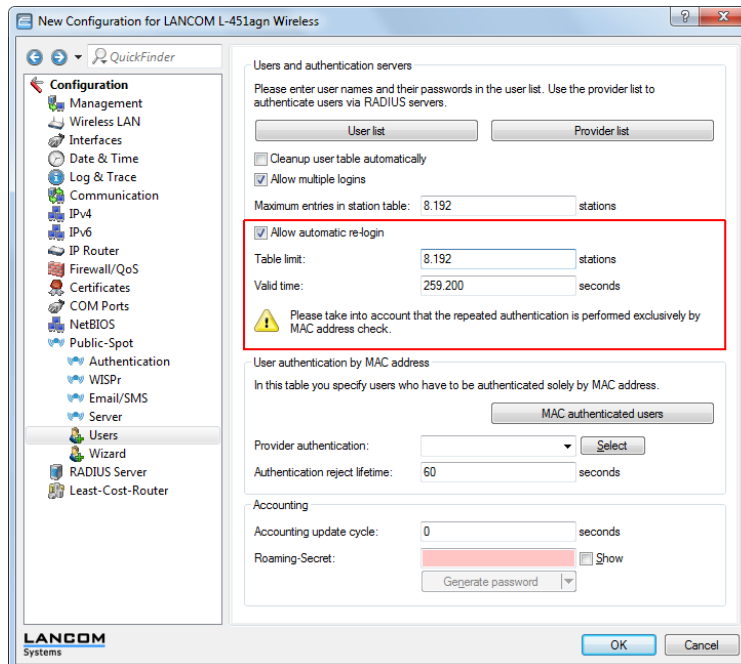
With automatic re-login, the user only has to be identified on the Public Spot once. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.



The authentication is only performed on the MAC address of the client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

The settings for automatic re-login can be found in LANconfig in the device configuration under **Public Spot > Users** in the section **Users and authentication servers**.



The selection box **Allow automatic re-login** enables this function.

You specify the number of clients (maximum 65536) in the field **Automatic re-login table limit** that the re-login function may use.

In the field **Automatic re-login valid time** you specify how long the Public Spot stores the credentials of a client in the table for a re-login. After this period expires, the Public Spot user must log in again using the login page of the Public Spot in the browser.

7.6.1 Additions to the Setup menu

Automatic re-login

Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) In these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

With automatic re-login, the user only has to be identified on the Public Spot the first time that they are within the cell. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.

 Please note that authentication only takes place using the MAC address when auto-re-login is enabled.

In this menu you configure the parameters for automatic re-login.

SNMP ID:

2.24.50

Telnet path:

Setup > Public-Spot-Module

Operating

Enable or disable the automatic re-login with this action.



The authentication is only performed on the MAC address of the WLAN client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

SNMP ID:

2.24.50.1

Telnet path:

Setup > Public-Spot-Module > Auto-Re-Login

Possible values:

Yes

No

Default:

No

Station table limit

You can increase the maximum number of clients that are allowed to use the re-login function to up to 65,536 participants.



While the device is operating, the only changes to the station table that take immediate effect are the additions to it. Restart the access point in order to immediately reduce the size of the station table.

SNMP ID:

2.24.50.2

Telnet path:

Setup > Public-Spot-Module > Auto-Re-Login

Possible values:

16 to 65536

Default:

8192

Exists timeout

This value indicates how long the Public Spot stores the credentials in the table of a WLAN client for a re-login. After this period (in seconds) has expired, the Public Spot user must log in again using the login page of the Public Spot in the browser.



If a Public Spot user has a time quota that is smaller than the timeout interval set here, this parameter has no effect. An automatic re-login does not occur if the user has the status "unauthenticated".

SNMP ID:

2.24.50.3

Telnet path:

Setup > Public-Spot-Module > Auto-Re-Login

Possible values:

Max. 10 characters

Default:

259200

7.6.2 Additions to the Status menu

Automatic re-login

This menu contains the status values for the automatic re-login of the Public Spot users.

SNMP ID:

1.44.8

Telnet path:

Status > Public-Spot

Station table

This table contains the login credentials of users who are logged in to the Public Spot. Based on this table, the Public Spot can allow users to automatically login again (re-login).

SNMP ID:

1.44.8.1

Telnet path:

Status > Public-Spot > Auto-Re-Login

MAC address

Contains the MAC address that the WLAN client last used to login to the Public Spot.



The authentication is only performed on the MAC address of the WLAN client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

IP address

Contains the IP address that the WLAN client last used to login to the Public Spot.

Username

Contains the username with which the user was last logged in to the Public Spot.

Exist-Timeout

Specifies the time, in seconds, during which the user can automatically log on to the Public Spot without having to authenticate again.

7.7 Login via WISPr

To support IEEE802.11u and Hotspot 2.0, LOCS 8.82 additionally offers you an interface to WISPr protocols, in order to automatically offer Smart or Legacy clients, which do not support 802.11u, automatic login to your hotspot. Please note that, as the operator, your Internet service provider and also the user's device must have the appropriate technical infrastructure.

7.7.1 Automatic authentication via WISPr

Your device provides an interface for authentication via WISPr. The **WISPr** standard is the technological predecessor of the 802.11u and Hotspot 2.0 specifications. The acronym stands for **Wireless Internet Service Provider roaming** and designates both a process and a protocol that allow users of WLAN enabled devices to roam seamlessly between the WLANs of different operators – and, therefore, between their Internet service providers. The idea behind it is similar to that of 802.11u and Hotspot 2.0; however, it requires more comprehensive support by the respective users.

Using the WISPr protocol, you can provide logins and network usage on your hotspot in a manner similar to Hotspot 2.0, even for end devices that no longer support Hotspot 2.0. The prerequisite is that your service provider provides the necessary infrastructure. Support for the user's device is provided either by the operating system or a suitable app (smart client). This client handles authentication to the hotspot for the user. If no credentials are available for the relevant network, the client queries the user for valid credentials at the system level. In any case, this eliminates the user having to log in via a login web page in the browser.

Because of its age, almost all current end devices with iOS, Android and Windows 8 support the WISPr protocol. In addition, larger WLAN Internet service providers often have their own apps to make the login for their clients easier: These apps include a preconfigured database of the provider's own hotspots and, optionally, those of their roaming partners. The authentication process corresponds to the following schema:

1. A customer installs his provider's hotspot app to act as a client, which provides a database of preconfigured hotspot SSIDs.
2. The client connects automatically with one of the hotspots and sends a HTTP-GET-Request to a random URL to test if direct Internet access is available or the Public Spot requires authentication.
3. In HTTP-Redirect the hotspot sends a WISPr-XML-Tag with the Login-URL.
4. The client sends its login data to the Login-URL in an HTTP-Post.

Example for an XML-Tag in redirect:

```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess
GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
  </WISPAccessGatewayParam>
</HTML>
```

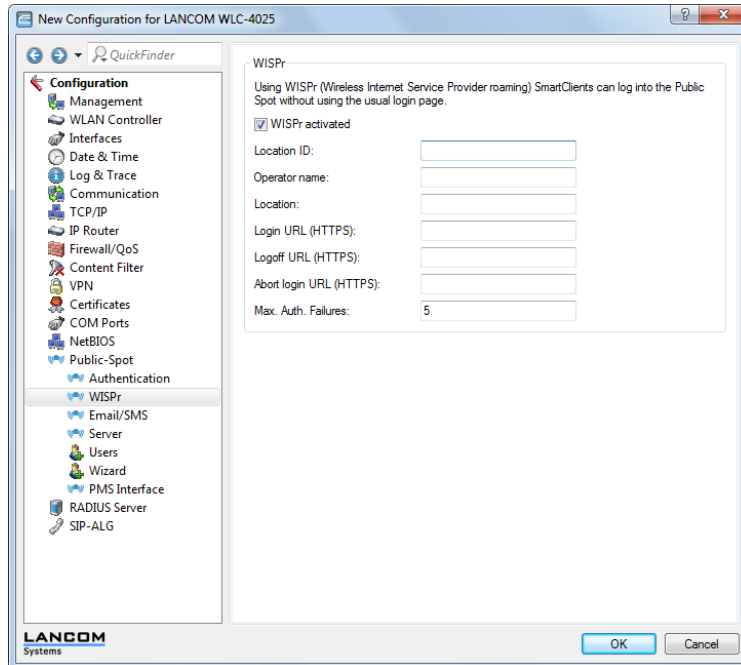


In order to use WISPr, the device must have an SSL certificate and a private key installed. Further information about loading these objects on your device can be found in the LANCOM techpaper "Certificate Management in Public Spots". The certificate must either be signed by a trusted authority or – if it is a self-signed certificate – be imported as a trusted certificate on the client. Otherwise the client will reject the login via WISPr.

7.7.2 Enhancements to LANconfig

Configuring WISPr

Configure the WISPr function of your device in the menu **Public Spot > WISPr**.



In this window you have the following options:

- **WISPr activated:** Enable or disable the WISPr function for the device.
- **Location ID:** Use this ID to assign a unique location number or ID for your device, for example, in the format `isocc=<ISO_Country_Code>, cc=<E.164_Country_Code>, ac=<E.164_Area_Code>, network=<SSID/ZONE>`
- **Operator name:** Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.
- **Location:** Describe the location of your device, e.g., `CafeX_Market3`. This helps to better identify a user in your hotspot.
- **Login URL (HTTPS):** Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider. Any external URL can be entered or the LANCOM Public Spot itself. If the LANCOM Public Spot should authenticate users using WISPr, enter the URL in the format `https://<FQDN-of-the-LANCOM>/wisprlogin`. For "wisprlogin" in the example, any freely defined path can be used.
- **Logoff URL (HTTPS):** Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider. The same rules apply as for the login URL.
- **Abort login URL (HTTPS):** Enter the HTTPS address to which the device forwards a WISPr client if authentication fails. The same rules apply as for the login URL.



The three URLs must be different, if the Public Spot is used in the LANCOM domain, for example:

- Login URL: `https://<FQDN-of-the-LANCOM>/wisprlogin`
- Logoff URL: `https://<FQDN-of-the-LANCOM>/wisprlogoff`
- Abort-Login-URL: `https://<FQDN-of-the-LANCOM>/wisprabort`

Finally, for test purposes, you can also configure an URL with IP addresses. In a production system, the client will check the FQDN of the certificate!

- **Max. auth. failures:** Enter the maximum number of failed attempts which the login page of your Internet service provider allows. If the Public Spot is used, the Public Spot rejects further login attempts by the specified client after this number of failed attempts.

RADIUS attributes transmitted via WISPr

If you enable WISPr and you use an external RADIUS server, the Public Spot transmits the attributes (access request):

- **Location ID**
- **Location name**
- **Logoff URL**

These attributes are subset of the values configured in the previous section. The provider or roaming broker can use them to identify the location of the client for accounting purposes. Vendor Specific Attributes (VSA) are used with the IANA Private Enterprise Number (PEN) 14122.

The Public Spot processes the attributes (access accept) from an external RADIUS server:

- **Redirection URL:** URL to which a client should be redirected after login. This function is not supported by all smart clients.
- **Bandwidth max up:** Maximum uplink bandwidth available to the client.
- **Bandwidth max down:** Maximum downlink bandwidth available to the client.
- **Session terminate time:** Time when the client should be automatically de-authenticated. According to ISO 8601, the format is `YYYY-MM-DDThh:mm:ssTZD`. If "TZD" is not entered, the client is de-authenticated according to the local time on the Public Spot.
- **Session terminate end of day:** The value of this attribute can be either 0 or 1. It indicates whether the client is de-authenticated on the Public Spot at the end of the accounting day.

For accounting purposes, the Public Spot uses the following attributes:

- **Location ID**
- **Location name**

7.7.3 Additions to the Setup menu

Disconnect login URL

Enter the HTTPS address to which the device forwards a WISPr client if authentication fails.

SNMP ID:

2.24.42.7

Telnet path:

Setup > Public-Spot-Module > WISPr

Possible values:

HTTPS URL, max. 255 characters

Default:

Operating

Enable or disable the WISPr function for your device.

SNMP ID:

2.24.42.1

Telnet path:

Setup > Public-Spot-Module > WISPr

Possible values:

No

Yes

Default:

No

Login URL

Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider.

SNMP ID:

2.24.42.5

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

HTTPS URL, max. 255 characters

Default:**Logout URL**

Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider.

SNMP ID:

2.24.42.6

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

HTTPS URL, max. 255 characters

Default:**Maximum authentication errors**

Enter the maximum number of failed attempts which the login page of your Internet service provider allows.

SNMP ID:

2.24.42.8

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

0 to 65535

Default:

5

Operator name

Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.

SNMP ID:

2.24.42.3

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

String, max. 255 characters, with the following restrictions:

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

Default:**Location ID**

Use this ID to assign a unique location number or ID for your device, for example, in the format
 isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,
 network=<SSID/ZONE>

SNMP ID:

2.24.42.2

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

String, max. 255 characters, with the following restrictions:

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

Default:**Location name**

Describe the location of your device, e.g., CafeX_Market3. This helps to better identify a user in your hotspot.

SNMP ID:

2.24.42.4

Telnet path:**Setup > Public-Spot-Module > WISPr****Possible values:**

String, max. 255 characters, with the following restrictions:

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

Default:

7.8 PMS interface

As of LCOS 8.82, you have the option of connecting the Public Spot module with the hotel property management system from Micros Fidelio in order to automatically provide your guests with access to your Public Spot when they register for their room. There is no need for an additional Public Spot administrator, e.g., for creating vouchers.



Currently, the PMS interface is only available for the following device types and series:

- LANCOM 1780 series

- LANCOM 1781 series
- LANCOM WLC-4006
- LANCOM WLC-4006+
- LANCOM WLC-4025
- LANCOM WLC-4025+
- LANCOM WLC-4100
- LANCOM 7100 VPN
- LANCOM 7100+ VPN
- LANCOM 9100 VPN
- LANCOM 9100+ VPN

7.8.1 Interface for property management systems

If you use a property management system (PMS), certain device types and series give you the option of connecting your Public Spot module with your PMS database via the PMS interface. If you operate a hotel, this offers you the possibility of automatically providing your guests with access to your Public Spot when they register. This access can optionally be free of charge or fee-based (using prepaid time credits), whereby all fees are charged to the guest's bill for their room. The last name, room number and, optionally, an additional security ID (for example, registration number or departure date) are used as login data.

In contrast to a voucher solution, using the PMS interface gives you the advantage of not requiring any additional administrative steps for the setup and management of a Public Spot user account. The device creates a user account by itself as soon as the user accesses the Public Spot and logs in with his registration data. Any future changes for this guest (room change, departure date change, check-out, etc.), which affect registration, are retrieved autonomously from your PMS.

The following login methods are currently supported:

1. Voucher
2. PMS login
3. PMS login and voucher
4. E-mail
5. SMS

With login method (2), the login, for example, for hotel guests, can be based on the room number and last name, while you sell vouchers to your guests in your restaurant. Of course, even with the PMS interface enabled, you still have the option to issue vouchers, for example, for day guests or visitors.



The login method is configured globally for each device, and is thus the same for all SSIDs or networks.



The PMS interface currently only includes support for hotel property management systems from Micros Fidelio via TCP/IP.



Currently, the PMS interface is only available for the following device types and series:

- LANCOM 1780 series
- LANCOM 1781 series
- LANCOM WLC-4006
- LANCOM WLC-4006+
- LANCOM WLC-4025
- LANCOM WLC-4025+
- LANCOM WLC-4100
- LANCOM 7100 VPN
- LANCOM 7100+ VPN

- LANCOM 9100 VPN
- LANCOM 9100+ VPN

7.8.2 Functional description

If you enable the PMS interface and provide a free or fee-based login page, the Public Spot portal page displays new input fields, which guests can use to authenticate by entering their surname, the room number and, if applicable, a further security identifier. The type of this identifier is set in the Setup menu; options include a registration number or the guest's arrival/departure date. If you have allowed access to your hotspot as a fee-based service, a drop-down menu additionally appears, which guests use to select the prepaid time quota or tariff/rate that they want to buy (e.g. 1 min for EUR 0.20, or 1 hours for EUR 1). The PMS working in the background automatically charges the costs to the room bill.

Every time a guest logs in to the Public Spot, the device initiates a comparison of the entered login data with that in the PMS. The PMS informs the device if it detects a valid match. The device then creates a new session for the guest and makes an entry in the corresponding accounting table (WEBconfig: **Status > PMS-Interface > Accounting**). The device records all hotel guests, and the corresponding prices, who have logged on via the PMS interface, irrespective of whether the connection is free or charged. The device then activates user access to the Internet.

A user with charged access can purchase additional time while logged on. Users who log off before the time quota expires can resume the session at a later time by selecting the corresponding field on the login page. The device stores the session until it becomes invalid, i.e. when the time quota is used up or when the PMS informs the device that the guest has departed. For a new login and synchronization with the PMS, the device recognizes that there is still a valid user account and continues using it instead of creating a new one.

If there is a change to the registration information (such as the room number), then an existing session initially remains unaffected. Only when the current session is closed and the guest logs on to the Public Spot again is it necessary to authenticate with the modified credentials. An exception occurs when a guest is checked-out of the PMS: In this case, the device immediately terminates an existing session.

! Your users should make sure that they log out properly from the Public Spot. Without a proper logout (caused by closing the browser, disconnecting the network, switching off the device, etc.) the user is considered to be still logged in. This can cause a problem for the user at login if you, as the Public Spot operator, have not allowed multiple logins.

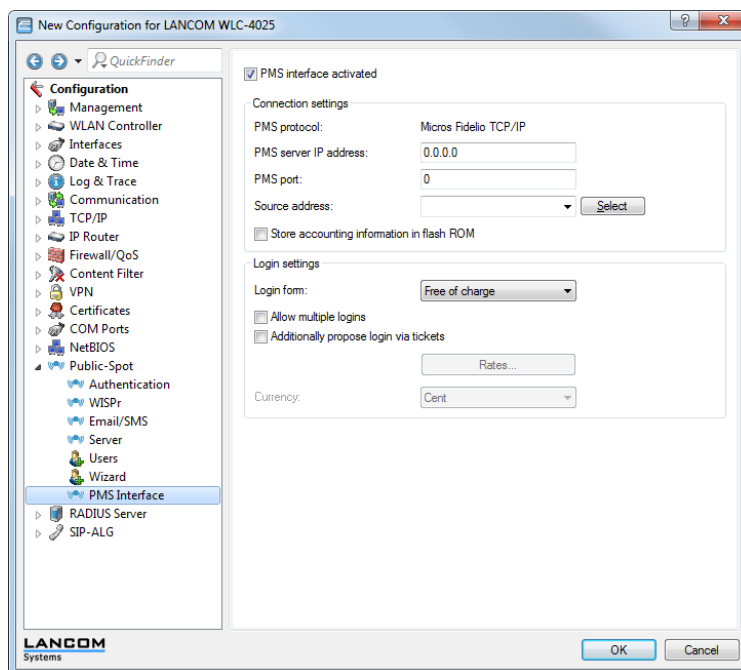
Using *Station monitoring*, you can automatically log off these users after a specified idle time. This feature is off by default. However, for fee-based access, you absolutely should enable this. Otherwise, the device's automatic internal logout will only occur after the user account has expired, i.e., when the purchased time credit has been used up completely.

! A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

7.8.3 Enhancements to LANconfig

Configuring the PMS interface

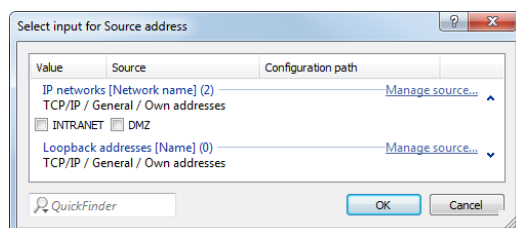
Configure the PMS interface of your device in the menu **Public Spot > PMS-Interface**.



In this window you have the following options:

- **PMS interface activated:** Enable or disable the PMS interface for the device.
- **PMS protocol:** Identifies the protocol used by your property management system. Currently, only support for hotel property management systems from Micros Fidelio is available via TCP/IP.
- **PMS server IP address:** Enter the IPv4 address of your PMS server.
- **PMS port:** Enter the TCP port where your PMS server is accessible.

- **Sender address:** Click on the **Select** button, in order to configure another address where your PMS server sends its reply messages. By default, the PMS server sends its replies back to the IP address of your device without having to enter it here.



Possible formats for entering the address include:

- Name of the IP network (ARF network), whose address should be used.
- INT for the address of the first Intranet
- DMZ for the address of the first DMZ

! If an interface with the name "DMZ" already exists, the device will select that address instead.

- LBO...LBF for one of the 16 loopback addresses or its name

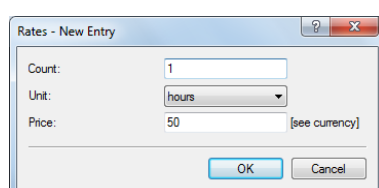
! The device always uses **unmasked** loopback addresses, even on masked remote stations!

- Any IPv4 address

- **Store accounting information in flash ROM:** Enable or disable whether your device stores accounting information in regular intervals on the internal flash-ROM. By default this occurs hourly, but you can change the interval using the setup menu. Enable this option in order to prevent a complete loss of accounting information in case of a power outage.

! Please note that frequent writing operations to this memory will reduce the lifetime of your device.

- **Login form:** Choose the login form that will be shown as a portal page for your PMS interface. Possible values include:
 - **Free-of-charge:** Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.
 - **Subject to charge:** Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate on the hotspot on the portal page with their username, room number and select a tariff.
- **Allow multiple logins:** Enable or disable this if you want to allow a hotel guest to use the same credentials to login to the hotspot with multiple devices.
- **Additionally propose login via tickets:** Enable or disable whether you also want to allow login with vouchers in addition to login with the combination of username/room number.
- **Rates:** If you offer fee-based Internet access, you manage the tariff rates for accounting using this table.



- **Count:** Enter the rate for the time quota, for example, 1. Combined with the unit, this is the value shown in the screenshot above, e.g., 1 hour.

- **Unit:** Select the unit for the time quota from the list. Possible values include: `Minutes`, `Hours`, `Days`
- **Price** Enter the amount charged for the time quota. Combined with the unit, this is the value shown in the screenshot above, e.g., 50 Cent.



A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

- **Currency:** If you offer fee-based Internet access, select the currency that you use to bill the time quotas that you offer (time quotas are set up using the tariff table). This unit is also displayed on the portal page. Please note that this currency must match the one on the PMS server. Possible values include:
 - Cent
 - Penny

7.8.4 Additions to the Status menu

PMS interface

This status menu includes the status values for the PMS interface (PMS = property management system).

SNMP ID:

1.78

Telnet path:

Status

Accounting

This table is an overview of the accounting information, which is available for all hotel guests that have used the Public Spot via the PMS interface. The device collects accounting information regardless of whether the specified user has a connection that is free or charged. At the same time, this table also provides an overview of which guests are active and inactive on the Public Spot.

SNMP ID:

1.78.2

Telnet path:

Status > PMS-Interface

Reservation number

Reservation number that the hotel guest was assigned in your PMS.

Username

Surname of the hotel guest as it was entered in your PMS.

Room number

Room number that the hotel guest is occupying

MAC address

MAC address of the device for which the accounting data is collected

Comment

Comment automatically generated by the device

Time budget

Prepaid time quota that the hotel guest paid for

Volume budget

Prepaid volume quota that the hotel guest paid for

! This column is a placeholder. Setting the volume quota is currently not available.

Total volume

Data volume that the user consumed in all sessions (previous and current). The total volume reflects the real-time value of the overall data traffic generated by the hotel guest since registration.

! Subtracting the initial total volume from the total volume results in the volume that the user consumed in his last active session.

Total time

The length of all of the hotel guest's sessions (previous and current) on the Public Spot.

! Subtracting the initial total time from the total time results in the length of time that the user was logged in to the Public Spot during his last active session.

Operating

This shows whether the end device of the specific hotel guest is currently logged on to the Public Spot and accounting data is being collected.

Last updated

This shows when the device last updated accounting data. You determine the update interval in the setup menu using the parameter **Update accounting table period**.

Initial total volume

Data volume that the user consumed in all previous sessions.

! Subtracting the initial total volume from the total volume results in the volume that the user consumed in his last active session.

Initial total time

The length of all of the hotel guest's previous sessions on the Public Spot.

! Subtracting the initial total time from the total time results in the length of time that the user was logged in to the Public Spot during his last active session.

Connection

This status value displays the activity on the PMS interface.

SNMP ID:

1.78.1

Telnet path:

Status > PMS-Interface

Possible values:

On

Off

7.8.5 Additions to the Setup menu

PMS interface

You make all settings for the PMS interface (PMS = property management system) using the tables and parameters in this menu.

SNMP ID:

2.64

Telnet path:**Setup****Accounting**

In this menu you configure the transfer of accounting information from your device to your PMS.

SNMP ID:

2.64.10

Telnet path:**Setup > PMS-Interface****Clean-up accounting table period**

Using this entry you configure the interval that the device uses to clean up expired sessions from the internal accounting table in the status menu. If the value is 0, automatic clean-up is disabled.

SNMP ID:

2.64.10.3

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

60

Save to flash ROM

Enable or disable whether your device stores accounting information in regular intervals on the internal flash-ROM. By default this occurs hourly, but you can change the interval using the setup menu. Enable this option in order to prevent a complete loss of accounting information in case of a power outage.



Please note that frequent writing operations to this memory will reduce the lifetime of your device.

SNMP ID:

2.64.10.1

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

No

Yes

Default:

No

Save to flash ROM period

Using this entry you configure the interval that the device uses to store collected accounting information to the internal flash ROM.



Please note that frequent writing operations to this memory will reduce the lifetime of your device.

SNMP ID:

2.64.10.2

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

15

Update accounting table period

Using this entry you configure the interval that the device uses to update the internal accounting table in the status menu. If the value is 0, the update is disabled and the status table does not display any values.

SNMP ID:

2.64.10.4

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

15

Login form

In this menu you make specific settings for the PMS for the login/portal pages which are displayed to your guests in case of unauthorized access attempts on the hotspot.

SNMP ID:

2.64.11

Telnet path:**Setup > PMS-Interface****Free VIP status**

In this table, you locally manage the VIP categories from your PMS.

SNMP ID:

2.64.11.6

Telnet path:**Setup > PMS-Interface > Login-Form****Status**

Enter the VIP category from your PMS for the members that you want to provide with free Internet access.

For example, if you set up three VIP statuses (VIP1, VIP2, VIP3) for your PMS server, but you only want to offer hotel guests in category VIP2 free Internet access, enter the corresponding ID here.

SNMP ID:

2.64.11.6.1

Telnet path:

Setup > PMS-Interface > Login-Form > Free-Of-Charge-VIP-Status

Possible values:

String, max. 20 characters

Default:**Fidelio free additional check**

Select the additional ID that a hotel guest uses – in addition to their username and room number – to authenticate on the Public Spot if you offer free Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.3

Telnet path:

Setup > PMS-Interface > Login-Form

Possible values:

none

Reservation number

Arrival date

Departure date

First name

Profile number

Default:

none

Fedelio free VIP additional check

Select the additional ID used by a VIP – in addition to their username and room number – to authenticate on the Public Spot if you offer your VIPs free Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.5

Telnet path:

Setup > PMS-Interface > Login-Form

Possible values:

none

Reservation number

Arrival date

Departure date

First name

Profile number

Default:

none

Fedelio charge additional check

Select the additional ID used by a hotel guest – in addition to their username and room number – to authenticate on the Public Spot if you offer fee-based Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.4

Telnet path:

Setup > PMS-Interface > Login-Form

Possible values:

none

Reservation number

Arrival date

Departure date

First name

Profile number

Default:

Reservation number

PMS login form

Choose the login page to be displayed by the portal page for your PMS interface.

SNMP ID:

2.64.11.2

Telnet path:

Setup > PMS-Interface > Login-Form

Possible values:

- `Free-of-charge`: Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.
- `Subject to charge`: Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate on the hotspot on the portal page with their username, room number and select a tariff.
- `free-VIP`: Select this setting, if you want to offer your otherwise fee-based Internet access free of charge to VIPs. Although your VIPs see the login screen for fee-based access, they will not be billed any fees.

Default:

Free-of-charge

PublicSpot login form

Enable or disable whether the portal page displays the Public Spot's own login screen. If you disable this setting, Public Spot users that use a combination of username and password as credentials (e.g., predefined or users with vouchers) can no longer login to the device.

SNMP ID:

2.64.11.1

Telnet path:**Setup > PMS-Interface > Login-Form****Possible values:**

No

Yes

Default:

No

Rate

If you offer fee-based Internet access, you manage the tariff rates for accounting using this table.

SNMP ID:

2.64.9

Telnet path:**Setup > PMS-Interface****Rate**

Enter the rate for the time quota, for example, 1. Combined with the unit, the value is, for example, 1 hour.

SNMP ID:

2.64.9.1

Telnet path:**Setup > PMS-Interface > Rate****Possible values:**

0 to 99999999999999999999

Default:**Unit**

Select the unit for the time quota from the list.

SNMP ID:

2.64.9.2

Telnet path:**Setup > PMS-Interface > Rate****Possible values:**

Hour(s)

Day(s)

Minute(s)

Default:

Hour(s)

Rate

Enter the amount charged for the time quota. Combined with the currency, the value is, for example, 50 Cent.

SNMP ID:

2.64.9.3

Telnet path:**Setup > PMS-Interface > Rate****Possible values:**

0 to 99999999999999999999

Default:**Operating**

Enable or disable the PMS interface for the device.

SNMP ID:

2.64.1

Telnet path:**Setup > PMS-Interface****Possible values:**

No

Yes

Default:

No

Guest name case sensitive

Enable or disable whether the device checks the last name for capitalization (case sensitively) against the name of the guest in the PMS database during login. If this setting is enabled, the guest's Public Spot access is rejected if the spelling and capitalization of his name does not match that transferred by the hotel.

SNMP ID:

2.64.12

Telnet path:**Setup > PMS-Interface****Possible values:**

No

Yes

Default:

Yes

Loopback address

Optionally enter a different address here (name or IP) to send the reply message to the PMS server. By default, the PMS server sends its replies back to the IP address of your device without having to enter it here.

SNMP ID:

2.64.4

Telnet path:**Setup > PMS-Interface****Possible values:**

- Name of the IP network (ARF network), whose address should be used.
- INT for the address of the first Intranet

- DMZ for the address of the first DMZ



If an interface with the name "DMZ" already exists, the device will select that address instead.

- LB0...LBF for one of the 16 loopback addresses or its name
- Any IPv4 address



If the sender address set here is a loopback address, these will be used **unmasked** on the remote client!

Default:**Multi-login**

Enable or disable this if you want to allow a hotel guest to use the same credentials to login to the hotspot with multiple devices.

SNMP ID:

2.64.13

Telnet path:

Setup > PMS-Interface

Possible values:

No

Yes

Default:

No

PMS port

Enter the TCP port where your PMS server is accessible.

SNMP ID:

2.64.5

Telnet path:

Setup > PMS-Interface

Possible values:

0 to 65535

Default:

0

PMS server IP address

Enter the IPv4 address of your PMS server.

SNMP ID:

2.64.3

Telnet path:

Setup > PMS-Interface

Possible values:

IPv4 address

Default:

No

PMS type

Identifies the protocol used by your property management system. Currently, only support for hotel property management systems from Micros Fidelio is available.

SNMP ID:

2.64.2

Telnet path:**Setup > PMS-Interface****Possible values:**

TCP/IP

Default:

TCP/IP

Separator

Using this entry you configure the separator that your PMS uses to transfer data records to an API. The Micros Fidelio specification, e.g., uses the pipe symbol by default (|, hex 7C).



You should not change this value if at all possible. An incorrect separator can lead to your PMS being unable to read the transmitted data records, and the PMS interface not working!

SNMP ID:

2.64.6

Telnet path:**Setup > PMS-Interface****Possible values:**

String, max. 1 characters

Default:

|

Currency

If you offer fee-based Internet access, select the currency that you use to bill the time quotas that you offer (time quotas are set up using the tariff table). This unit is also displayed on the portal page. Please note that this currency must match the one on the PMS server.

SNMP ID:

2.64.8

Telnet path:**Setup > PMS-Interface****Possible values:**

CENT

PENNY

Default:

CENT

Character set

Choose the character used by the PMS to transmit your guests' surnames to the device.

SNMP ID:

2.64.7

Telnet path:

Setup > PMS-Interface

Possible values:

CP850

W1252

Default:

CP850

8 LCMS

8.1 SSH configuration protocol in LANconfig

In conjunction with CC compliance (Common Criteria), LANconfig supports the configuration of LANCOM CC products via SSH or data transfer via SCP as of the LCOS version 8.82.

8.1.1 Enhancements to LANconfig

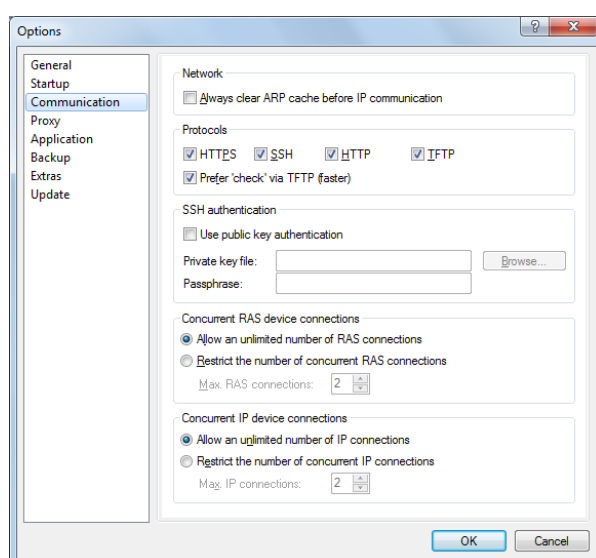
Device-specific settings for communications protocols

The transfer of configuration data when working with LANconfig can be handled by various protocols: HTTPS, SSH, HTTP or TFTP.

Widely available protocols are defined globally. In addition, it is possible to disable protocols for specific devices. However, it is not possible to re-enable a globally disabled protocol for an individual device.

Configuration of the global communication settings

The configuration of the communication protocols differentiates between the protocol strictly for testing the device and the protocols for other operations, such as firmware uploads, etc.:



LANconfig: **Extras > Options > Communication**

- **HTTPS, SSH, HTTP, TFTP**

When this is selected, you enable the individual protocols for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, SSH, HTTP and TFTP. If the transfer fails when using one of the selected protocols, LANconfig automatically tries the next protocol.

- **Prefer checks via TFTP**

The device evaluation only transfers small amounts of data with the system information. As such, it makes sense to perform device checks in the LAN by TFTP protocol. When this option is activated, LANconfig first uses the TFTP protocol to check the device, regardless of the communication protocols set previously. If the check via TFTP fails, then LANconfig attempts the protocols HTTPS, SSH, and HTTP.

■ **Using public key authentication**

If you have selected the SSH protocol, you can alternatively perform the authentication via a private key. In this case, the authentication dialog for password entry is not invoked. Enter the path to your private key file in the fields, and, if necessary, the passphrase that you used to encrypt the file. Load the corresponding public key with LANconfig or WEBconfig onto each device.



The global communication settings take precedence over the device-specific settings in order to prevent, for example, the central use of a protocol.

LANconfig menu structure

Using the menu bar, you can manage devices and their configurations, and you can customize the appearance and functioning of LANconfig.

File

The menu item **File** is used to manage devices in general, and to exit LANconfig as needed.

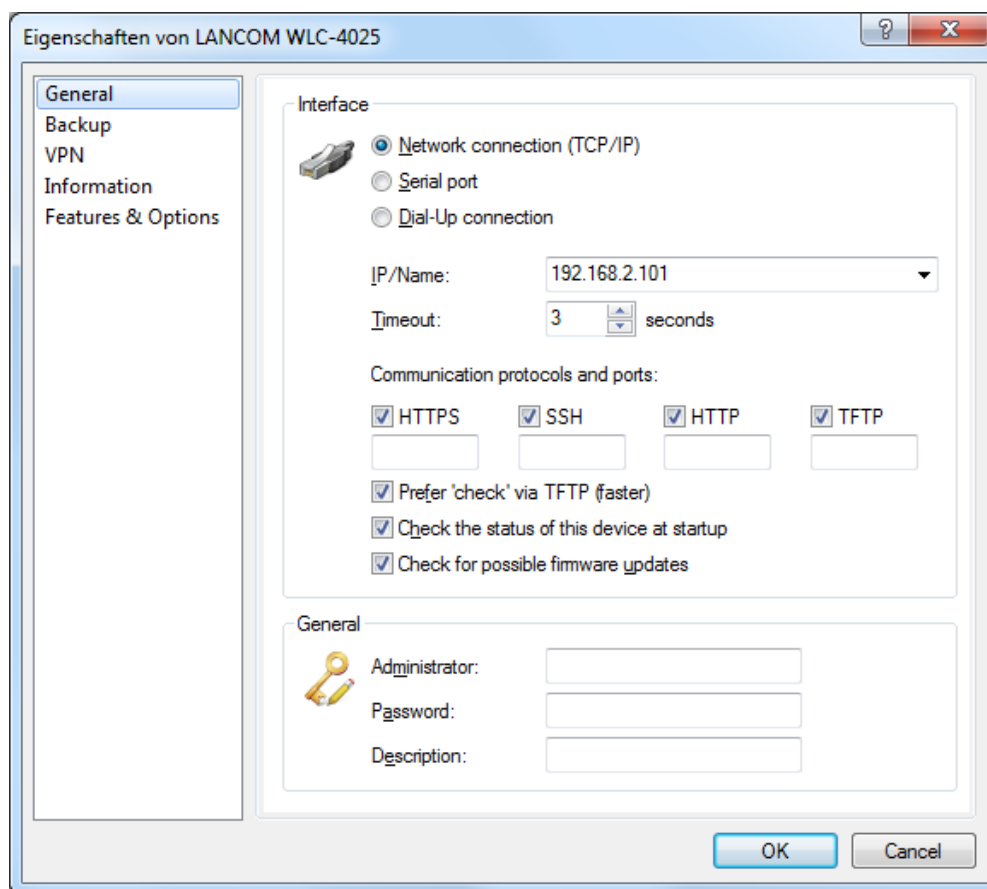
Add device

You can add a new device under **File > Add device**. A window is displayed where you can make the settings for the device, the connection, and backups.

General

Interface

In **Interface** you can configure the connection settings for a device.



Please select how the device is to be reached:

- **Network connection (TCP/IP):** Select this option if the device can be reached over an IP network.
- **Serial port:** Select this option if the device is connected directly to your computer's serial port.
- **Dial-up connection:** Select this option if the device can be reached via Dial-Up Networking.



Please note that some routers do not support remote configuration via a dial-up connection.

- **IP/Name:** Enter the IP address of the device. You can also enter a domain name (DN or FQDN) or a NetBIOS name. This name is checked at every access. LANconfig stores and uses the resolved IP address. If this check is not possible, then LANconfig takes the last IP address that was last used successfully.
- **Timeout:** Here you enter how many seconds the program should wait for a response from this device.
- **HTTPS, SSH, HTTP, TFTP:** When this is selected, you enable the individual protocols for the operations firmware upload, configuration up/download, and script up/download. In these operations, LANconfig attempts to use these protocols in the order HTTPS, SSH, HTTP and TFTP. If the transfer fails when using one of the selected protocols, LANconfig automatically tries the next protocol.
- **Prefer 'check' via TFTP:** This option causes LANconfig to perform checks with TFTP, irrespective of other protocols that are selected. This is advantageous for devices located in the LAN. The checks are faster and place less load on the computer, which makes an appreciable difference when processing a large number of devices. The fact that HTTPS is not used should not be a problem in the LAN.
- **Check the status of this device at startup:** Check this box if LANconfig should check the status of the device every time it is started.

- **Check for possible firmware updates:** Select this option if LANconfig should check for possible firmware updates.

As described in the section 'Communication protocols and ports', LANconfig tests other protocols and executes them if TFTP is not available. Here, too, global settings take priority over the device-specific settings.

After you have made the settings, the program tries to access the device and retrieve its name and version.

If this fails, LANconfig shows a short error message in the **Device status** column.

General

In this section you can access the credentials for the device and enter a description.



- **Administrator:** Enter the username for the administrator.
- **Password:** Enter the associated password here.
- **Description:** Enter the description of the device that you want LANconfig to display in the main window.

LANconfig stores the credentials persistently, so that you no longer need to enter them when re-accessing the device.



If you save the username and password permanently, any user who is permitted to run LANmonitor also has access to the device.

Communication protocols and ports

LANconfig performs these checks, i.e. the transfer of system information, by using the communications protocols set here.

LANconfig performs device actions such as uploading scripts, firmware and configurations, as well as configuration download, with the communications protocols selected here.



For devices with LCOS versions predating version 5.20, LANconfig uses the TFTP protocol for all actions, irrespective of the protocols set here.

LANconfig attempts to carry out the device actions outlined above in the order HTTPS, SSH, HTTP, and TFTP and SSH. If an action fails because of the protocol, then LANconfig repeats them with the next selected protocol.

At least one protocol must be selected in order for the action to function.



When using HTTP(S) and a proxy server, it may be necessary to circumvent this proxy server so that LANconfig can reach the device. You can bypass the proxy server for local addresses by using a setting in the Window's Control Panel, Internet options. In the Internet options' advanced settings, you can also define further addresses which should not be contacted via the proxy server.

Protocols can be set globally or by means of device-specific settings. The global settings in the options menu take priority over the device-specific settings. A benefit of this is that a single global switch can be used to disable a protocol for all devices.

Tips

- When shipped, the device does not yet have an IP address. In this case, enter the IP address of your computer and replace the last part of the number sequence by 254: If your computer's IP address is 192.168.1.1, then assign the IP address 192.168.1.254 to the device.

- Also, if you do not know the device's IP address, you additionally have the option of searching for it with **File > Devices**.

Potential problems when connecting with a new device

If LANconfig cannot reach a device at all, then one of the following error messages is displayed under status.

To check a device again, mark it in the list and click on **Device > Check** in the menu bar.

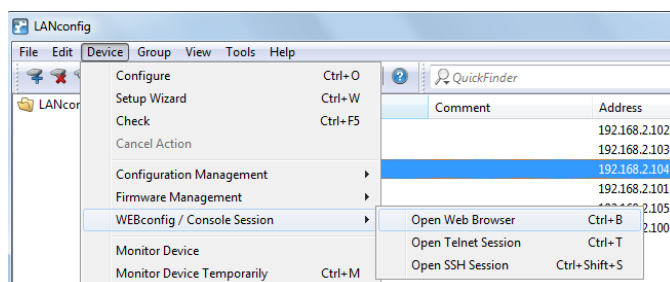
- **Serial error:** LANconfig could not open the serial interface. Close any program that may be accessing the port.
- **IP error:** Check that the IP address of the device is correct and that your computer is properly connected to the network. You can also check that the TCP/IP protocol is installed properly and correctly configured.
- **No response:** Check if the IP address of the device is correct. Another possibility is that the network connection between your computer and the device is too slow or unreliable.
- **Status unknown:** LANconfig reached the device via the specified IP address, but was unable to request any additional information. LANconfig may not support this device.
- **Access denied:** Access to this device from your computer is blocked.

Device

Under the menu item **Device** you can edit the configurations of devices connected to the network, organize firmware updates and monitor device connections.

The functions in the **Device** menu are only offered for selection if at least one device has been chosen from the list of devices. The menu can also be called by clicking on a device with the right mouse button when it is marked.

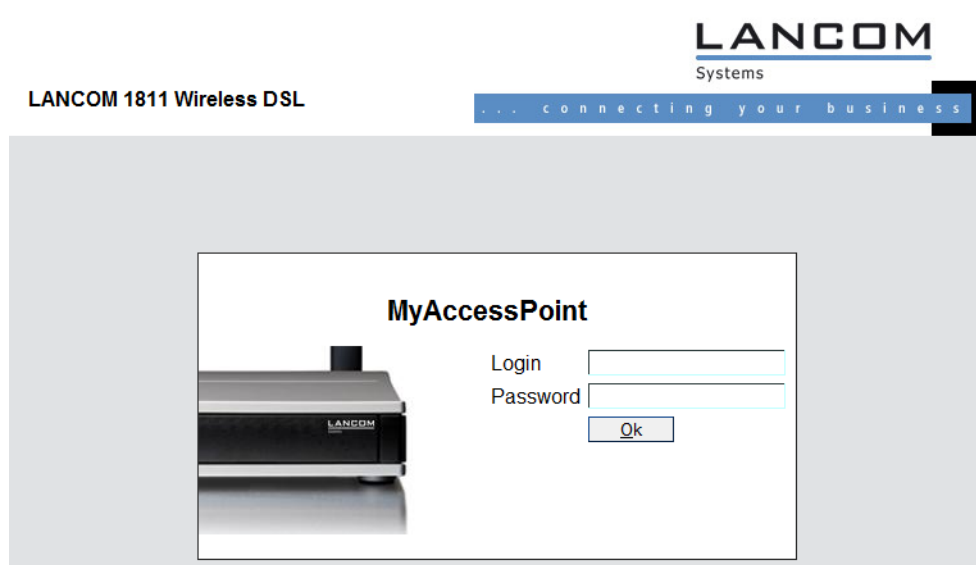
WEBconfig / console session



You can select the following actions under **Device > WEBconfig / console session**:

Open web browser

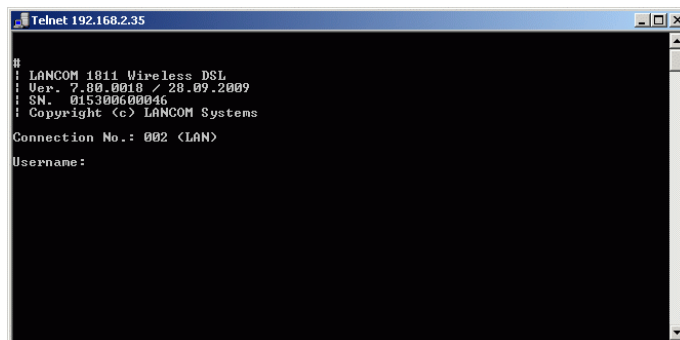
Opens the web browser for the device marked.



Under **Tools > Options > Extras > Browser used to display WEBconfig**, you choose whether LANconfig should use the system default browser or its own internal browser.

Open Telnet session

Opens the telnet session.



Open SSH session

Opens a configuration session with an SSH client.

Extras

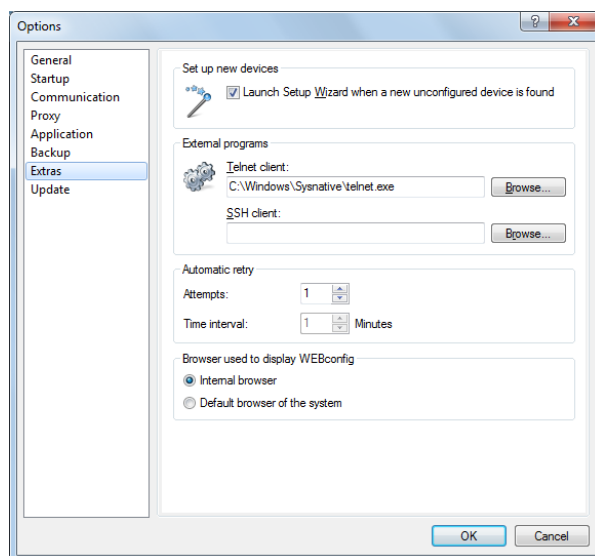
Clicking on **Tools > Options** opens up the dialog box for further optional settings. (You can also reach this dialog box by pressing F7).

Options

Under the menu item **Options** you can invoke additional functions, for example to communicate with connected devices, invoke external applications, or carry out automatic searches for firmware updates.

Extras

This dialog window allows you to make **additional settings**.



Set up new devices

If this option is checked, LANconfig launches the Setup Wizard whenever it finds an unconfigured device.

External programs

This item specifies the executable files for the Telnet client and the SSH client to be used by LANconfig for connections to the devices.

Automatic retry

Attempts

Specify the number of attempts for a firmware or configuration upload. You can set a number between 1 and 9999. LANconfig always attempts to make a connection. If this fails a retry is attempted after the defined interval. The operation is retried until LANconfig reaches the number of defined attempts or until the operation succeeds. LANconfig may terminate the retries if a situation arises in which completion is unlikely without external intervention. This may be when the device cannot open a file, for example.

Time interval

Enter the time interval in minutes between two attempts to upload the firmware or configuration. You can set an interval between 1 and 9999.

Browser used to display WEBconfig

This item sets the default browser used by LANconfig to display WEBconfig. You can choose between your operating system's default browser and LANconfig's internal browser, LCCEF (LANCOM Chromium Embedded Framework).

9 IPv6

9.1 Reconfigure function of the DHCPv6 server

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

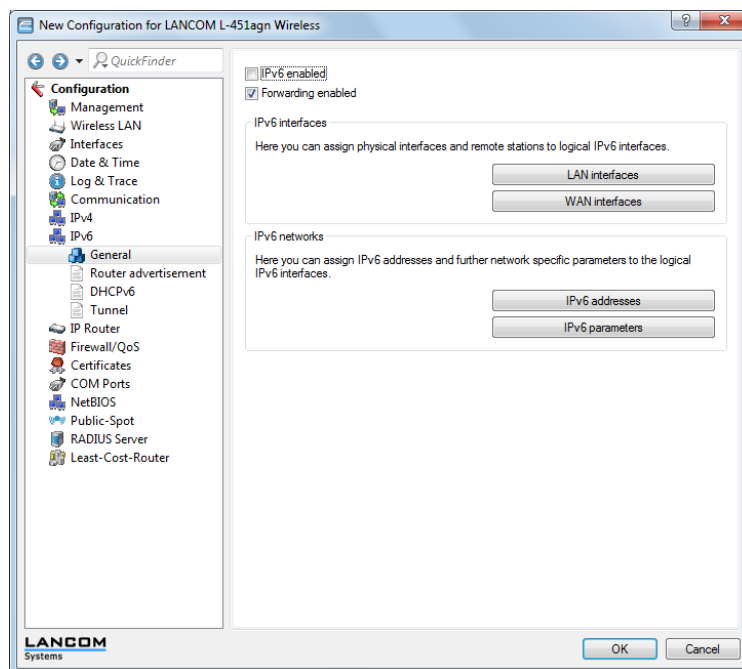
However, if the WAN prefix changes, for example, due to disconnection and reconnection of an Internet connection or a request for a new prefix (Deutsche Telekom Privacy feature), the server has no way to inform the network devices that the prefix or address has changed. This means that a client is still using an old address or an old prefix, and can no longer communicate with the Internet.

As of the LCOS 8.82 version, the DHCPv6 server on IPv6-capable LANCOM devices can require clients in the network to renew their leases/bindings.

9.1.1 Enhancements to LANconfig

IPv6 configuration menu

Where previous versions provided configuration menus for TCP/IP for IPv4, you now find the options **IPv4** and **IPv6**.



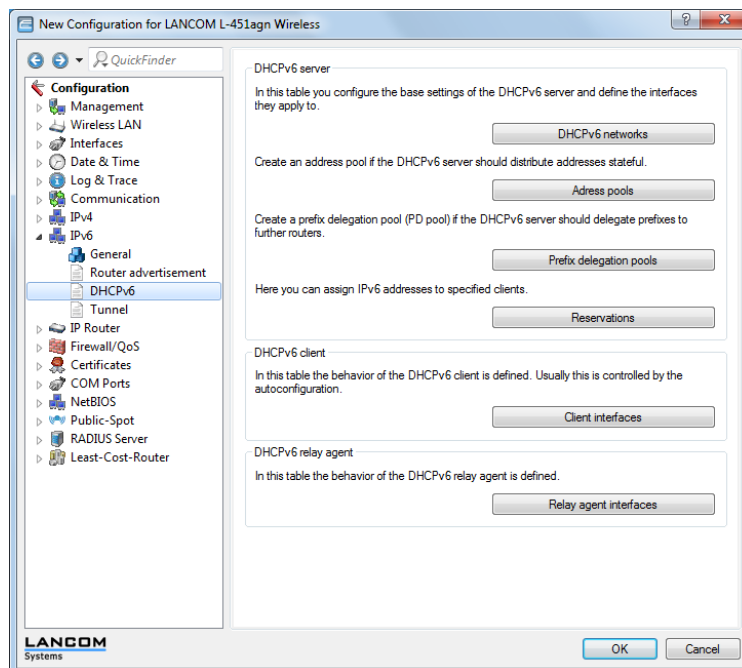
Click on **IPv6** to adjust the settings for this protocol. The **IPv6** configuration is divided into the options

- **General**,
- **Router advertisement**,
- **DHCPv6** and
- **Tunnel**.

By default a click on **IPv6** takes you straight to the **General** options.

DHCPv6

This is where you configure the DHCPv6 server, the DHCPv6 client and the DHCPv6 relay agent.

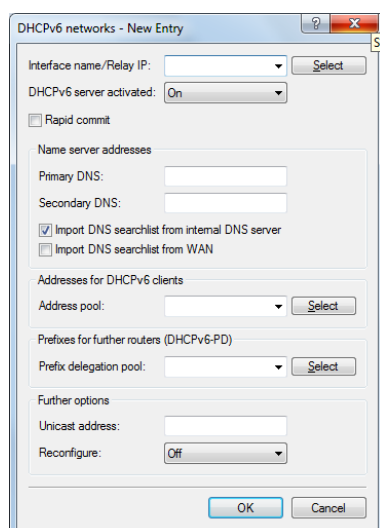


DHCPv6 server

Use the following buttons to access the tables and adjust the respective functions:

DHCPv6 networks

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.



Interface name/Relay IP

Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote DHCPv6 relay agent.

DHCP server activated

Activates or deactivates the entry.

Rapid commit

With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.



The client must explicitly include the rapid commit option in its solicit message.

DNS default

IPv6 address of the primary DNS server.

DNS backup

IPv6 address of the secondary DNS server.

Import DNS search list from internal DNS server

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under **IPv4 > DNS > General settings**. The default setting is "enabled".

Import DNS search list from WAN

Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. The default setting is "disabled".

Address pool

Name of the address pool used for this interface.



If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the **Address pools** table.

Prefix delegation pool

Name of prefix pools to be used by the DHCPv6 server.



If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table **Prefix delegation pools**.

Unicast address

By default the DHCPv6 server exclusively responds to multicast requests. If the DHCPv6 server should respond to a unicast request, this IPv6 address can be configured here. Generally speaking, multicast is sufficient for communication.

Reconfigure

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

However, if the WAN prefix changes, for example, due to disconnection and reconnection of an Internet connection or a request for a new prefix (Deutsche Telekom Privacy feature), the server has no way to inform the network devices that the prefix or address has changed. This means that a client is still using an old address or an old prefix, and can no longer communicate with the Internet.

The reconfigure feature allows the DHCPv6 server to require the clients in the network to request a renewal of leases / bindings. If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called *Reconfigure Key*, so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation.

The *Reconfigure Key Authentication Protocol* according to RFC 3315 is supported for *Renew* and *Information-Request*, as well as *Rebind* according to RFC 6644. Reconfiguration is started on the console of the device using a "do" command in the status tree (see the description of the status tree).



You can find more about the status of a client regarding the Reconfigure function under **Status > IPv6 > DHCPv6 > Server > Clients**.

The following settings are available:

- **Off:** Disables the reconfigure function
- **Reject:** Clients that have used the Reconfigure Option in queries are rejected by the server and are not assigned an address, prefix or other options.
- **Allow:** If the client sets the Reconfigure Option in queries, the server negotiates the necessary parameters with the client in order to start a reconfiguration at a later time.
- **Require:** Clients have to set the Reconfigure Option in queries, otherwise the client rejects these clients. This mode makes sense when you want to ensure that the server only serves clients which support Reconfigure. This ensures that all clients can use Reconfigure to update their addresses, prefixes, or other information at a later point in time.

Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:

Address pool name

Name of the address pool

Start address

First address in the pool, e.g. "2001:db8::1"

End address

Last address in the pool, e.g. "2001:db8::9"

Preferred lifetime:

Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

Validity period

Here you specify the time in seconds that the client should treat this address as 'valid'.




If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

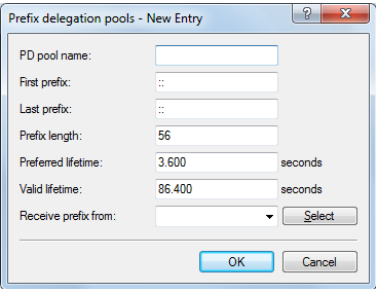
With this parameter you can assign addresses to the network clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then enter the value "::1"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

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

 You should only use this mechanism if the provider assigns a fixed prefix. Otherwise, it is possible that the provider delegates a new prefix to the router, but the client still has an address from the pool with the old prefix. In this case, the client must update its address at the server.

Prefix delegation pool

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:



The dialog box 'Prefix delegation pools - New Entry' contains the following fields and controls:

- PD pool name:
- First prefix:
- Last prefix:
- Prefix length:
- Preferred lifetime: seconds
- Valid lifetime: seconds
- Receive prefix from:
-

PD pool name

Name of the PD pool

First prefix

First prefix for delegation in the PD pool, e.g. "2001:db8:1100::"

Last prefix

Last prefix for delegation in the PD pool, e.g. "2001:db8:FF00::"

Prefix length


Length of the prefixes in the PD pool, e.g. "56" or "60"

Preferred lifetime:

Here you specify the time in seconds that the client should treat this prefix as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

Validity period

Here you specify the time in seconds that the client should treat this prefix as 'valid'.

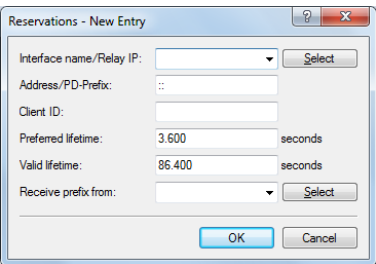
 If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can use this table to make a reservation for each client.



The dialog box 'Reservations - New Entry' contains the following fields and controls:

- Interface name/Relay IP:
- Address/PD-Prefix:
- Client ID:
- Preferred lifetime: seconds
- Valid lifetime: seconds
- Receive prefix from:
-

Interface name or relay

Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.

Address/PD prefix

IPv6 address or PD prefix that you want to assign statically.

Client ID

DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `ipconfig /all` or in WEBconfig under **Status > IPv6 > DHCPv6 > Client > Client ID**.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under **Status > IPv6 > DHCPv6 > Server > Address bindings**, and retrieved IPv6 prefixes are under **Status > IPv6 > DHCPv6 > Server > PD bindings**.

LANmonitor displays that client IDs under **DHCPv6 server**.

Preferred lifetime:

Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

Validity period

Here you specify the time in seconds that the client should treat this address as 'valid'.



If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

Receive prefix from

Name of the WAN interface from which the client should use the prefix to form the address or prefix.

9.1.2 Additions to the Setup menu

Reconfigure

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

However, if the WAN prefix changes, for example, due to disconnection and reconnection of an Internet connection or a request for a new prefix (Deutsche Telekom Privacy feature), the server has no way to inform the network devices that the prefix or address has changed. This means that a client is still using an old address or an old prefix, and can no longer communicate with the Internet.

The reconfigure feature allows the DHCPv6 server to require the clients in the network to request a renewal of leases / bindings.

SNMP ID:

2.70.3.1.4.13

Telnet path:

Setup > IPv6 > DHCPv6 > Server > Interface-List

Possible values:

Off: Disables the reconfigure function

Prohibit: Clients that have used the Reconfigure Option in queries are rejected by the server and are not assigned an address, prefix or other options.

Allow: If the client sets the Reconfigure Option in queries, the server negotiates the necessary parameters with the client in order to start a reconfiguration at a later time.

Force: Clients have to set the Reconfigure Option in queries, otherwise the client rejects these clients. This mode makes sense when you want to ensure that the server only serves clients which support Reconfigure. This ensures that all clients can use Reconfigure to update their addresses, prefixes, or other information at a later point in time.

Default:

Off

9.1.3 Additions to the Status menu

Reconfigure

This action causes the clients in the network to renew their leases/bindings. It can be triggered by a Reconfigure for Renew, Rebind, or Information Request.

The reconfigure function will then expect the following parameters:

- **renew:** (optional, default) Asks the client to perform a renewal for his address and/or prefix.
- **rebind:** (optional) Asks the client to perform a rebind for his address and/or prefix.
- **info:** (optional) Asks the client to send an Information-Request, in order to, for example, update its DNS server.
- **-c <Client-ID>:** The reconfigure function applies to the client with the specified client ID.
- **-b <Address/Prefix>:** The reconfigure function applies to the client with the specified address and the specified prefix.
- **-i <Interface/Relay>:** The reconfigure function applies to all clients that are connected to the specified interface or relay.
- **-a:** The reconfigure function applies to all clients.

SNMP ID:

1.77.3.1.7

Telnet path:

Status > IPv6 > DHCPv6 > Server

10 Diagnosis

10.1 SYSLOG: Configuration of the retention period for system events

As of Version LCOS 8.82 you can also enter the retention period for system events in hours, days, and months.

10.1.1 Additions to the Setup menu

Message age unit

This parameter determines whether the message age is specified in hours, days and months.



In this case, a month is 30 days.

SNMP ID:

2.22.11

Telnet path:

Setup > SYSLOG

Possible values:

Hour

Day

Month

Default:

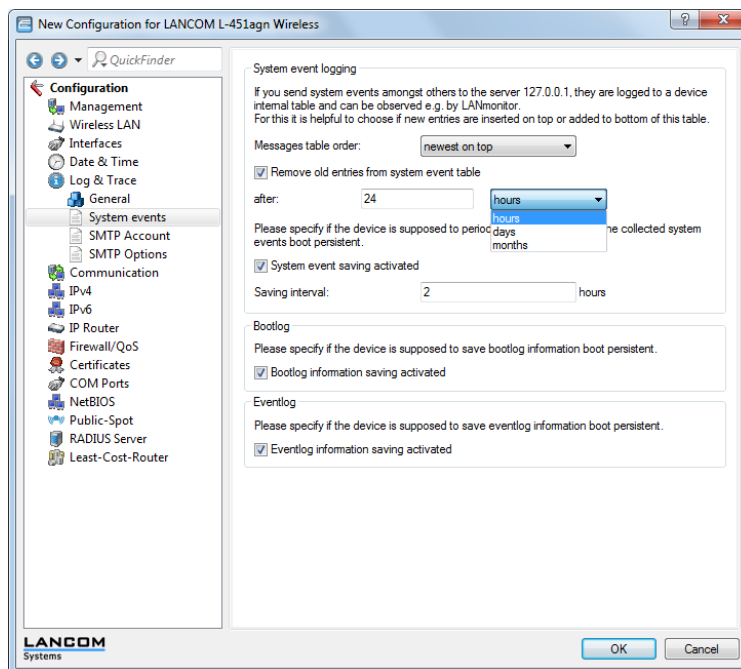
Hour

10.1.2 Enhancements to LANconfig

Configuration of the retention period for system events

Under **log & Trace > System events** you can specify how long the device should save system events in the section **System event logging**. You can specify both the quantity (0-9999) and the unit (hour, day, month).

! In this case, a month is 30 days.



10.2 SYSLOG: Extension of log entries of the internal SYSLOG server

As of LCOS version 8.82, the internal syslog server for certain devices can store up to 23,000 entries.

This change currently applies to the following device types and series:

- LANCOM 17xx+ series
- LANCOM 1781 series
- LANCOM 1780EW-4G
- LANCOM L-460agn dual Wireless
- LANCOM L-451agn Wireless
- LANCOM L-452agn dual Wireless
- LANCOM 7100+ VPN
- LANCOM 9100+ VPN
- LANCOM WLC-4006+

10.3 SYSLOG: Extended status display of the login to the cellular network

As of LCOS version 8.82, the SYSLOG displays detailed information about the status of the login process on a cellular network (UMTS/3G+, GPRS, LTE/4G).

10.3.1 Extended status display of the login to the cellular network

In order to more quickly analyze connection problems in a cellular network, WWAN-capable LANCOM routers report all logon procedures to the SYSLOG. In this manner, the user can recognize if and why the cellular service provider rejected the connection, for example.

The device generates a SYSLOG entry for each of the following events:

Modification or problem when setting the registration status

Status	Meaning	SYSLOG severity
not searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
registered to home network	The modem has registered on its service provider's cellular network.	INFORM
registered to foreign network	The modem has successfully registered on the cellular network of the service provider's roaming partner.	INFORM
unknown registration	Initial value. The modem has not yet received a response from the radio module regarding the registration status.	INFORM
network registration denied	The cellular service provider has rejected the login on the cellular network.	ERROR
lost network registration	The modem lost the connection to the registered cellular network.	NOTICE
failed to set network	The modem has replied to the command to assign the network with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
failed to set network mode	The modem has replied to the command to assign the network mode with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR

Problem when setting the network mode

Status	SYSLOG severity
Auto	ERROR
UMTS	ERROR
GPRS	ERROR
LTE	ERROR

Problem when setting the APN

Status	Meaning	SYSLOG severity
Invalid APN	An invalid APN was selected for the SIM or the cellular network.	ERROR
failed to set APN	The modem has replied to the command to assign the APNs with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR

10.3.2 Additions to the Status menu

Network registration

This entry shows the status value of the network registration. Every status change generates an SNMP trap message for subsequent evaluation and processing (e.g., by an SNMP manager).

Possible values include:

- **No_Network:** The modem is not registered and is not searching for a cellular network.
- **Home_Network:** The modem has registered on its service provider's cellular network.
- **Searching:** The modem is not registered and is not searching for a cellular network.
- **Searching(Denied):** The modem is not registered and is searching for a network, but was rejected at least once during the search. This addition disappears as soon as the modem successfully registers.
- **Unknown:** Initial value. The modem has not yet received a response from the radio module regarding the registration status.
- **Roaming:** The modem has successfully registered on the cellular network of the service provider's roaming partner.
- **Denied:** The cellular service provider has rejected the login on the cellular network.

SNMP ID:

1.49.7

Telnet path:

Status > Modem-Cellular-Network