

LCOS 10.80

WLAN Management

11/2023

Contents

1 WLAN management.....	5
1.1 Initial situation.....	5
1.2 Technical concepts.....	5
1.2.1 WLC features in the LANCOM vRouter.....	5
1.2.2 The CAPWAP standard.....	6
1.2.3 Smart controller technology.....	6
1.2.4 Communication between access point and WLAN controller.....	8
1.2.5 Zero-touch management.....	10
1.2.6 Split management.....	10
1.2.7 Protection against unauthorized CAPWAP access from the WAN.....	10
1.3 Basic configuration of the WLAN controller function.....	11
1.3.1 Setting the time information for the WLAN controller.....	11
1.3.2 Example: Default configuration.....	11
1.3.3 Assigning the default configuration to the new access points.....	15
1.3.4 Configuring the access points.....	16
1.4 Configuration.....	17
1.4.1 General settings.....	17
1.4.2 Profiles.....	17
1.4.3 Access point configuration.....	35
1.4.4 IP-dependent auto configuration and tagging of APs.....	70
1.5 Access point administration.....	72
1.5.1 Accepting new access points into the WLAN infrastructure manually.....	72
1.5.2 Manually removing access points from the WLAN infrastructure.....	74
1.5.3 Deactivating access points or permanently removing them from the WLAN infrastructure.....	74
1.6 AutoWDS – wireless integration of APs via P2P connections.....	75
1.6.1 Notes on operating AutoWDS.....	77
1.6.2 How it works.....	79
1.6.3 Setup by means of preconfigured integration.....	85
1.6.4 Accelerating preconfigured integration by pairing.....	87
1.6.5 Express integration.....	87
1.6.6 Switching from express to preconfigured integration.....	88
1.6.7 Manual topology management.....	88
1.6.8 Redundant paths by means of RSTP.....	91
1.7 Central firmware and script management.....	92
1.7.1 General settings for firmware management.....	93
1.8 RADIUS.....	96
1.8.1 Checking WLAN clients with RADIUS (MAC filter).....	97
1.8.2 External RADIUS server.....	98
1.8.3 Dynamic VLAN assignment.....	100

1.8.4	Activating RADIUS accounting for logical WLANs in the WLAN controller.....	101
1.9	Displays and commands in LANmonitor.....	103
1.10	RF optimization.....	104
1.10.1	Group-related radio field optimization.....	105
1.11	Client steering by WLC.....	106
1.11.1	Configuration.....	107
1.12	Channel-load display in WLC mode.....	110
1.13	Backing up the certificates.....	111
1.13.1	Create backups of the certificates.....	111
1.13.2	Uploading a certificate backup into the device.....	112
1.13.3	Backing up and restoring further files from the SCEP-CA.....	113
1.13.4	One-click backup of the SCEP-CA.....	113
1.13.5	Using LANconfig to backup and restore certificates.....	114
1.14	Backup solutions.....	115
1.14.1	WLC cluster.....	115
1.14.2	Backup with redundant WLAN controllers.....	119
1.14.3	Backup with primary and secondary WLAN controllers.....	121
1.14.4	Primary and secondary controllers.....	121
1.14.5	Automatic search for alternative WLCs.....	122
1.14.6	One-click backup of the SCEP-CA.....	122
1.15	Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option.....	123
1.15.1	Special LANconfig icon for devices in a cluster or using Config Sync.....	124
1.15.2	Special LANmonitor icon for devices in a cluster or using Config Sync.....	125
2	Appendix.....	126
2.1	Overview of CAPWAP parameters with the show command.....	126

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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

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

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

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

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

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

Products from LANCOM Systems include cryptographic software written by Eric Young (ey@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Germany

www.lancom-systems.com

1 WLAN management

1.1 Initial situation

The widespread use of wireless access points (APs) and wireless routers provides great convenience and flexibility in network access for businesses, universities and other organizations.

Yet in spite of the numerous advantages WLAN infrastructures offer, there are still a number of unsettled issues:

- All APs must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the APs, especially for larger WLAN infrastructures with the appropriate security mechanisms, requires advanced qualifications and experience on the part of those responsible, and it ties up considerable resources in the IT departments.
- The manual customization of the configurations in the APs when changes are made to the WLAN infrastructure can be time-consuming, with the result that different configurations can be present in the WLAN at the same time.
- Combined utilization of the shared communications medium (air) requires effective coordination of the APs to avoid frequency interference and optimize network performance.
- In public places, APs are a potential security risk because the devices themselves, including the security-related data in them such as passwords, etc., are susceptible to theft. In addition, rogue APs may be able to connect to the LAN unnoticed, bypassing the security policies that are in place.

1.2 Technical concepts


Centralized WLAN management is the solution to these problems. The configuration of the AP is then no longer carried out in the devices themselves but by a central authority instead, the WLAN controller (WLC). The WLC authenticates the APs and transmits the correct configuration to the approved devices. This allows for convenient configuration of the WLAN from a central point and the changes to the configuration affect all of the APs simultaneously. Optionally the configuration provided by the WLC is not stored in the AP's flash memory but in RAM, so security-related data cannot fall into the hands of unauthorized persons in the event that devices are stolen. Only in "standalone" operation is the configuration optionally saved for a defined period to flash memory (in an area that cannot be read out with LANconfig or other tools).

1.2.1 WLC features in the LANCOM vRouter

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

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

Product	VPN licenses	AP licenses
vRouter unlimited	1000	1000


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

1.2.2 The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless Access Points) introduced by the IETF (Internet Engineering Task Force) is a standard for the centralized management of large WLAN infrastructures.

CAPWAP uses two channels for data transfer:

- Control channel, encrypted with Datagram Transport Layer Security (DTLS). This channel is used to exchange administration information between the WLC and the AP.

-  DTLS is an encryption protocol based on TLS but, in contrast to TLS itself, it can be used for transfers over connectionless, unsecured transport protocols such as UDP. DTLS therefore combines the advantages of the high security provided by TLS with the fast transfer via UDP. This also makes DTLS suitable for the transfer of VoIP packets (unlike TLS) because, even after the loss of a packet, the subsequent packets can be authenticated again.
- The payload data from the WLAN is transferred through this data channel from the AP via the WLC into the LAN—encapsulated in the CAPWAP protocol.

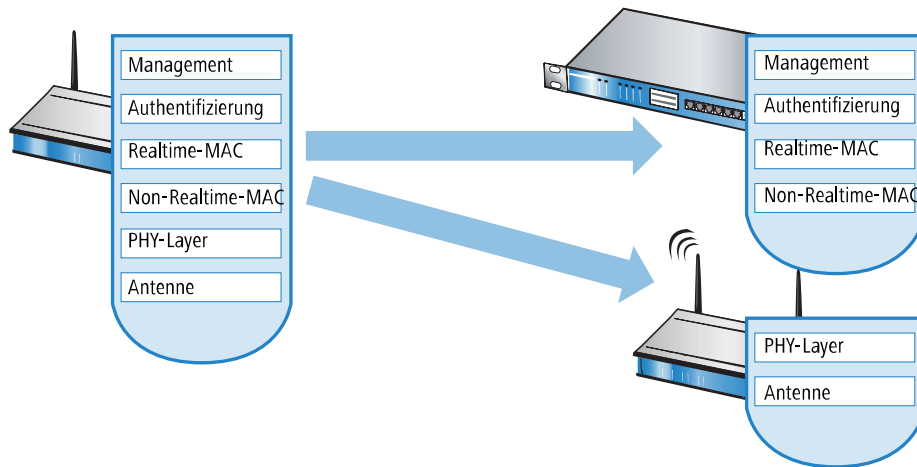
1.2.3 Smart controller technology

In a decentralized WLAN structure with stand-alone APs (operating as so-called “rich access points”) all functions for data transfer take place in the PHY layer, the control functions in the MAC layer, and the management functions are integrated in the APs. Centralized WLAN management divides these tasks among two different devices:

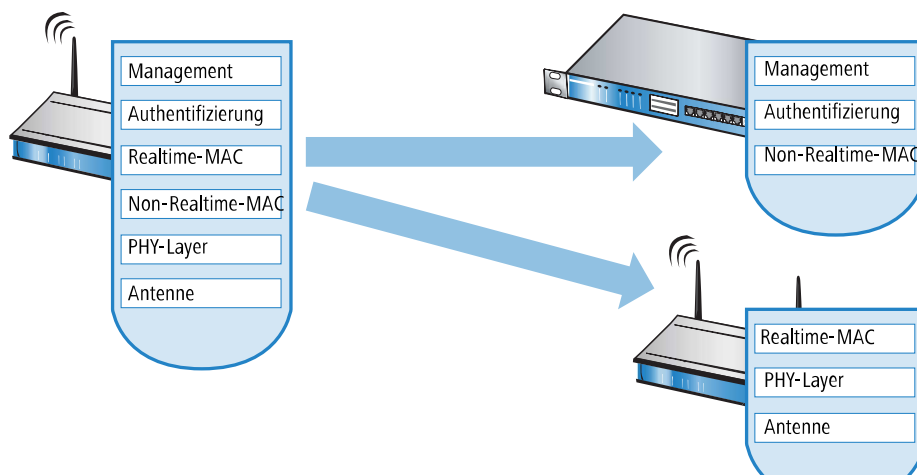
- The central WLC assumes the administration tasks.
- The decentralized APs handle the data transfer at the PHY layer and the MAC features.
- A RADIUS or EAP server can be added as a third component RADIUS or for authentication of WLAN clients (which can also be the case in stand-alone WLANs).

CAPWAP describes three different scenarios for the relocation of WLAN functions to the central WLC.

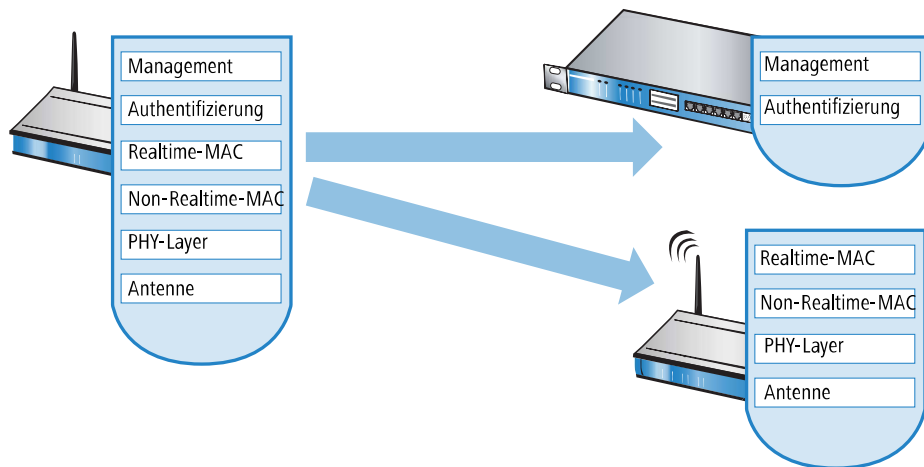
- Remote MAC: In this case, all of the WLAN functions are transferred from the AP to the WLC. Here, the APs only serve as "extended antennas" without independent intelligence



- Split MAC: With this variant, only a portion of the WLAN functions are transferred to the WLC. Normally, realtime applications will continue to be processed in the AP; the non-realtime applications are processed via the central WLC.



- Local MAC: The third possibility provides for complete management and monitoring of the WLAN data traffic directly in the APs. The only information exchanged between the AP and the WLC is for network management and ensures that the APs have a uniform configuration.



Smart Controller Technology from LANCOM uses the local MAC procedure. Thanks to the reduction of centralized tasks, these WLAN infrastructures offer optimum scalability. At the same time, infrastructure of this type prevents the WLC from becoming a central bottleneck that has to process large portions of the overall data traffic. In remote MAC and split MAC architectures, all payload data is forced to run centrally via the WLC. In local MAC architectures the data can alternatively be broken out from the APs directly to the LAN to provide high-performance data transfer. With break-out into the LAN, data can also be directly routed into special VLANs. This makes it very easy to set up closed networks, such as for guest access accounts.

Layer 3 tunneling and layer 3 roaming

WLCs with LCOS also support the transfer of payload data through a CAPWAP tunnel. This allows selected applications such as VoIP to be routed via the central WLC, for example. If WLAN clients change to a different radio cell, the underlying IP connection will not be interrupted because it continues to be managed by the central WLC (layer-3 roaming). In this way, mobile SIP telephones can easily roam between Ethernet subnets, even during a call.

Managing data streams centrally can also make configuring VLANs at the switch ports unnecessary in environments with numerous VLANs because all CAPWAP tunnels are centrally managed on the WLC.

1.2.4 Communication between access point and WLAN controller

Communication between an AP and the WLC is always initiated by the AP. In the following cases, the devices search for a WLC that can assign a configuration to them:

- When shipped, the WLAN modules in LANCOM APs are set to the 'Managed' operating mode. In this mode, APs search for a central WLC that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLC or until the operating mode of the WLAN module is changed manually.
- While the AP searches for a WLC, its WLAN module is switched off.
- Ex-factory, the WLAN modules in LANCOM wireless routers are set to the 'access point' operating mode. In this mode, wireless routers function as standalone access points with a configuration that is stored locally in the device. For integration into a WLAN infrastructure that is centrally managed by WLAN controllers, the operating mode of the WLAN modules in wireless routers has to be switched into the 'managed' mode.



Communication between the access point and the WLAN-Controller takes place via **CAPWAP** as well as via **SCEP**. For **CAPWAP** the **UDP port 1027** is used in the default configuration (can be changed in the WLAN-Controller configuration). For the communication via **SCEP** the protocol **HTTP (TCP port 80)** is used.

The AP sends a "discovery request message" at the beginning of communication to find the available WLCs. This request is sent as a broadcast. However, because in some structures a potential WLC cannot be reached by a broadcast, special addresses from additional WLCs can also be entered into the configuration of the APs.

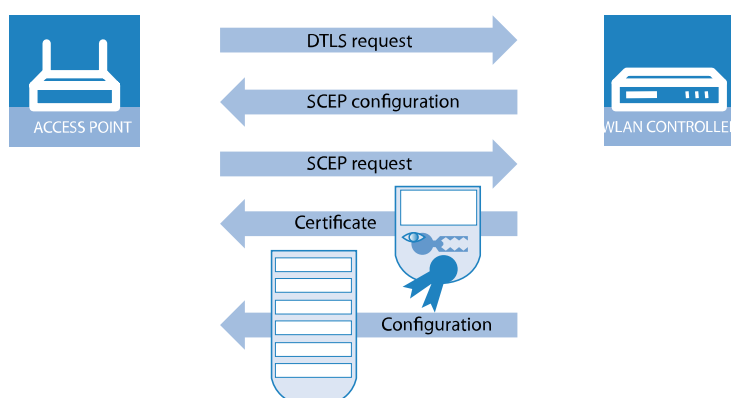
! The DNS names of WLCs can also be resolved. All APs with LCOS 7.22 or higher have the default name 'WLC-Address' preconfigured so that a DNS server can resolve this name to a WLC. The same applies to the DHCP suffixes learned via DHCP. This also makes it possible to reach WLCs that are not located in the same network, without having to configure the APs.

From the available WLCs, the AP selects the best one and requests it to establish the DTLS connection. The "best" WLC for the AP is the one with the least load, i.e. the lowest ratio of managed APs compared to the maximum possible number of APs. In case of two or more equally "good" WLCs, the AP selects the nearest one in the network, i.e. that with the fastest response time.

The WLC then uses an internal random number to determine a unique and secure session key, which it uses to secure the connection to the AP. The CA in the WLC issues a certificate to the AP by means of SCEP. The certificate is protected by a one-time-only "challenge" (password). The AP uses this certificate for authentication at the WLC to collect the certificate.

The AP is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the AP uses the SCEP to retrieve its certificate from the SCEP CA. Once this is done, the assigned configuration is transferred to the AP.

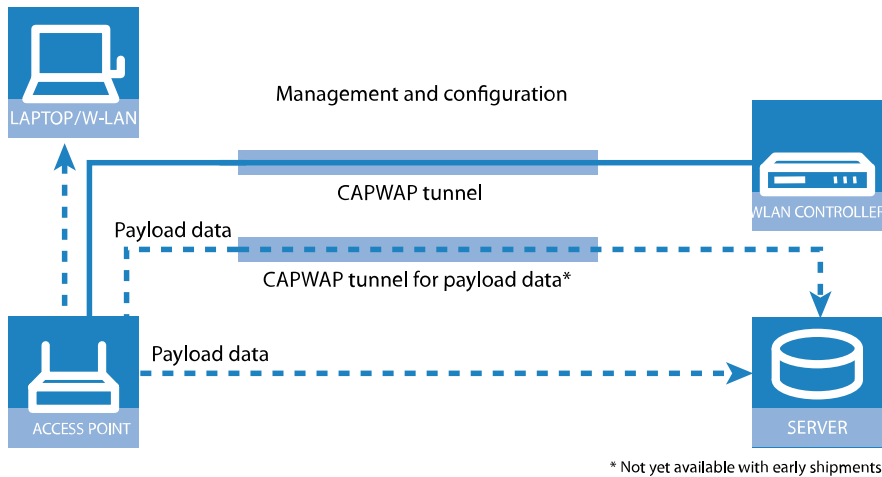
! SCEP stands for Simple Certificate Encryption Protocol, CA for Certification Authority.



Authentication and configuration can both be carried out either automatically or only with a corresponding entry of the AP's MAC address in the AP table of the WLC. If the AP's WLAN modules were deactivated at the beginning of the DTLS communication, these will be activated after successful transfer of the certificate and configuration (provided they are not explicitly deactivated in the configuration).

1 WLAN management

The management and configuration data will then be transferred via the CAPWAP tunnel. The payload data from the WLAN client is then released in the AP directly into the LAN and transferred, for example, to the server.



1.2.5 Zero-touch management

With their ability to automatically assign a certificate and configurations to the requesting APs, WLCs implement true "zero-touch management". Simply connect new APs to the LAN—no further configuration is necessary. This simplification to only having to install devices reduces the workload for IT departments, especially in decentralized structures, because no special IT or WLAN expertise is required for the setup at the remote locations.

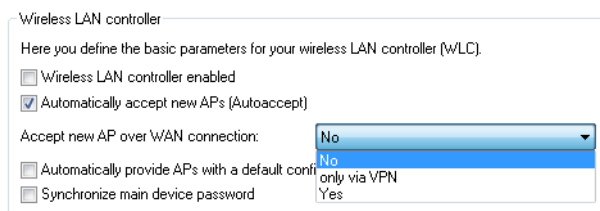
1.2.6 Split management

APs are able to search for their WLC in remote networks—a simple IP connection, such as via a VPN path, is all you need. As the WLCs only influence the WLAN part of the configuration in the AP, all other functions can be managed separately. This division of the configuration tasks makes WLCs ideal for establishing a company-wide WLAN infrastructure that is based at the headquarters and includes all of the branch and home offices connected to it.

1.2.7 Protection against unauthorized CAPWAP access from the WAN

The WLC or LANCOM router with activated WLC option handles CAPWAP requests from the LAN and the WAN in the same way. In the case of requests from WAN remote stations, it accepts the APs into its AP management and, under certain circumstances, it sends a default configuration. If configured appropriately, the CAPWAP service is no longer available to WAN remote stations, meaning that for WAN remote stations, APs are no longer accepted and configurations are not provisioned.

The configuration is done under **WLAN Controller > General** in the section **Wireless LAN controller**. If the automatic acceptance of new APs is enabled, you can use the feature **Accept new AP over WAN connection** to control whether the CAPWAP service is available to WAN remote stations.



No

The device accepts no new APs over the WAN connection.

Only via VPN

The device only accepts new APs if the WAN connection is via VPN.

Yes

The device accepts all new APs over the WAN connection.

1.3 Basic configuration of the WLAN controller function

To get started, a WLC requires the following two pieces of information to carry out the mainly automated configuration of the APs:

- Current time information (data and time) for checking the validity of the necessary certificates.
- A WLAN profile that the WLC can assign to the APs.

Further optional examples for configuration include setting up redundant WLC, the manual disconnection and connection of APs, and backing up any necessary certificates.

 By default the WLC listens for connections on the UDP port 1027 (configurable). The certificates are distributed by SCEP, which uses the TCP port 80 (HTTP).


1.3.1 Setting the time information for the WLAN controller

The management of APs in a WLAN infrastructure is based upon the automatic distribution of certificates via the Simple Certificate Enrollment Protocol (SCEP).

The WLC can only check the temporal validity of these certificates if it is set with the current time. If the time is not set in the WLC, the WLAN LED illuminates in red and the device is not operational.

 Routers with the WLC option do not have a WLAN LED.

To set the time in the device start LANconfig, click on the entry for the WLC with the right-hand mouse key and select **Set date/time** from the context menu. Alternatively in WEBconfig you can click on **Extras** and then **Set date and time**.

 Alternatively, WLCs can automatically retrieve the current time from a time server by means of the Network Time Protocol (NTP). Information on NTP and its configuration can be found in the LCOS reference manual.

As soon as the WLC has valid time information it begins with the generation of the certificates (root and device certificate) and it determines a random number. Once the necessary certificates have been generated, the WLC indicates that it is operational and the WLAN LED blinks red.

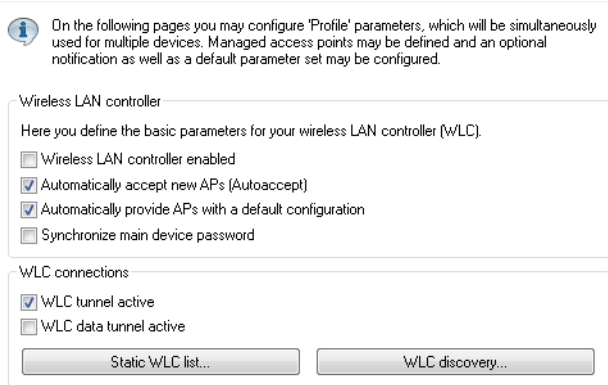
 Once operational, you should make a backup copy of the certificates (*Backing up the certificates*)

1.3.2 Example: Default configuration

1. Open up the configuration of the WLC by double-clicking on its entry in LANconfig.

1 WLAN management

2. Activate the options for the automatic acceptance of new APs and the provision of a default configuration under **WLAN controller > General**.



- > **Automatically accept new APs (Auto-accept)** Enables the WLC to provide a certificate to all new APs without a valid certificate. To this end, either a configuration for the AP has to be entered into the AP table, or 'Automatically provide APs with a default configuration' has to be activated.
- > **Automatically provide APs with a default configuration:** This enables the WLC to assign a default configuration to any new AP, even if no explicit configuration has been stored for it.

By combining these two options, the WLC can automatically integrate any managed-mode AP found in the LAN into its WLAN infrastructure. This may, for example, be a temporary measure during the rollout phase of a WLAN installation.

3. On the **Profiles** page, move to the logical WLAN networks. Add a new entry with the following values:

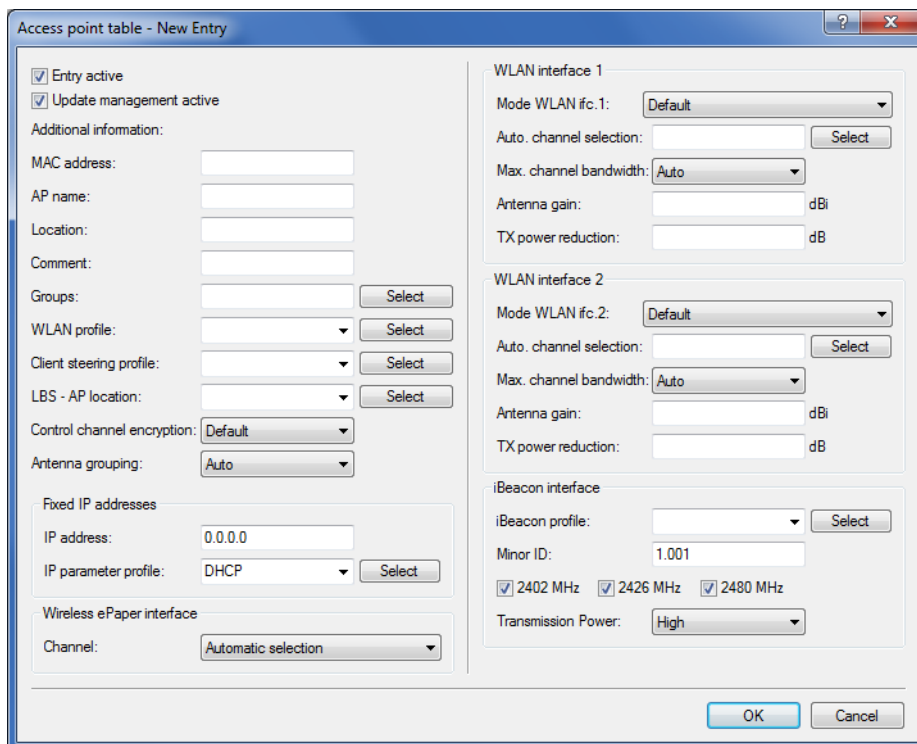
- **Name:** Give the WLAN a name. This name is used only for administrative purposes in the WLC.
 - **SSID:** This SSID is used for the WLAN clients to connect.
 - **Encryption:** Select the encryption method suitable for the WLAN clients being used, and enter a key or passphrase, as applicable.
 - Deactivate the MAC check. Instructions on the use of MAC filter lists in managed WLAN infrastructures can be found under [Checking WLAN clients with RADIUS \(MAC filter\)](#).
4. A new entry also has to be added to the physical WLAN parameters. In most cases involving the default configuration, just entering a name is sufficient. Adjust the other settings to meet your needs, if necessary.

! For normal AP applications you should use only the 5-GHz subbands 1 and 2. Subband 3 is for special applications only (e.g. BFWA, Broadband Fixed Wireless Access).

5. Create a new WLAN profile, give it a unique name, and assign the above logical WLAN network and physical WLAN parameters to it.

6. Change to the **AP configuration** view, open the **Access point table** and add a new entry by clicking on the **Default** button. Assign the WLAN profile to it as defined above. Leave **AP name** and **Location** empty.

! The **MAC address** is set to 'ffffffff' for the default configuration and it cannot be edited. This entry is thus a standard for any AP that is not explicitly listed in this table with its MAC address.

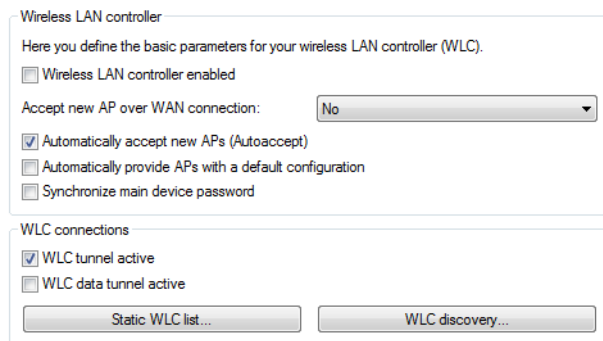


1.3.3 Assigning the default configuration to the new access points

With these settings you have defined all of the necessary values for the WLC to provide the APs with the required WLAN parameters. Upon assignment of the configuration, the APs change their status in the WLC management from "New access point" to "Expected access point", and they are listed in the device display under **Exp. APs**. Once the default configuration has been assigned to all new APs, the New APs LED switches off.

! After the initial start-up phase, the option **Automatically accept new APs** can be deactivated again so that no further APs are automatically accepted into the network.

i On the following pages you may configure 'Profile' parameters, which will be simultaneously used for multiple devices. Managed access points may be defined and an optional notification as well as a default parameter set may be configured.



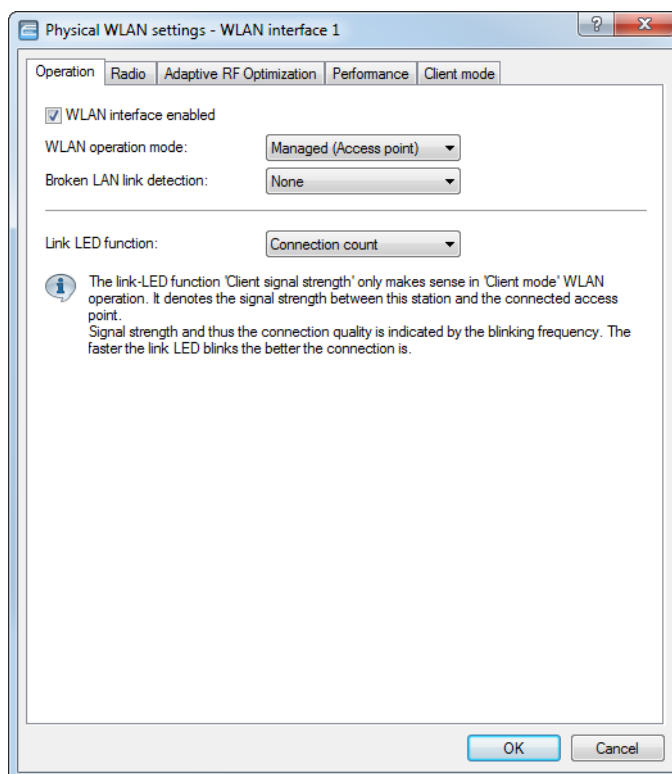
1.3.4 Configuring the access points

LANCOM access points and LANCOM wireless routers differ with regard to the ex-factory default settings in the WLAN modules.

- When shipped, the WLAN modules in APs are set to the 'Managed' operating mode. In this mode, APs search for a central WLC that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLC or until the operating mode of the WLAN module is changed manually.
- Ex-factory, the WLAN modules in wireless routers are set to the 'access point' operating mode. In this mode, wireless routers function as standalone APs with a configuration that is stored locally in the device. For integration into a WLAN infrastructure that is centrally managed by WLCs, the operating mode of the WLAN modules in wireless routers has to be switched into the 'managed' mode.

! The operating mode can be set separately for every WLAN module. For models with two WLAN modules, one module can work with a local configuration and the second module can be centrally managed with a WLC.

For individual devices, the operating mode of the WLAN modules can be found in LANconfig under **Wireless LAN > General > Physical WLAN settings > Operation mode**:



If you need to change the operating mode for multiple devices, you can use a simple script on the devices with the following lines:

```
# Script
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```


1.4 Configuration

Most of the parameters for configuring the 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.

1.4.1 General settings

This area is for the basic settings of your WLC.

> Automatically accept new APs (auto accept)


Enables the WLC to provide all new APs with a configuration, even those not in possession of a valid certificate.

Enables the WLC to provide a certificate to all new APs **without** a valid certificate. a valid certificate. One of two conditions must be fulfilled for this:

- > A configuration for the AP is entered into the AP table under its MAC address.
- > The option 'Automatically provide APs with the default configuration' is enabled.

> Automatic provision of the default configuration

This enables the WLC to assign a default configuration to every new AP (even those **without** a valid certificate), even if no explicit configuration has been stored for it. In combination with auto-accept, the WLC can accept all managed-mode APs which are found in the WLAN infrastructure managed by it (up to the maximum number of APs that can be managed by one WLC). Any APs accepted by default are also entered into the MAC list.

 This option can also lead to the acceptance of unintended APs into the WLAN infrastructure. For this reason this option should only be activated during the start-up phase when setting up a centrally managed WLAN infrastructure.

Combining the settings for auto-accept and default configuration can cater for a variety of different situations for the setup and operation of APs:

Auto accept	Default configuration	Suitable for
On	On	Rollout phase: Use this combination only if you can be sure that no APs can unintentionally connect with the LAN and thus be accepted into the WLAN infrastructure.
On	Off	Controlled rollout phase: Use this combination if you have entered all of the approved APs into the AP table along with their MAC addresses, assuming that these are to be automatically accepted into the WLAN infrastructure.
Off	Off	Normal operation: No new APs will be accepted into the WLAN infrastructure without the administrator's approval.

1.4.2 Profiles

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

WLAN profiles

The WLAN profiles are collections of the various settings that are to be assigned to the APs. The allocation of WLAN profiles to the APs is set in the AP table.


For each WLAN profile you can specify the following parameters under **WLAN controller > Profiles > WLAN profiles**:

Profile name

Name of the profile under which the settings are saved.

Log. WLAN network list

List of the logical WLAN networks that are assigned via this profile.

 From this list, APs use only the first 16 entries that are compatible with their own hardware. This means that 16 WLAN networks for purely 2.4-GHz operations and 16 for purely 5-GHz operations can be defined in a profile. Consequently, each AP—be it a model offering 2.4 GHz or 5 GHz support—can choose from a maximum of 16 logical WLAN networks.

Physic. WLAN parameters

A set of physical parameters that the AP WLAN modules are supposed to work with.

IP address of alternative WLCs

A list of WLCs that the APs should attempt to connect with. The AP starts searching for a WLC with a broadcast. Defining alternative WLCs is worthwhile when a broadcast cannot reach all WLCs (e.g. if the WLC is located in another network).

802.11u venue profile


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.

Configuration delay

Here you specify a time delay before an AP managed by the WLAN controller activates the configuration transmitted to it.

This is especially useful in AutoWDS scenarios where multiple managed APs are connected in a chain of point-to-point links. A premature change in configuration on an AP that connects to a more distant AP would otherwise cause this connection to be cut.

A rule of thumb for calculating the delay is (regardless of the topology): One second per managed AP, e.g. 200 seconds for 200 APs.

 The delay does not apply to transmitted scripts.

Device LED profile

The device LED profile selected here applies to the WLAN profile. To manage the devices LED profiles, see **WLAN controller > Profiles > Advanced profiles > Device LED profiles**.

LBS general profile

The general LBS profile selected here applies to the WLAN profile. You select the general LBS profile under **WLAN Controller > Profiles > Advanced profiles** with the button **LBS - General**.

Wireless ePaper profile

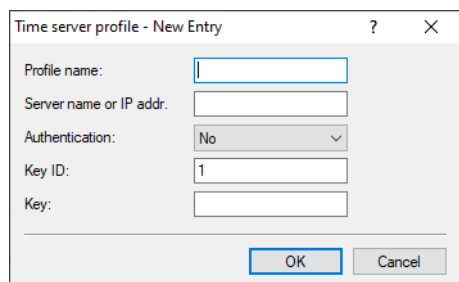
The Wireless ePaper profile selected here applies to the WLAN profile. You manage the Wireless ePaper profiles under **WLAN Controller > Profiles > Advanced profiles** with the button **Wireless ePaper profiles**.

Wireless IDS profile

The Wireless IDS profile selected here applies to the WLAN profile. You manage the Wireless IDS profiles under **WLAN Controller > Profiles > Advanced profiles** with the button **Wireless IDS profiles**.

Time server profile

The Time server profile selected here applies to the WLAN profile. You manage the Time server profiles under **WLAN Controller > Profiles > Advanced profiles** with the button **Time server profiles**.



Time server profile - New Entry

Profile name:

Server name or IP addr.:

Authentication:

Key ID:

Key:

OK Cancel

Profile name

The name of this NTP profile.

Server name or IP addr.

The server name or IP address of the NTP server.

Authentication

Enables or disables MD5 authentication for the server.

Key ID

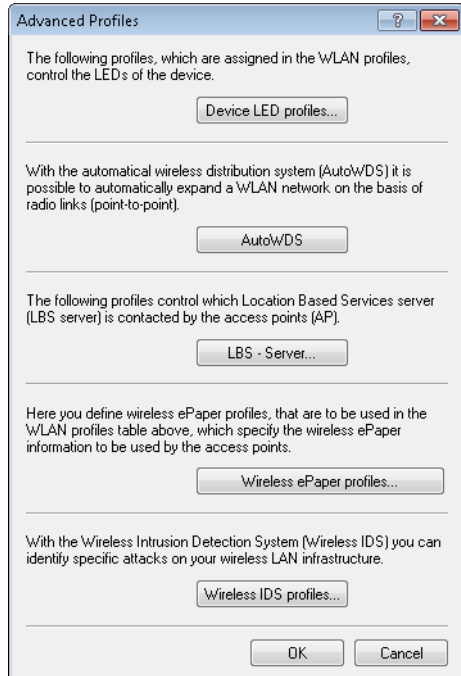
Identifies the key used for MD5 authentication for the server.

Key

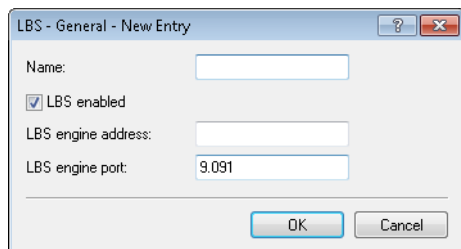
The value of the key for authentication with the NTP server.

General LBS profile and device location profile

In order to conveniently manage the settings for location-based services servers (LBS) and the AP locations by means of a WLC, you create the appropriate profiles for LBS servers via the menu **WLAN Controller > Profiles** and the button **Advanced profiles**.



The button **LBS - Server** opens the dialog for creating a general LBS server profile.



Name

Enter a descriptive name for the profile.

LBS enabled

Enable or disable LBS.

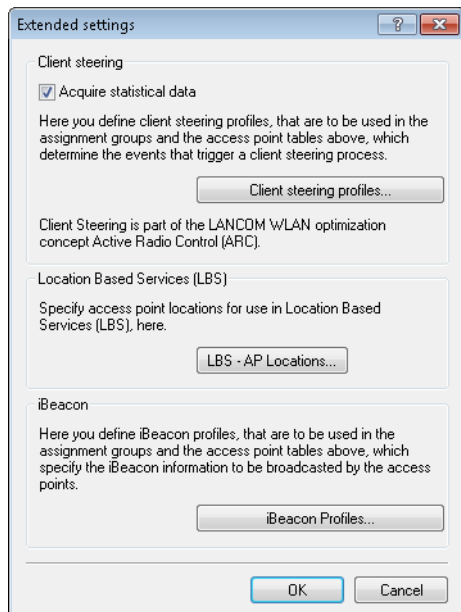
LBS server address

Enter the address of the LBS server.

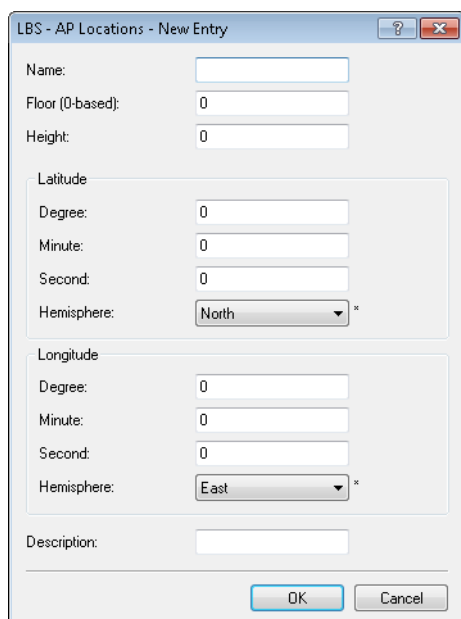
LBS server port

Enter the port used by the LBS server (default: 9091).

You create the corresponding profile for locations of the LBS APs under **WLAN controller > AP configuration** with the button **Extended settings**.



The button **LBS - AP locations** opens the dialog for creating a location profile for the LBS APs.



Name

Enter a descriptive name for the profile.

Floor (0-based)

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Degrees (latitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (latitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (latitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (latitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical latitude:

- > North: Northerly latitude
- > South: Southerly latitude

Degrees (longitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (longitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (longitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (longitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical longitude:

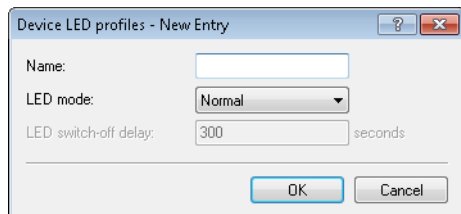
- > East: Easterly longitude
- > West: Westerly longitude

Description

Enter a description of the device.

Device LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile under **WLAN Controller > Profiles > Device LED profiles** and assign this to a WLAN profile.



Name

Give a name to the device LED profile here.

LED mode

The following options are available:

- > **Normal:** The LEDs are always enabled, also after rebooting the device.

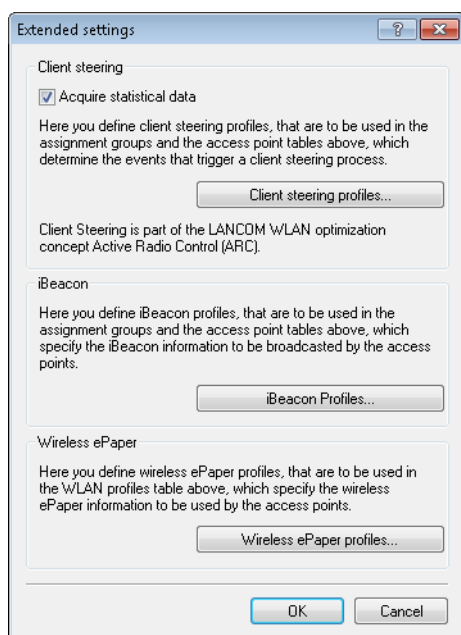
- **Timed off:** After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.
- **All off:** The LEDs are all off. Even after restarting the device, the LEDs remain off.

LED switch-off delay

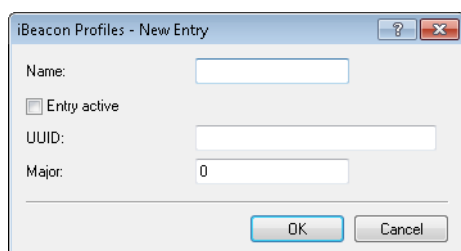
The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

ESL- and iBeacon profiles

In order to use a WLC to manage the settings of the Wireless ePaper information and iBeacon information of the individual APs, you create the corresponding profiles for Wireless ePaper and iBeacon via **WLAN-Controller > AP-Configuration** with the button **Extended settings**.



The button **iBeacon profiles** is used to create iBeacon profiles for the assignment groups and the AP table, which specify the iBeacon information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

UUID

Unique identification of the transmitter

Major

Specifies the Major value of the iBeacon.

The button **Wireless ePaper profiles** is used to create Wireless ePaper profiles for the WLAN-profiles table, which specify the Wireless ePaper information to be broadcast by the individual APs.

Name

Name of the profile

Entry active

Activates or deactivates this profile.

Server address

IP address of the Wireless ePaper Server.

Source address (optional)


Enter loopback address here.

Port

Specifies the port.

Channel Profile Table

You create the configuration of the WLAN channels via **WLAN Controller > Profiles > Advanced Profiles > Channel Profiles**. Within the channel profile, the WLAN channels can be defined for each frequency band. In this way, you can also uniquely define channels whose numbering is repeated in different frequency bands (e.g., at 2.4 GHz and 6 GHz). Then link newly created channel profiles within the physical WLAN profile.

 The DEFAULT profile activates all allowed channels.

Name

Name of the profile.

2.4 GHz channels

Select the 2.4 GHz channels for this profile.

5 GHz channels

Select the 5 GHz channels for this profile.

6 GHz channels

Select the 6 GHz channels for this profile.

Link Aggregation profiles

LACP according to IEEE 802.1AX allows several Ethernet connections to be bundled in a so-called LAG (Link Aggregation Group) in order to increase the achievable data throughput within the LAG. For this purpose, the outgoing packets on the sending side are distributed to the various individual links within the LAG on the basis of the configured frame distribution policy.

You create the configuration of the link aggregation profiles under **WLAN Controller > Profiles > Advanced Profiles > Link aggregation profiles**.

Name

The name of this LAG (Link Aggregation Group).

Activated

Enables or disables this LAG (Link Aggregation Group).

System priority

The system priority of this LAG (Link Aggregation Group).

Frame distribution policy

Frame distribution policy of this LAG (Link Aggregation Group). Possible options:

Flow-Hash

For outgoing packets, a flow hash is formed over the IP addresses and TCP/UDP ports contained and the packets are distributed to the individual links of the LAG on the basis of this. This achieves a distribution at session level, so that sessions of a single client can also be distributed to multiple links. This setting is recommended for most scenarios.

Source-Dest-MAC

Outgoing packets are distributed to the individual links of the LAG based on the contained pair of source MAC address and destination MAC address.

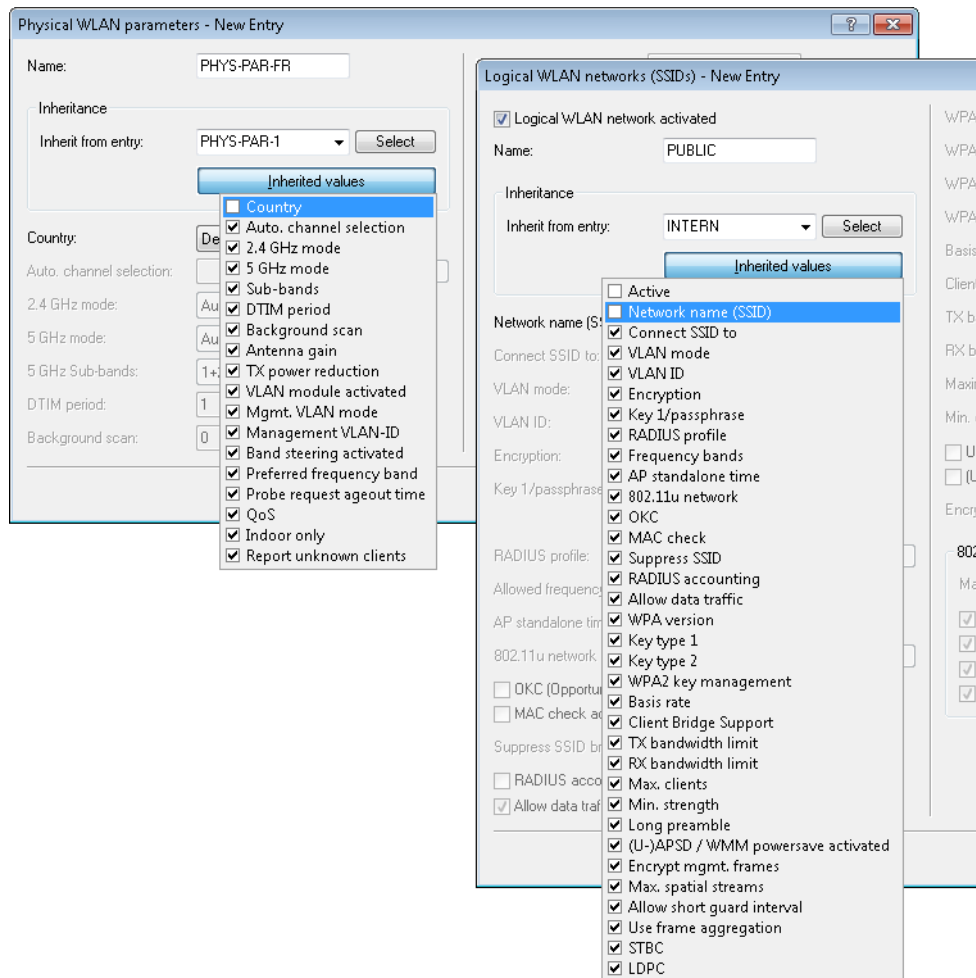
Inheritance of parameters

A WLC is capable of managing a wide range of different APs at different locations. However, WLAN profiles include settings that are not equally suitable for every type of AP that can be managed. For example, there are differences between the country settings and the device properties.

In order to avoid having to maintain multiple redundant WLAN profiles to cater for countries or device types, it is possible to "inherit" selected properties from the logical WLAN networks and the physical WLAN parameters.

1 WLAN management

1. You should initially generate the basic settings that are valid for the majority of the managed APs.
2. You can then start to generate entries for the more specific values, e.g. physical settings for a certain country, or a logical WLAN network for public access by mobile clients.



3. Select the entry from which the values are to be inherited and mark the values for inheritance. Parameters inherited in this way are displayed in the configuration dialog in gray and they cannot be edited.
4. Depending on the application, the WLAN settings collected in this way are then grouped into separate profiles, and these are then assigned to their respective access points.

! Inheritance fundamentally allows chains over multiple stages (cascading). This means, for example, that country and device-specific parameters can be grouped for convenience.

Recursion is also possible—profile A inherits from profile B, and at the same time B inherits from A. However, the parameters available for inheritance are limited to one "inheritance direction" per parameter.

Logical WLAN networks

Under **WLAN Controller > Profiles > Logical WLAN networks** you set the logical WLAN network parameters that the WLC assigns to the APs. The following parameters can be defined for each logical WLAN network:

Logical WLAN network activated


Enable the logical WLAN network by clicking on this option.

Name

Here, specify a name which uniquely identifies the logical WLAN network.

Inheritance

If you wish to create entries that differ only slightly from existing ones, you can choose a "parent" entry here and select the parameters which are to be applied each time it is used.

 A "parent" entry itself can contain inherited entries. Try to ensure that the structure of inherited entries is not too complex, otherwise they may be difficult to understand and configure.

Network name (SSID)

Enter the SSID of the WLAN network here. All stations that belong to this WLAN network must use the same SSID.

SSID connect to

Here you select which of the AP's logical interfaces is to be associated with the SSID, i.e. where the AP sends the data packets for this SSID.

- > "LAN": The AP forwards the data packets locally into the LAN (LAN-1) by default. It must be configured appropriately to do this.
- > "WLC-Tunnel-x": The SSID is connected to a WLC bridge layer-3 tunnel. The AP sends all data packets to this tunnel and thus to the WLC. This tunnel must be configured on the WLC.
- > "L2TP-ETHERNET-x": The SSID is connected to an L2TPv3-Ethernet tunnel. This enables the automatic break-out of WLAN SSIDs through L2TP-Ethernet tunnels. General information about L2TPv3 can be found in the reference manual in section "Layer-2 tunneling protocol (L2TP)". L2TPv3 tunnels are recommended as an alternative to the classic WLC layer-3 tunnel if the latter limits the WLAN throughput. Higher maximum throughputs can be achieved with L2TPv3. Then adjust the usage of the L2TP-ETHERNET-x interface used on the WLC, e.g. for further use on the IP router or LAN bridge.



Both the WLC and the managed access points must support LCOS 10.50 or higher.



Note that although forwarding all data packets to the WLC allows you to define routes and filters centrally, this creates a heavy load on the WLC. This model demands a correspondingly high bandwidth in order to transfer all of the data traffic of this and any other SSIDs that are connected to this WLC via WLC tunnel.

VLAN mode

This item sets the AP VLAN mode for packets belonging to this WLAN network (SSID). VLAN IDs are used if the VLAN module is enabled in the physical WLAN parameters of the AP. Otherwise the AP ignores all VLAN settings in the logical networks. Even with VLAN activated, it is possible to operate the network untagged.

- > "Untagged": The AP does not tag data packets from this SSID with a VLAN ID.



Even with VLAN activated, it is possible to operate a WLAN network untagged. The VLAN ID '1' is reserved internally for this.

- > "Tagged": The AP marks the data packets with the VLAN ID specified as follows.

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).

Encryption

This item sets the encryption method or, in the case of WEP, the key length for packet encryption in this WLAN.

Key 1 / passphrase

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "0x". The following character string lengths result for the formats used:

- > WPA-PSK: 8 to 63 ASCII characters
- > WEP128 (104 bit): 13 ASCII or 26 hex characters
- > WEP64 (40 bit): 5 ASCII or 10 hex characters

RADIUS profile

Specify which RADIUS profile the AP should receive for this network, so that it can connect directly to the RADIUS server if necessary. Leave this field blank if the WLC is to handle RADIUS requests.



You configure the RADIUS profiles in the corresponding table.

Allowed frequency bands

Here you set the frequency band used by network participants for transmitting data on the wireless network. You can select the 2.4-GHz band, the 5-GHz band, or both bands. In addition, the 6 GHz band is available.

Indefinite standalone operation

If the standalone operation for the WLC is configured so that the WLAN networks are broadcast indefinitely (value: 9999), this applies to networks with local break-out on the LAN as well as to networks connected via WLC tunnel. If the WLC fails, both types of network will continue to be broadcast: However, this only makes sense for local break-out networks on the LAN, since networks connected via the WLC tunnel have lost their end point (the WLC) and are therefore out of operation.

This option allows the two types of networks to be treated separately.

- > With this option enabled, local break-out networks will indefinitely operate standalone. In contrast, networks that break-out via a WLC tunnel are only broadcast if the WLC can be reached.
- > Without this option enabled, the time specified under **AP standalone time** applies.


AP standalone time


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

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

If there is no connection to the WLC after this time period has expired then the flash configuration is deleted and the AP goes out of operation. As soon as the WLC can be reached again, the WLC transmits the configuration to the AP again.

This represents an effective measure against theft as the AP deletes all security-related configuration parameters after this time has expired.

 If the AP establishes a backup connection to a secondary WLC then the countdown to the expiry of standalone operation stops. The AP and its WLAN networks remain active as long as there is a connection to a WLC.

 Please note that the AP only deletes the configuration in flash memory after the time for standalone operation has expired, and not when the power is lost!

Timeframe

Select one of the time frames defined in **WLAN controller > General > Time frame**. This can be used to restrict the broadcast of this SSID to the times defined there. This can be used, for example to activate a WLAN in a school only during class times.

802.11u network profile

Select the Hotspot 2.0 profile from the list.

OKC activated

This option enables the opportunistic key caching. OKC makes it easy for WLAN clients to quickly and conveniently roam between WLAN cells in wireless environments with WPA2-Enterprise encryption.

MAC check activated

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

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 AP publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the AP responds with the SSID of the radio cell (public WLAN).
- **Yes:** The AP does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the AP similarly responds with an empty SSID.
- **Tightened:** The AP does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the AP does not respond.



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

RADIUS accounting activated

Select this option if you want to enable the RADIUS accounting in this logical WLAN network.

Allow traffic between stations of this SSID

Check this option if all stations logged on to this SSID may communicate with one another.

WPA-Version

Here you select which WPA version the AP is to offer to the WLAN clients for encryption.

- WPA1: WPA2 only
- WPA2: WPA2 only
- WPA3: WPA3 only
- WPA1/2: WPA1 and WPA2 in one SSID (radio cell)
- WPA2/3: WPA2 and WPA3 in one SSID (radio cell)
- WPA1/2/3: WPA1, WPA2 and WPA3 in one SSID (radio cell)

WPA1 session key type

If you use "802.11i (WPA)-PSK" for encryption, the method for generating a WPA1 session or group key can be selected here:

- AES: The AP uses the AES method.
- TKIP: The AP uses the TKIP method.
- AES/TKIP: The AP uses the AES method. If the client hardware does not support the AES method, the AP will change to the TKIP method.

WPA2 and WPA3 session key types

The method for generating the session or group key for WPA2 and WPA3 is selected here.


Basis rate

The defined basis rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster". By setting the transmission rate to auto, the AP collects information about the transmission rates of the various WLAN clients. Clients automatically notify the AP of this rate with each unicast communication. The AP takes

the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

Client bridge support

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

 Client-bridge mode is only available between two LANCOM devices.

TX bandwidth limit

With this setting, you define the overall bandwidth that is available for transmission within this SSID. A value of 0 disables the limit.

RX bandwidth limit

With this setting, you define the overall bandwidth that is available for reception within this SSID. A value of 0 disables the limit.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

Maximum count of clients

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


Min. 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 AP stops sending probe responses and discards the client's requests.

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

Client disassociation signal strength

If values drop below this threshold, the client is disassociated. This prevents the client from sticking with a WLAN connection that is actually unusable because of the poor signal rather than switching to a better cell phone connection—behavior that is all too common for mobile phones and can be very annoying for the user.

 This threshold only works if the value **Minimum client signal strength** is also set and the **Client disassociation signal strength** is less than this value.

Enable LBS tracking

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



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

LBS tracking list

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

Use long preamble for 802.11b

Normally, the clients in 802.11b mode negotiate the length of the preamble with the AP. "Long preamble" should only be set when the clients require this setting to be fixed.

(U)APSD / WMM Power Save activated

Enable this option to signal stations that the power saving function (U)APSD ([Unscheduled] 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 AP. If the AP 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 APs are WMM® Power Save CERTIFIED by the Wi-Fi Alliance.

Max. spatial streams

The spatial multiplexing function allows the AP to transmit multiple data streams over separate antennas in order to increase the data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.



In the 'Auto' setting, the AP uses all of the spatial streams supported by this WLAN module.

Allow short guard interval

This option is used to reduce the transmission pause between two signals from 0.8 s (default) to 0.4 s (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

Use frame aggregation

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This procedure reduces the overhead of the packets to increase the throughput.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

STBC (space time block coding) activated

Activate the space time block coding here.

The function 'STBC' additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

LDPC (low density parity check) activated

Activate the low density parity check here.

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Physical WLAN parameters

Here the physical WLAN parameters are set for assignment to the access points. For each set of physical WLAN parameters you can specify the following parameters under **WLAN controller > Profiles > Physical WLAN parameters**:

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.

Channel profile

Select a channel profile. See [Channel Profile Table](#) on page 24.

 The DEFAULT profile activates all allowed channels of the set country.

DTIM period


If just one mobile client operates power-saving mechanisms, broadcasts and multicasts are no longer transmitted in the radio cell immediately. Instead, they are buffered and sent after the beacon that is transmitted regularly by the access point. The clients are informed about their next relevant beacon so they can synchronize with the broadcasts and multicasts, and this allows them to leave their radio module switched off for most of the time and to activate it only when necessary.

The DTIM period specifies how many beacons are sent before the buffered broadcast and multicasts are transmitted. Higher values allow clients to save more power, but also increase the latency of delivering these packets.

The default value is 1, i.e. buffered broadcasts and multicasts are sent after every beacon.

Management VLAN-ID

The VLAN ID of the management network used to manage the APs.

 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.

Client steering

This entry sets the method used for client steering and whether the AP should activate band steering. In this case, a dual-port access point can forward a WLAN client to a preferred frequency band.

With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLAN controller. Managed access points constantly report the current values to the WLAN controller, which uses these criteria to decide which access points may respond to requests from WLAN clients. For this reason, client steering is only possible with access points that are centrally managed by a WLAN controller.

Off

Client steering is deactivated.

On

The AP lets the WLC handle the client steering.

Client management


The client steering is handled decentrally by the APs.

AP-based band steering


The AP independently steers the WLAN client to a preferred frequency band.

Report seen unknown clients

By default, the access point only reports associated clients to the WLC. If all other seen clients should be reported, i.e. unassociated clients as well, you can activate this switch. This will increase the traffic on the network. You should therefore activate this switch only temporarily or for test purposes.

 If you have a large number of unknown clients (e.g., with a Public Spot or in areas with lots of traffic), you should not activate this switch, otherwise you will be flooded by inbound messages.

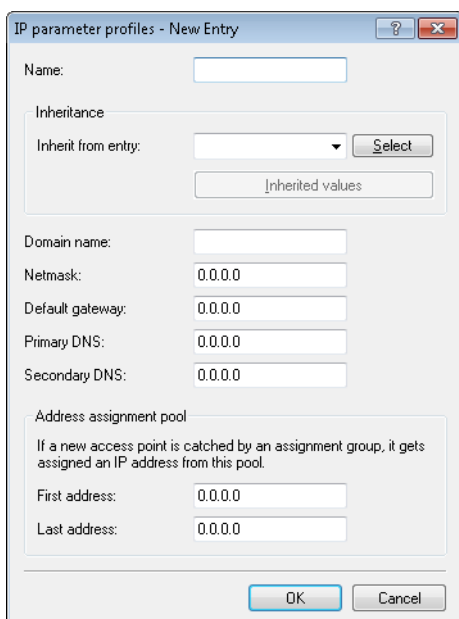
 All other physical WLAN parameters correspond to those for the standard configuration of APs.

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

1.4.3 Access point configuration

IP parameter profiles

This table is used to configure specific network profiles that are assigned with APs that must not be automatically configured by the WLC by means of DHCP. In this way you set which specific IP parameters are used by an AP.



Name

Name of the IP parameter profiles.

Inheritance

Selection of an IP parameter profile defined earlier and from which the settings are to be inherited (see [Inheritance of parameters](#) on page 25).

Domain name

Name of the domain (DNS suffix) which is to use this profile.

Netmask

Netmask of the profile

Default gateway

The gateway used by the profile as standard.

DNS default

The DNS (Domain Name System) to be used by the profile.

DNS backup

Second, alternative DNS if the first is unavailable.

Start address

The start of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

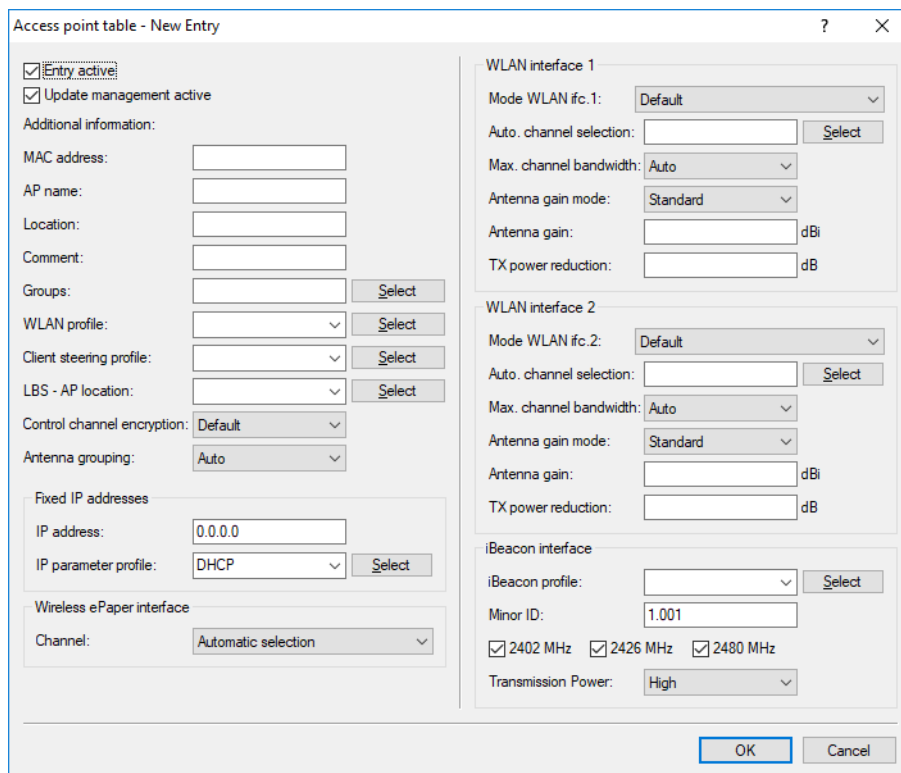
End address

The end of the IPv4 address range from which a new AP receives an IP address if the WLC can allocate an assignment group to the AP and you have not defined a specific IP address for the AP in the AP table.

For further information on assignment groups, please refer to the section *IP-dependent auto configuration and tagging of APs* on page 70.

List of access points

The access point table is a central element of the configuration for WLCs. Here, the WLC assigns WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) to the access points via their MAC addresses. Furthermore, the mere existence of an entry in the access-point table for a particular access point affects its ability to establish a connection to a WLC. Under **WLAN Controller > AP Configuration > Access point table** you can define the following parameters for each access point:



Active

Activates or deactivates this entry.

Update management active

Activating update management for this access point enables it to download the latest firmware and script versions automatically. All other settings are adjusted under access point update (*Central firmware and script management*).

MAC address

MAC address of the access point

AP name

Name of the access point in managed mode.

Location

Location of the access point in managed mode.

Groups

Assigns the access point to one or more groups

WLAN profile

WLAN profile from the list of defined profiles.

Client steering profile

Client-steering profiles control how the WLC decides which access points are to accept a client at the next login attempt.

LBS AP location profile

LBS location profile from the list of defined profiles.

Control channel encryption

Encryption for the communication over the control channel. Without encryption, access points and WLC exchange their control data in cleartext. In both cases authentication is by certificate.

Antenna grouping

Antenna grouping can be configured in order to optimize the gain from spacial multiplexing.

IP address

Here you specify a fixed IP address of the access point.

IP parameter profile

Here you specify the profile name used by the WLC to reference the IP settings for the access point. If you retain the default setting DHCP, the WLC ignores the setting for the fixed IP address and the access point is forced to obtain its IP address via DHCP.

Channel (Wireless ePaper interface)

Here you specify how the channel is selected for the Wireless ePaper interface.

Mode WLAN ifc.1 1

This setting allows you to configure the frequency band in which the access point operates the 1st physical WLAN interface. When set to **Default**, the access point independently selects the frequency band for the physical WLAN interface. The access point prefers the 2.4 GHz band, if available.

Mode WLAN ifc.1 2

This setting allows you to configure the frequency band in which the access point operates the 2nd physical WLAN interface. When set to **Default**, the access point independently selects the frequency band for the physical WLAN interface. The access point prefers the 5 GHz band, if available.



If a managed access point only has one physical WLAN interface, the access point ignores the settings for the 2nd physical WLAN interface.

Auto Channel selection

Access points automatically carry out channel selection for the frequency band available in the country of operation, assuming that no entry is made here.

Enter the channels to be available for automatic selection by the first WLAN module. If you enter just one channel here, the access point uses this channel only and no automatic selection takes place. For this reason

you should ensure that the channels entered here are legal for use in the defined country of operation. The access point ignores channels that are invalid for the frequency band.

Max. channel bandwidth

Enter how and to what extent the access point specifies the channel bandwidth for the physical WLAN interface(s). The following values are possible:

- **Automatic:** The access point automatically detects the maximum channel bandwidth (default).
- **20 MHz:** The access point uses channels bundled at 20 MHz.
- **40 MHz:** The access point uses channels bundled at 40 MHz.
- **80 MHz:** The access point uses channels bundled at 80 MHz.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Antenna gain mode

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

Possible values:

Standard

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

Userdefined

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

Antenna gain

This item allows you to specify the antenna gain factor (in dBi) minus attenuation of the cable and (if applicable) lightning protection. Based on this, as well as depending on the country where the system is operated and the frequency band, the access point calculates the maximum permitted transmission power.


If you leave the field blank, the access point uses the default setting from the configuration group in the relevant WLAN profile.

You can reduce the transmission power to a minimum of 0.5 dBm in the 2.4-GHz band or 6.5 dBm in the 5-GHz band. This limits the maximum value that can be added to 17.5 dBi in the 2.4-GHz band and 11.5 dBi in the 5-GHz band.



Be sure that your combination of antenna, cable and lightning-protection complies with the legal requirements of the country where the system is operated.

The receiver's sensitivity is unaffected by this.

 The current transmission power is displayed by WEBconfig or telnet under **Status > WLAN-statistics > WLAN-parameters > Transmission-power** or with LANmonitor under **System information > WLAN card > Transmission power**.

TX power reduction

If you use an antenna with a high amplification factor, you can use this entry to attenuate the transmission power of your access point to the level permitted on the frequency band in the country of operation.

If you leave the field blank, the access point uses the default setting from the configuration group in the relevant WLAN profile.

The same values and constraints apply as for the field **Antenna gain**.

iBeacon profile (iBeacon interface)

Select an iBeacon profile from the list of profiles created.

 You create iBeacon profiles under **WLAN Controller > AP configuration > Extended settings > iBeacon profiles**.

Minor

Set a minor ID for the iBeacon module.

2402 MHz, 2426 MHz, 2480 MHz

Specify here which channels the iBeacon module uses to transmit.

Transmission power

Specify the power used by the iBeacon module to transmit. The following values are possible:

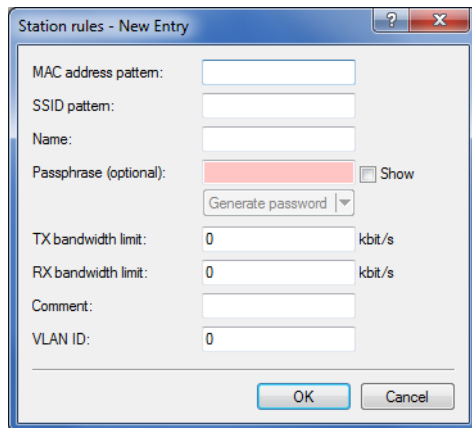
- > **High:** The module sends with maximum power (default).
- > **Medium:** The module sends with medium power.
- > **Low:** The module sends with minimum power.

Stations

The station rules define which WLAN clients can associate with the WLAN networks of the APs that are centrally managed by the WLC. Furthermore, the method offers a convenient way to give each WLAN client an individual authentication passphrase and a VLAN ID.

To use the station rules, it is imperative that the RADIUS server is activated in the WLC under **WLAN Controller > Stations/LEPS > LEPS-MAC > Station rules**. As an alternative, requests can be forwarded to another RADIUS server. More information on RADIUS is available under [RADIUS](#).

For every logical WLAN in which WLAN clients are authenticated by RADIUS, the MAC check has to be activated.



MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address


A MAC address in the format 00a057112233, 00-a0-57-11-22-33 or 00:a0:57:11:22:33.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. 00a057*, 00-a0-57-11-??-?? or 00:a0:?:?:11:.*.


Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

 It is possible to use wildcards.

SSID pattern

WLAN clients with the corresponding MAC addresses have access that is limited to this SSID.

 The use of wildcards makes it possible to allow access to multiple SSIDs.

Name

You can enter any name you wish and a comment for any WLAN client. This enables you to assign MAC addresses more easily to specific stations or users.

Passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

TX bandwidth limit

Transmission-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.

RX bandwidth limit

Reception-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses these two values to set the minimum bandwidth.


 The RX bandwidth restriction is only active for WLAN devices in client mode. For value is not used by normal WLAN clients.

Comment


You can enter a comment here.

VLAN-ID

The ID of the VLAN that this client belongs to. Consequently the client can only be reached by packets originating from the same VLAN. Packets sent by the client are marked with this VLAN ID. You only need to set this value if you want this client to belong to a different VLAN than the logical WLAN (SSID) that it is connected to. Valid VLAN IDs are in the range 0 to 4094. 0 means that the client belongs to the VLAN of its logical WLAN (SSID), if this belongs to a VLAN at all.

 If you use IPv6, or if multicast is operating on a VLAN, different group keys must be assigned to the different VLANs of an SSID. Otherwise the different multicasts are not be assigned to the correct clients. When using IPv6, for example, clients are informed of IPv6 prefixes that do not function on the VLAN ID. The group keys are configured under **Wireless LAN > Encryption > VLAN group key mapping**.

If filter rules contradict, the individual rule has a higher priority: A rule without wildcards in the MAC address or SSID takes precedence over a rule with wildcards. When creating these entries, the user should ensure that filter rules do not contradict. The definitions in the filters can be checked in a Telnet session with the trace command `trace WLAN-ACL`.

 The filter criteria in the station list either allow or deny WLAN clients to access your wireless network. The entries **Name**, **Bandwidth limit**, **VLAN ID** and **Passphrase** are meaningless if the device uses valid filter criteria to deny access to the WLAN.

Options for the WLAN controller

The **Options** area in the WLC configuration is used to define notifications in case of events and to set various default values.

Event notification

Notifications can be sent via SYSLOG or e-mail. You can define the following parameters:

LANconfig: **WLAN Controller > Options**

Activate event logging (SYSLOG)

Activates notification by SYSLOG.

Activate e-mail notification

Activates notification by e-mail.

Events

Selects the events that trigger notification. Possible values:

- > Report active AP
- > Report lost AP
- > Report new AP

Default parameters

For some parameters, default values can be defined centrally and these serve as reference default values for other parts of the configuration.

Here you define the logical WLAN networks for activation and operation via the associated access points (APs).

Logical WLAN networks (SSIDs)...

Here you define the physical WLAN parameters which apply to all of the logical WLAN networks that share a managed access point.

Physical WLAN parameters...

The following setting can be referenced in table entries by value 'Default'.

Default country: Europe

Here you define entire WLAN profile on the managed APs. This includes physical WLAN parameters.

By default, the WLAN controller will f communication between AP and RA the WLAN networks list.

With the automatical wireless distribu WLAN network on the basis of radio

... settings which can be used N networks and a set of

To enable direct DIUS profiles here for use in

... able to automatically expand a

- Europe
- Finland
- France
- Germany
- Ghana
- Greece
- Guatemala
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Ireland
- Israel
- Italy
- Japan
- Jordan
- Kuwait
- Latvia
- Lebanon
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Macedonia
- Malaysia
- Malta
- ...

LANconfig: WLAN Controller > Profiles > Default country

> Default 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.

- > Possible values:
 - > Selection from the list of available countries
- > Default:
 - > Europe

Default values

The following parameters are default settings which can be referenced in access point table entries by value 'Default'.

Mode WLAN ifc.1: 2.4 GHz

Mode WLAN ifc.2: 5 GHz

Control channel encryption: DTLS

LANconfig: WLAN controller > AP configuration >

WEBconfig: LCOS menu tree > Setup > WLAN-Management > AP-Configuration

> WLAN-Interface 1

Frequency of the first WLAN module. This parameter can also be used to deactivate the WLAN module.

> WLAN-Interface 2

Frequency of the second WLAN module. This parameter can also be used to deactivate the WLAN module.

> **Encryption**

Encryption for the communication over the control channel. Without encryption the control data is exchanged as cleartext. In both cases authentication is by certificate.

Virtualization and guest access via WLAN controller with VLAN

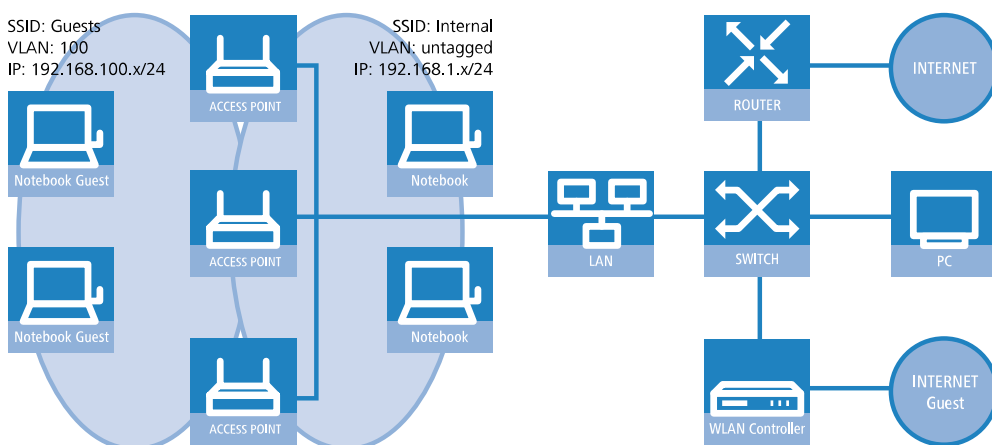
Many companies wish to offer Internet access to their visitors via WLAN. In larger installations the required settings apply to multiple access points, and these can be programmed centrally in the WLAN controller.

Targets

- > Wireless LAN infrastructure available to internal employees and guests
- > Shared physical components (cables, switches, access points)
- > Separation of networks with VLAN and ARF
- > Break-out of data streams to certain target networks:
 - > Guests: Internet only
 - > Internal employees: Internet, all local devices and services
- > Guests login to the WLAN with a Web form.
- > Internal employees use WLAN encryption for authentication.

Establish

- > Management of the access points is handled by the WLC.
- > The WLC serves as the DHCP server for the WLAN clients in the guest network.
- > The guest network is provided with Internet access via the WLC (e.g. separate DSL access or Internet access via the company DMZ).
- > The wired infrastructure is based on managed VLAN-capable switches:
 - > Access point VLAN management is handled by the WLC.
 - > The VLAN management of the switches is handled separately by the switch configuration.
- > The access points operate within the internal VLANs.



Wireless LAN configuration of the WLAN controllers

During the configuration of the WLAN, the necessary WLAN networks are defined and, along with the physical WLAN settings, are assigned to the access points managed by the controller.

1. Create a logical WLAN for guests and one for the internal employees:

- The WLAN with the SSID `GUESTS` uses the VLAN ID 100 (VLAN operating mode **Tagged**) and uses **no** encryption.
- The WLAN with the SSID `INTERNAL` receives no VLAN ID (VLAN operating mode **untagged**, i.e. packets are transferred in the Ethernet without a VLAN tag) and uses WPA encryption, e.g. **802 11i (WPA)-PSK**.

> LANconfig: **WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**

Logical WLAN networks (SSIDs) - New Entry

Logical WLAN network activated

Name: GUEST

Inheritance

Inherit from entry: [] Select

Inherited values

Network name (SSID): GUEST

Connect SSID to: LAN at AP

VLAN mode: Tagged

VLAN ID: 2

Encryption: None

Key 1/passphrase: [redacted] Show

Generate password

RADIUS profile: DEFAULT Select

Allowed frequency bands: 2.4/5 GHz

AP standalone time: 0 minutes

802.11u network profile: [] Select

OKC (Opportunistic Key Caching) activated

MAC check activated

Suppress SSID broadcast: No

RADIUS accounting activated

Allow data traffic between stations of this SSID

WPA version: WPA1/2

WPA1 session key type: TKIP

WPA2 session key type: AES

WPA2 key management: Standard

Basis rate: 2 Mbit/s

Client Bridge Support: No

TX bandwidth limit: 0 kbit/s

RX bandwidth limit: 0 kbit/s

Maximum count of clients: 0

Min. client signal strength: 0 %

Enable LBS tracking

LBS tracking list: []

Convert to unicast: DHCP

Use long preamble for 802.11b

(U-)APSD / WMM powersave activated

Encrypt mgmt. frames: No

802.11n

Max. spatial streams: Auto

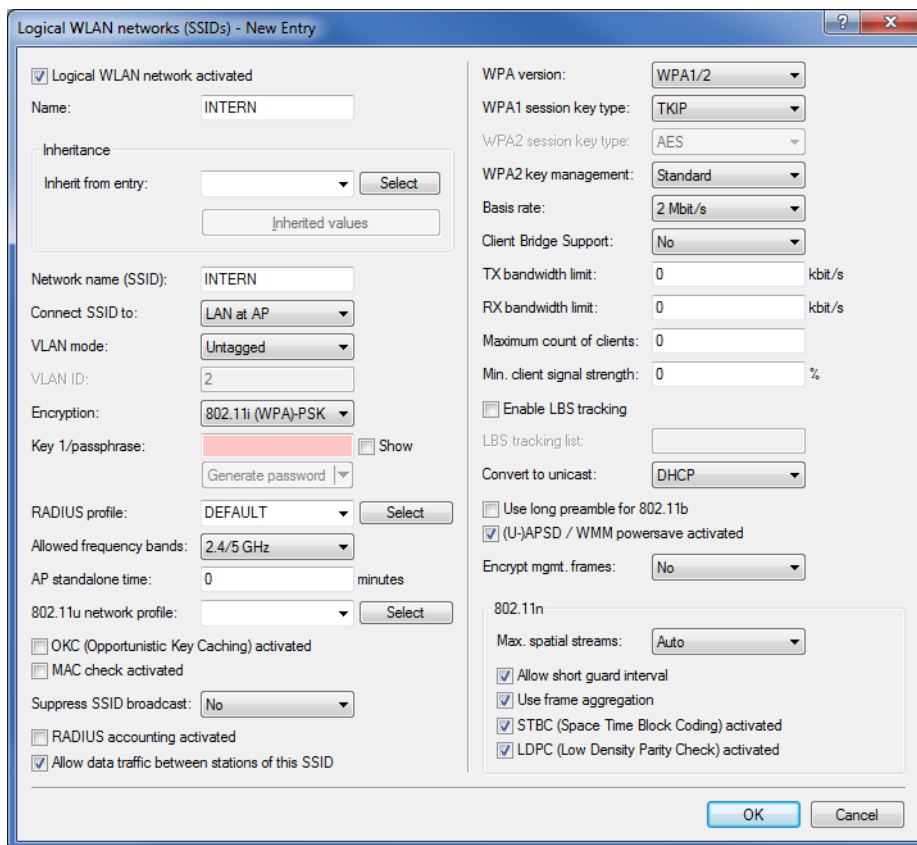
Allow short guard interval

Use frame aggregation

STBC (Space Time Block Coding) activated

LDPC (Low Density Parity Check) activated

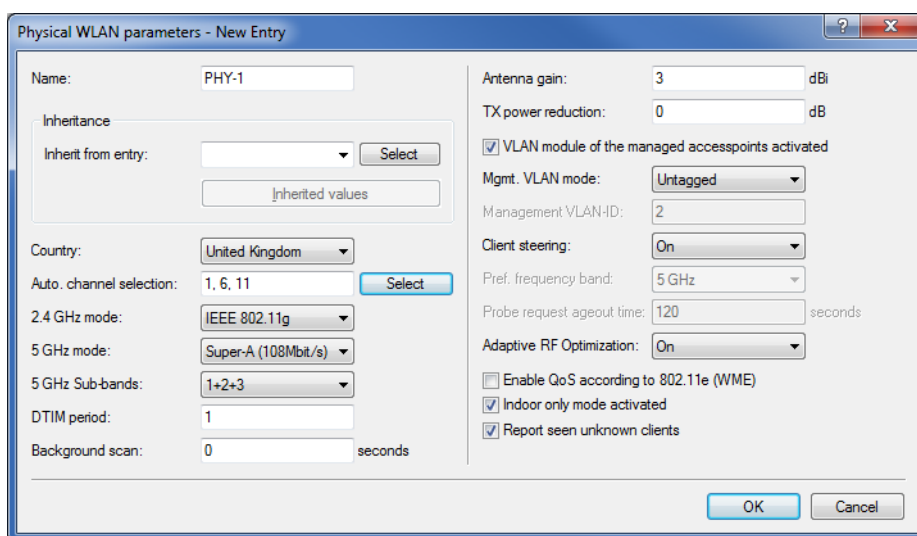
OK Cancel



! If you set the **VLAN mode** to **untagged**, LANconfig will gray-out the **VLAN ID** input field in the add/edit dialog shown above. However, the corresponding table **Logical WLAN networks (SSIDs)** still displays the assigned VLAN as a value in the grayed-out box. This entry is only of internal significance, as the acceptable range is between 2 and 4094. Ultimately it is the VLAN operating mode which is decisive: If this is set to **untagged**, then a VLAN ID is not transmitted under any circumstances.

2. Create a set of physical parameters for the access points.
The management VLAN ID is set to 1, which serves to activate the VLAN function (but without a separate management VLAN for the device; the management data traffic is transmitted untagged).

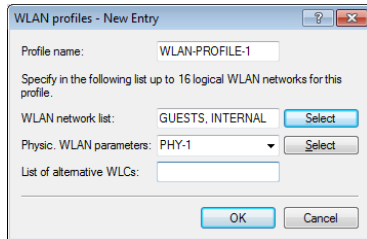
> LANconfig: **WLAN-Controller > Profiles > Physical WLAN parameters**



1 WLAN management

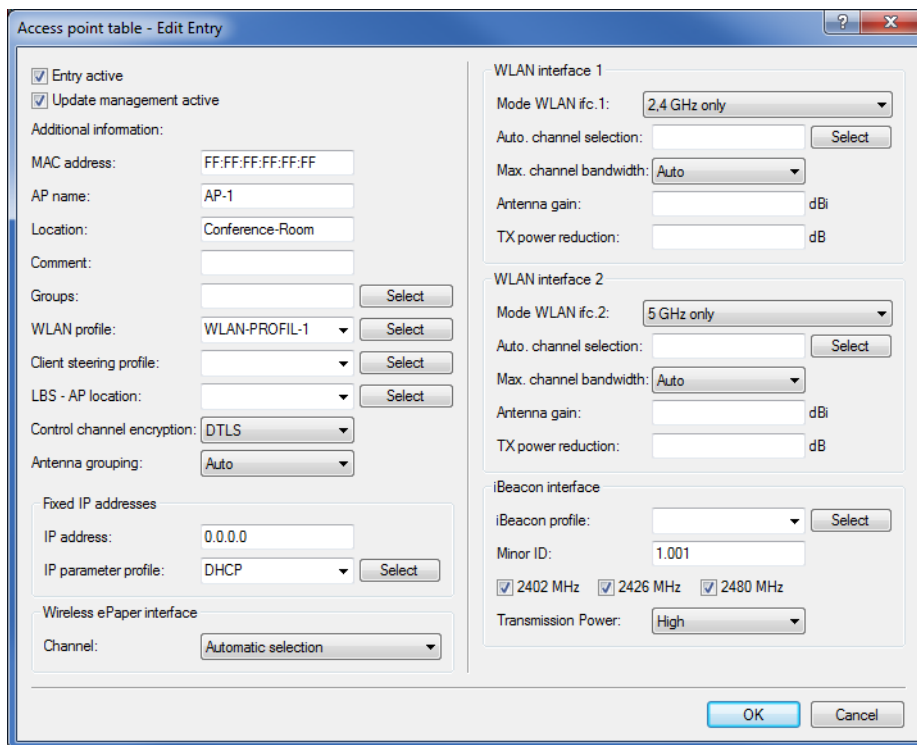
3. Create a WLAN profile that you can assign to the access points.
The two logical WLAN networks and the set of physical parameters defined earlier are collected into this WLAN profile.

➤ LANconfig: **WLAN-Controller > Profiles > WLAN-Profiles**



4. Assign this WLAN profile to the access points managed by the controller.
Do this by entering each access point with its MAC address into the access point table. Alternatively you can use the **Default** button to create a default profile, which applies to all access points.

➤ LANconfig: **WLAN controller > AP configuration > Access point table**



Configuring the switch (LANCOM GS-2326P)

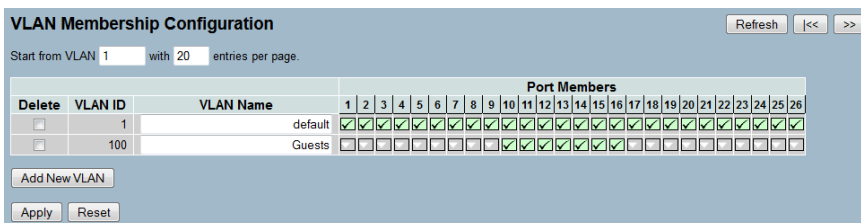
In this section we describe the configuration of the switch using the LANCOM GS-2326P as an example.

1. Under **Configuration > VLAN > VLAN-Membership**, create an additional VLAN group for the guest network.

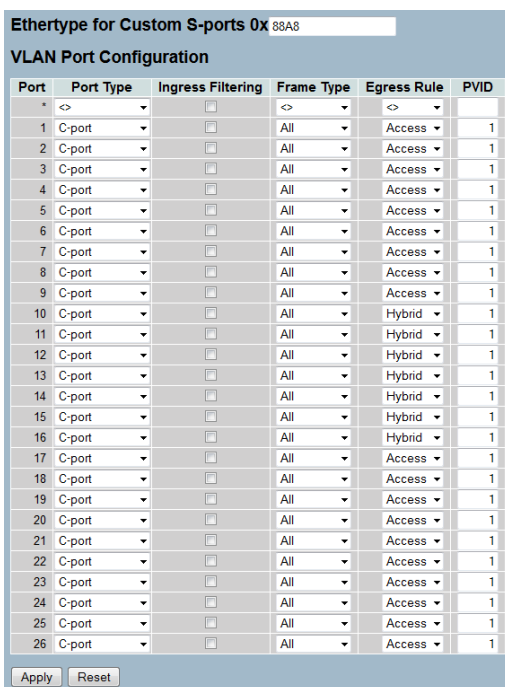
To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the group `default`, and that for the guests is mapped to the group `guests`.

➤ The VLAN group for the internal employees uses the default VLAN ID 1. This VLAN ID used for internal administration applies on all ports and is operated untagged, i.e. all untagged incoming data packets are given the VLAN ID 1 for internal routing, and this is removed again from outgoing data packets (see also "PVID" in the next step).

- The VLAN group for the guests uses the VLAN ID 100, which you entered earlier when configuring the WLAN in the controller. This ID applies only to the ports which the WLAN controller and the access points are connected to (in this example: Port 10 to 16, green checkmarks for **Port members**). The switch does not remove tags from outgoing data packets. i.e. all tagged incoming packets with VLAN ID 100 retain this tag and are routed only to the ports that are members of the corresponding group.



2. Under **Configuration > VLAN > Ports** set the **Port Type** for all ports to **C-port**. See the documentation about your switch for details about this setting.
3. Configure the **Egress rule** for each port.
 - All ports except port 10 to 16 are given the **Access** rule. As a result, these ports forward only tagged packets and all others are dropped.
 - The ports 10 to 16 are given the rule **Hybrid**. As a result, these ports forward both untagged and tagged packets.



⚠ Ensure that the **PVID** (port VLAN ID) for each port is set to a value of 1. The PVID is the VLAN ID that a port assigns to incoming data packets which do not already have a VLAN tag; Therefore, the PVID corresponds to the VLAN ID of the `default` group.

4. OPTIONAL: If you wish to allow access to the guest network via Ethernet, go to **Configuration > VLAN > Ports** and, for example, set the **PVID** to 100 for ports 17 to 20 and, under **Configuration > VLAN > VLAN-Membership**, assign these ports to the group `Guests`. All untagged incoming data packets arriving at these ports are given VLAN ID 100.

⚠ Note that these data packets can only leave the switch via the ports of the guest network.

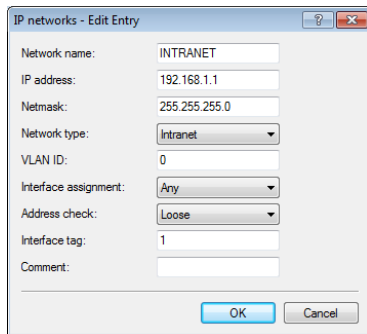
Configuring the IP networks in the WLAN controller

To separate the data streams on layer 3, two different IP networks are employed (ARF – Advanced Routing and Forwarding).

1. For the internal network, set the **INTRANET** to the address 192.168.1.1.

This IP network uses the **VLAN ID 0**. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The **interface tag 1** is used for the subsequent break-out of data in the virtual router.

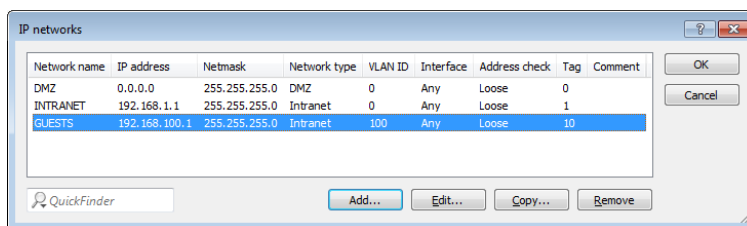
➤ LANconfig: **TCP/IP > General > IP networks**



2. For guests, create a new IP network with the address 192.168.100.1.

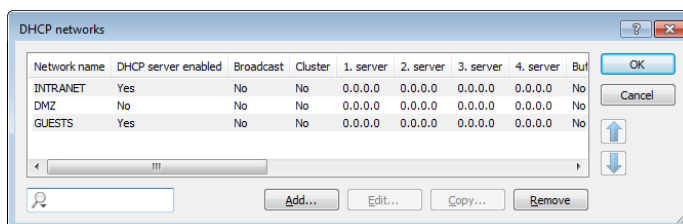
This network uses the **VLAN ID 100**. In this way, all data packets with this ID are assigned to the guest network. Here, too, the **interface tag 10** is used later by the virtual router.

➤ LANconfig: **TCP/IP > General > IP networks**

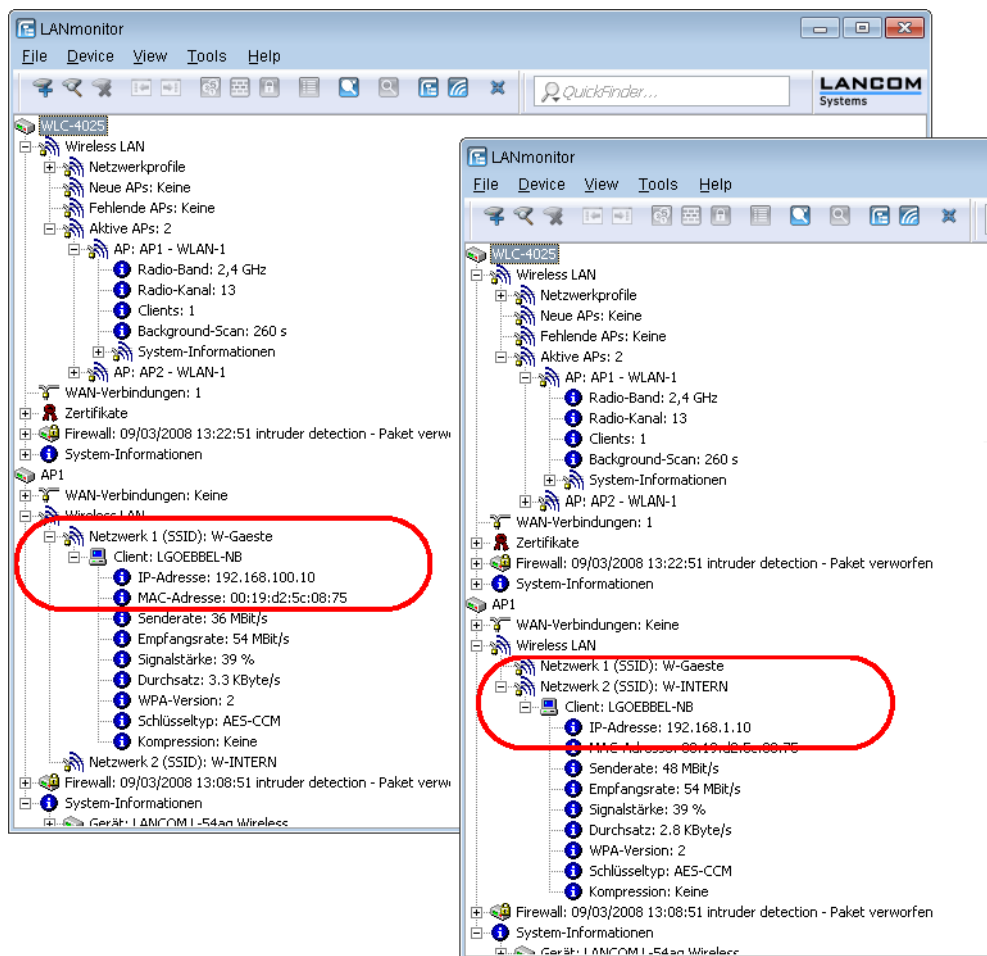


3. Enable the DHCP server for both IP networks.

➤ LANconfig: **TCP/IP > General > IP networks**



With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.

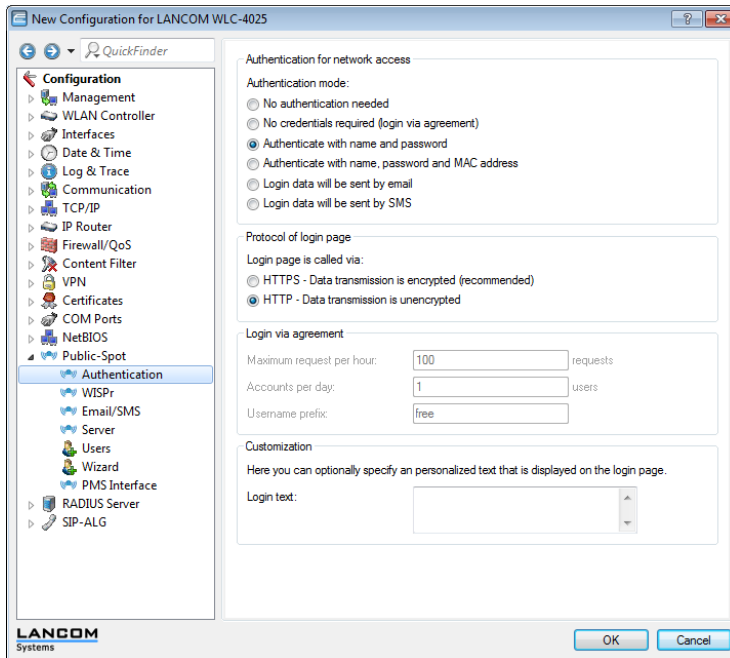


Configuring Public Spot access accounts

The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. Authentication is performed by requesting user information via a web interface. If necessary, you can set a time limit for the access.

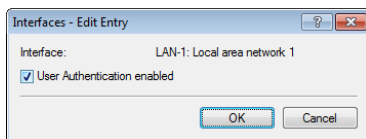
1. You should activate authentication for network access by name and password.

> LANconfig: **Public Spot > Authentication > Authentication for network access**



2. Activate user authentication for the controller's interface that is connected to the switch.

> LANconfig: **Public Spot > Server > Operation settings > Interfaces**

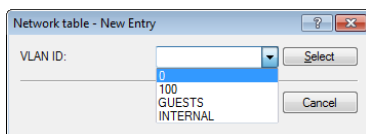


3. Restrict access to the Public Spot.

You restrict use of the Public Spot to data packets from this virtual LAN by entering the VLAN ID of "100" for the guest network into VLAN table. Other data packets from other VLANs will be forwarded to the Public Spot without a login.

! If the interface is not restricted to the VLAN ID, the controller will no longer be reachable at the specified physical Ethernet port!

> LANconfig: **Public Spot > Server > VLAN table**



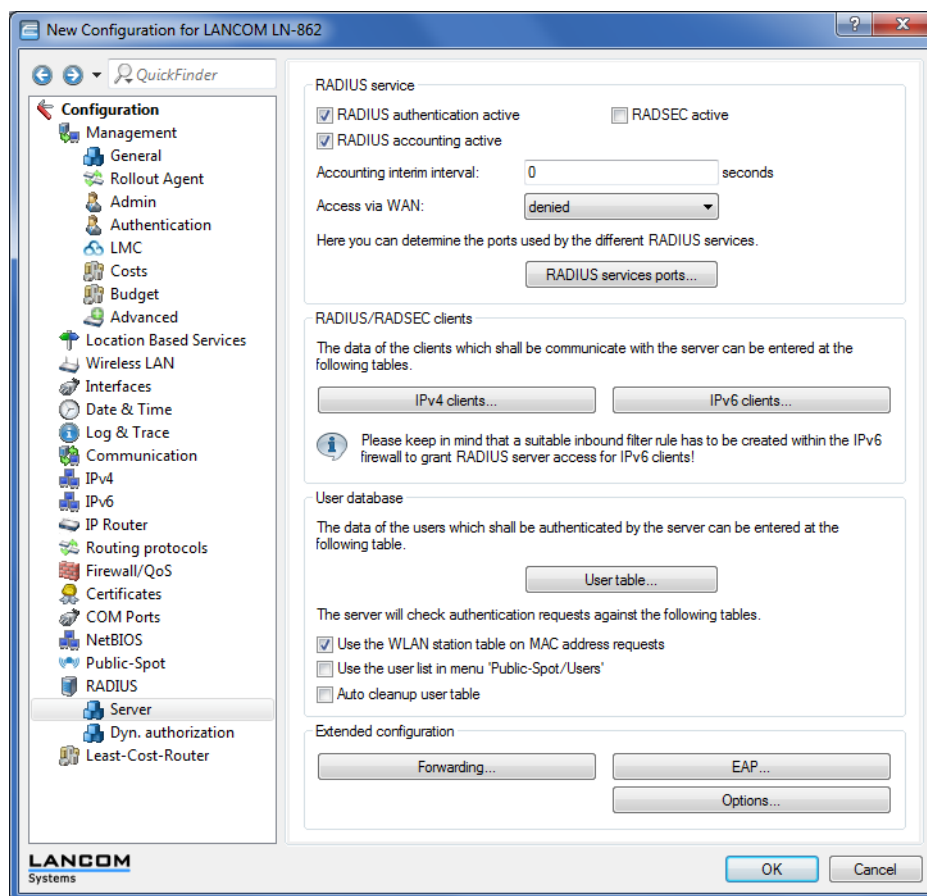
4. Enable the option to clean up the user table so that your device automatically deletes entries that are no longer needed.

> LANconfig: **RADIUS > Server > User table > Auto cleanup user table**

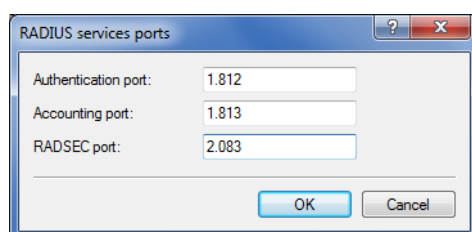
Configuring the internal RADIUS server for Public Spot operation

The Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. In order to use these Public Spot access accounts, the internal RADIUS server has been preconfigured with default values. You can inspect this setup in **LANconfig** as follows:

1. Navigate to **RADIUS > Server > RADIUS service**.
2. Ensure that checkmarks have been set for **RADIUS authentication active** and **RADIUS accounting active**.



3. Click the button **RADIUS services ports**.

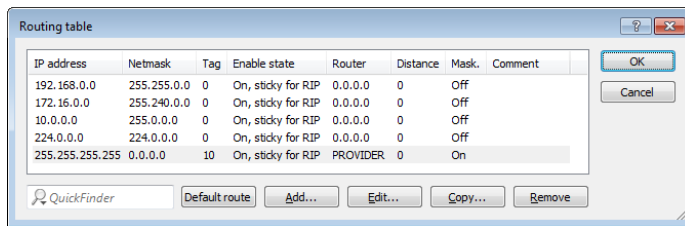


! The default settings are available here for inspection.

Configuring Internet access for the guest network

1. In order to provide Internet access for guest network users, there is a wizard to set up access to a provider network.
2. Limit access to the provider network.
In order for this access to be available to users of the guest network only, set the routing tag "10" for the corresponding route. This ensures that only data packets from the IP network "GUEST" with the interface tag "10" are transmitted to the provider's network. The different routing tag values ensure that data cannot be routed between the guest network and the internal network.

› LANconfig: **IP router > Routing > Routing table**



IP address	Netmask	Tag	Enable state	Router	Distance	Mask	Comment
192.168.0.0	255.255.0.0	0	On, sticky for RIP	0.0.0.0	0	Off	
172.16.0.0	255.240.0.0	0	On, sticky for RIP	0.0.0.0	0	Off	
10.0.0.0	255.0.0.0	0	On, sticky for RIP	0.0.0.0	0	Off	
224.0.0.0	224.0.0.0	0	On, sticky for RIP	0.0.0.0	0	Off	
255.255.255.255	0.0.0.0	10	On, sticky for RIP	PROVIDER	0	On	

3. Optional: If necessary, use **Device > Configuration Management > Upload certificate or file** in LANconfig to upload an HTML template and an image as a template to the device for output of the voucher. The image can be a GIF, JPEG or PNG file of max. 64 KB in size.

WLAN layer-3 tunneling

Introduction

The CAPWAP standard for centralized WLAN management offers two different channels for transmissions:

- › The obligatory control channel transports administrative data between the managed AP and the WLC.
- › The optional data channel transmits the payload data from the various WLAN networks (SSID) between the managed AP and the WLC.

The decision whether to use of the optional data channel between the managed AP and the WLC depends on the route to be taken by the payload data:

- › If you deactivate the data channel, the AP forwards the payload data directly to the LAN. In this case, you control the allocation of WLAN clients to specific LAN segments, for example by assigning VLAN IDs. The advantage of this application lies in the low load on the WLC and on the network as a whole, because the AP transmits only the management data via the CAPWAP tunnel and it transmits the payload data over the shortest available route.
- › If you activate the data channel, the AP additionally forwards the payload data to the central WLC. This approach has the following advantages:
 - › The APs can provide access to networks that are only available on the WLC, such as a central Internet access for a Public Spot.
 - › The WLANs provided by the APs (SSIDs) can be separated from one another without the use of VLAN. Avoiding the use of VLAN reduces the effort required for the configuration of other network components such as switches, etc.
 - › WLAN clients associated with the APs and in different IP networks can roam to other APs without interruption to their IP connections, because the connection is continually managed by the central WLC and not by the APs (layer-3 roaming).

The use of data channels forms additional logical networks on the basis of the existing physical infrastructure. These logical networks are known as overlay networks.

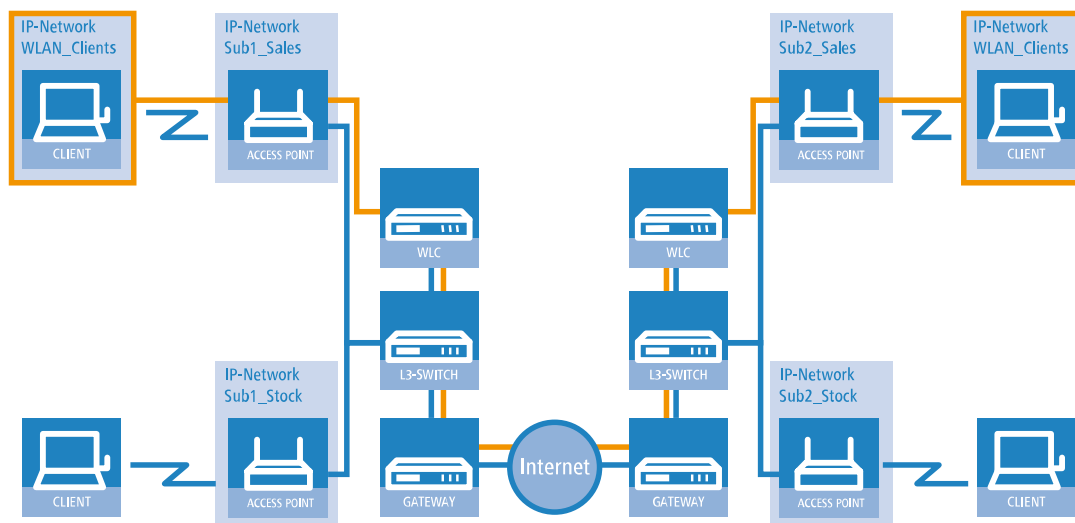


Figure 1: Overlay network across multiple IP networks

Using the data channel even allows you to span logical overlay networks across multiple WLCs.

Several WLCs within a single broadcast domain can support the same overlay network. Disable the WLC data channel between these WLCs (WEBconfig: LCOS Menu Tree > Setup > WLAN-Management > WLC-Cluster > WLC-Data-Tunnel-active). Otherwise the multiple reception of the broadcast messages would give rise to loops. Since routers drop broadcast messages, you can activate the CAPWAP data channel for WLCs in separate networks.

The APs use virtual WLC interfaces (WLC tunnels) to manage each SSID's data channels between AP and WLC. Depending on the model, each WLC provides 16 to 32 WLC tunnels that you can use when configuring the logical WLANs.

! Virtual WLC interfaces are available for selection in all dialogs used to select logical interfaces (LAN or WLAN), such as in the port table of the LAN and VLAN settings or for the definition of IP networks.

Tutorials

The following sections present specific scenarios with step-by-step instructions for a number of standard situations when operating WLCs.

Overlay network: Separating networks for access points without using VLAN

In many cases, networks in a shared physical infrastructure are separated by using VLANs. However, this method assumes that the switches operated in the network are VLAN-capable and that these are configured for VLAN operations. Consequently, the administrator has to rollout the VLAN configuration for the whole network.

WLCs enable you to separate the networks while minimizing the use of VLANs. The APs use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the WLC, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the WLC and a single, central switch. All of the other switches in this example work without a VLAN configuration.

! With this configuration, you reduce the VLAN to the core of the network structure (illustrated with a blue background). What's more, only 3 of the switch ports in use require a VLAN configuration.

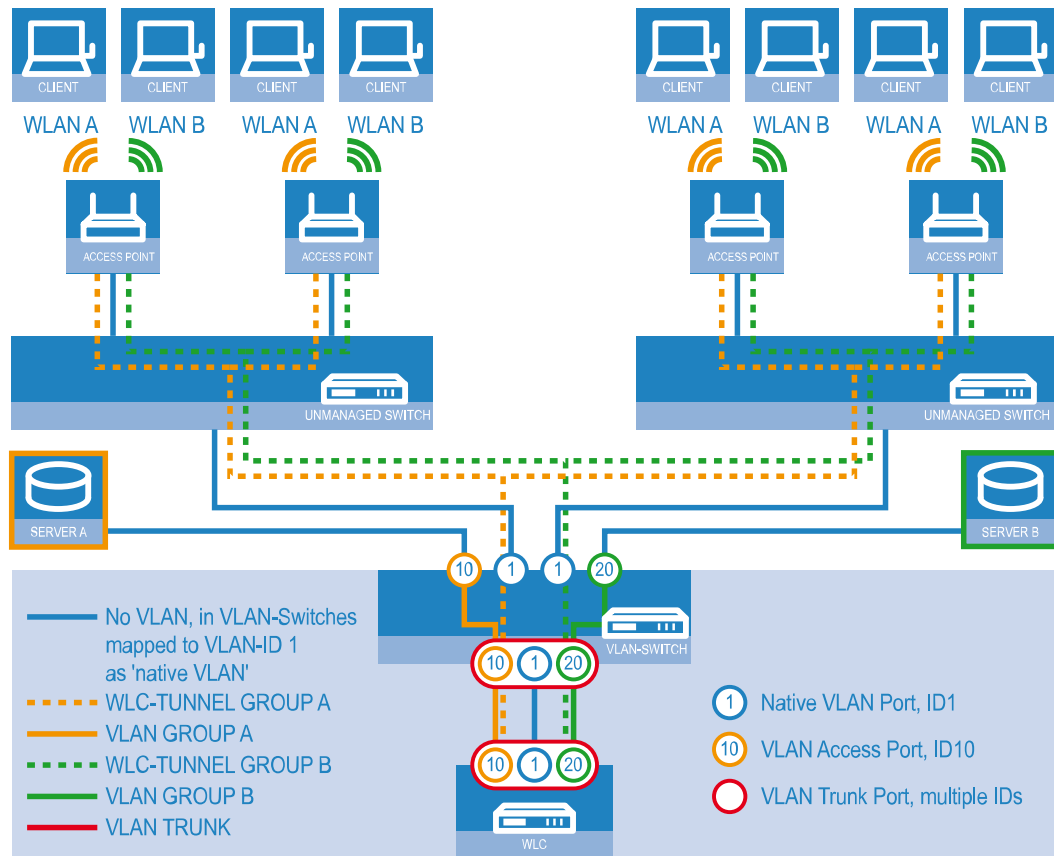


Figure 2: Example application: Overlay network

The diagram shows a sample application with the following components:

- > The network consists of two segments, each with its own (not necessarily VLAN-capable) switch.
- > Each segment contains several APs, each of which is connected to one of the switches.
- > Each AP provides two SSIDs for the WLAN clients in two different user groups, shown in the diagram in green and orange.
- > Each user group has access to its own dedicated server that is separated from other user group. The servers can only be accessed via the corresponding VLANs, i.e. through the access ports configured on the switch.
- > A single WLC manages all of the APs in the network
- > A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLC.

The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which AP is being used and regardless of the segment in which the client is located.

! The following description assumes a working basic configuration of the WLC. The configuration of the VLAN switch is not part of this description.

Configuring the WLAN settings

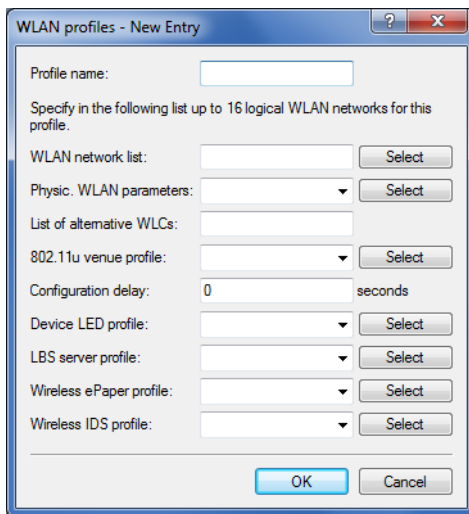
1. For each SSID, create an entry in the list of logical networks, each with a suitable name and the corresponding SSID. Connect the SSID to a WLC tunnel, for example the first SSID to "WLC-TUNNEL-1" and the second to "WLC-TUNNEL-2". Set the VLAN mode to 'tagged', set the VLAN ID '10' for the first logical network and the VLAN ID '20' for the

second logical network. In LANconfig you find these settings under **Configuration > WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**.

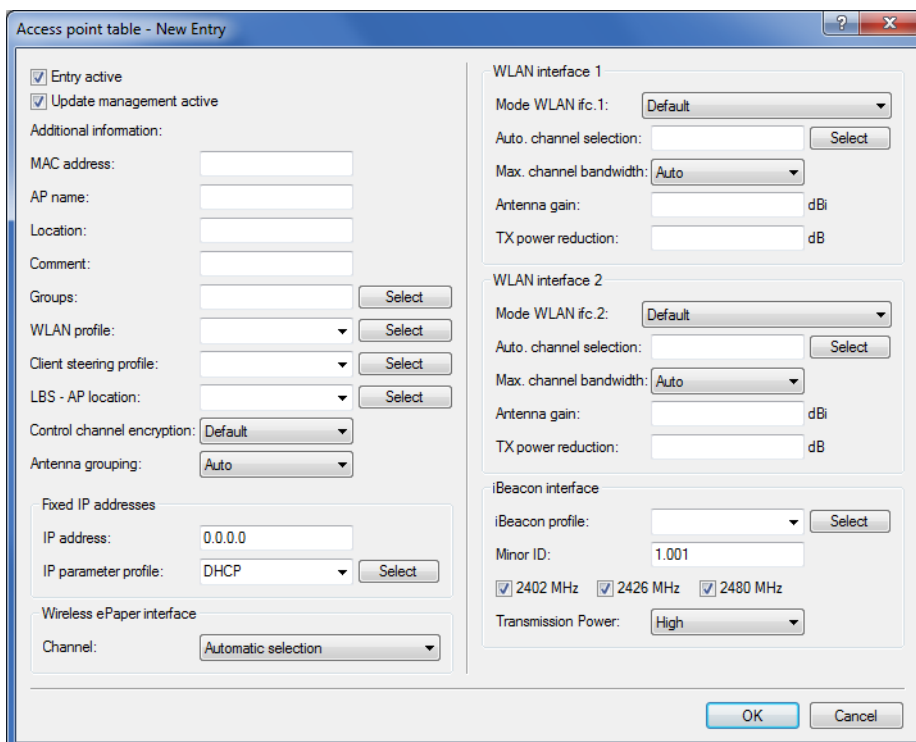
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. For this profile in the physical WLAN parameters, enable the option to turn on the VLAN module on the APs. Set the operating mode for the management VLAN in the APs to 'Untagged'. In LANconfig you find this setting under **Configuration > WLAN Controller > Profiles > Physical WLAN parameters**.

1 WLAN management

3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration > WLAN Controller > Profiles > WLAN profiles**.

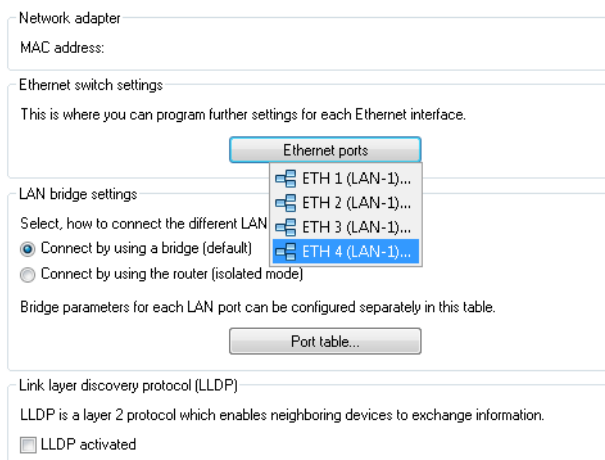


4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find these settings under **Configuration > WLAN Controller > AP config. > Access point table**.

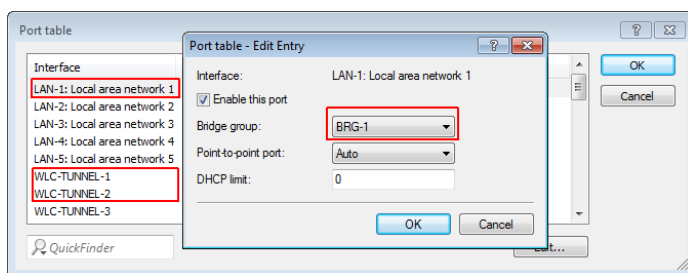


Configuring the interfaces on the WLC

- Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Make sure that the other Ethernet ports are not assigned to the same LAN interface. In LANconfig you find these settings under **Configuration > Interfaces > LAN > Ethernet ports**.



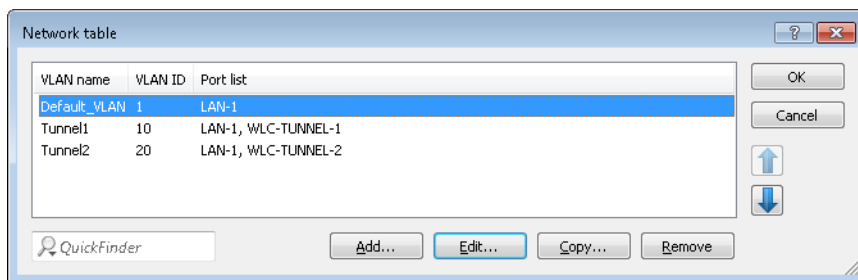
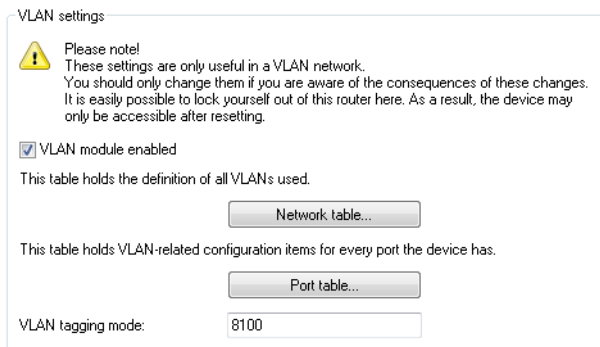
- Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find this setting under **Configuration > Interfaces > LAN > Port table**.



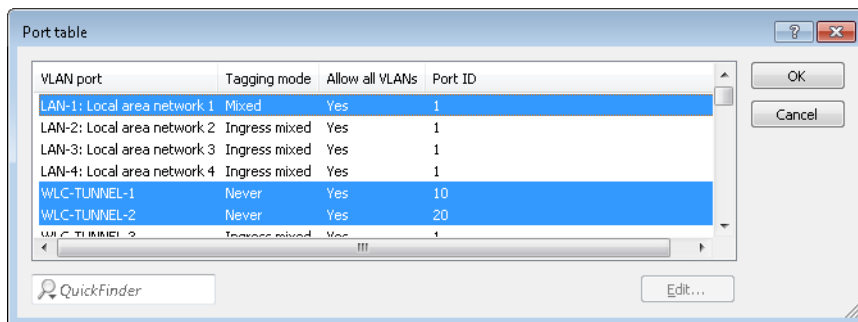
! By default, the LAN interfaces and WLC tunnels do not belong to a bridge group. By assigning the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-Tunnel-1' and 'WLC-Tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

1 WLAN management

7. Activate the VLAN module of the WLC under **Interfaces > VLAN** and, under **VLAN table**, assign the LAN port you selected above (LAN 1) and also the corresponding WLC tunnel to the desired VLAN.



8. Under **Interfaces > VLAN > Port table**, set the Tagging mode of the tunnel interface and the LAN interface, and set the corresponding port VLAN ID.



Depending on how the switch is configured, set the Tagging mode of the LAN interface to 'Mixed' or 'Always'.

In most cases the tunnel interfaces are operated with the mode 'Never', because packets here (from the WLAN) always arrive untagged and the WLC marks them with the port VLAN ID

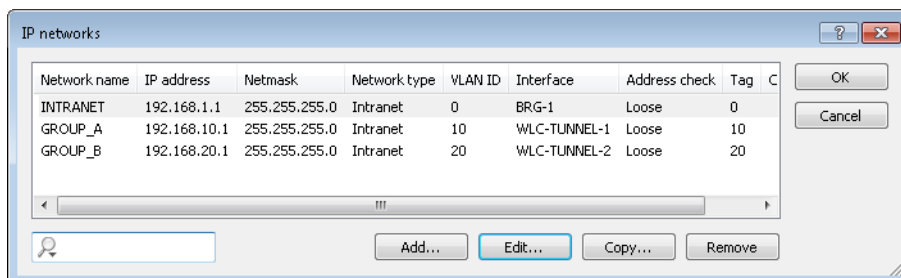
! When you activate the VLAN module, please observe that the ARF networks configured on the WLC must be given a VLAN ID. In the VLAN configuration outlined above, you need to set the VLAN ID for the IP network to '1' in order for the WLC to reach the network without a VLAN tag.

i A similar configuration is achieved by making the access point set a VLAN tag for packets that are to be sent via the tunnel, in which case the VLAN module of the WLC is not used.

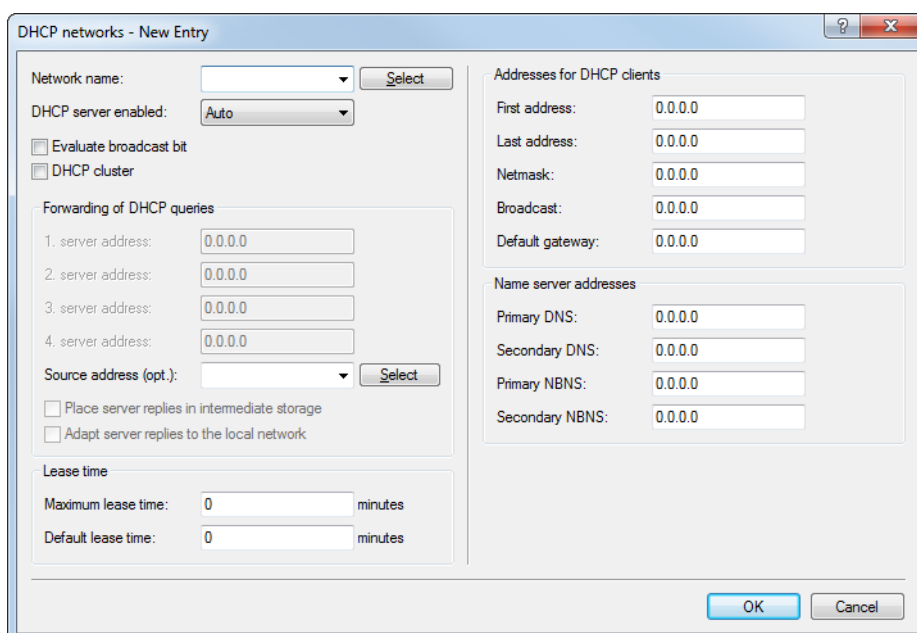
However, this bridging of the various WLC tunnels with one another causes broadcasts to be redirected into all of the tunnels; with a certain number of tunnels/SSIDs and APs, this can lead to load problems on the network and on the WLC. The VLAN module configuration presented here prevents this.

9. In addition you configure the IP settings for the networks that are separated on layer 2 under **IPv4 > General > IP networks**.

! To prevent the device from connecting these networks via layer 3, a separation must also be configured on layer 3, for example by using a port tag or by means of the firewall.



10. The WLC optionally acts as a DHCP server for the APs. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **IPv4 > DHCPv4 > DHCP networks**.



"Layer 3 roaming"

Allowing payload data from the wireless LAN to pass-through the WLC tunnel to the WLC enables roaming even beyond the limits of broadcast domains. In this example application, a layer-3 switch between the floors prevents the transmission of broadcasts, and thus separates the broadcast domains.

1 WLAN management

In this example, two user groups A and B each have access to their own WLAN (SSID). On all floors of the building, the APs provide two SSIDs, 'GROUP_A' and 'GROUP_B'.

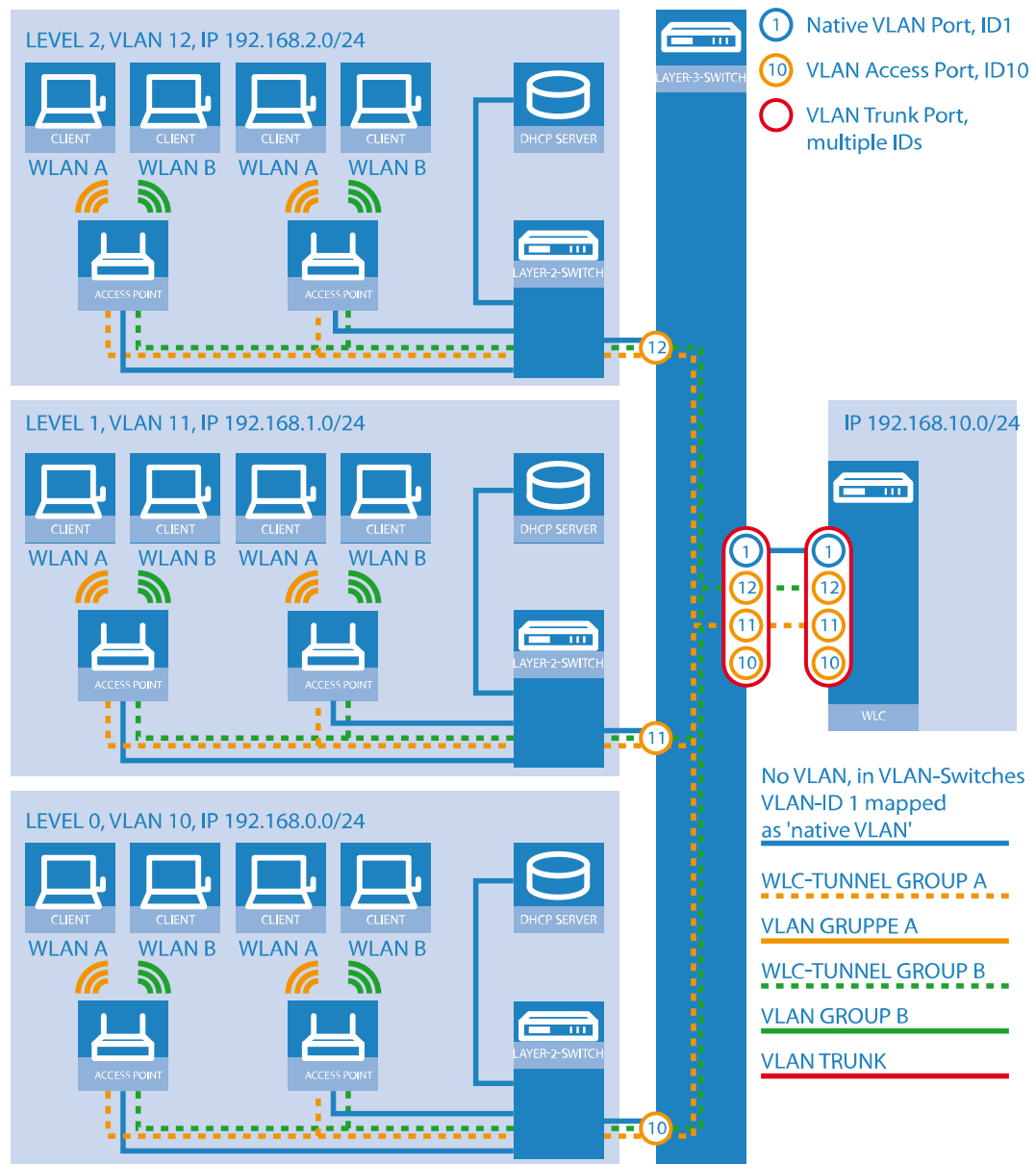


Figure 3: Example application for layer-3 roaming

The diagram shows a sample application with the following components:

- > The network consists of three segments on separate floors of a building.
- > A central layer-3 switch connects the segments and divides the network into three broadcast domains.
- > Each segment uses its own IP address space and its own VLAN.
- > Each segment operates a local DHCP server, which transmits the following information to the APs:
 - > IP address of the gateway
 - > IP address of the DNS server
 - > Domain suffix

! This information enables the APs to contact the WLC in another broadcast domain.

The aim of the configuration: When moving to another floor, a WLAN client that associates with a particular SSID is to retain access to its "own" WLAN, regardless of which AP is being used and regardless of the segment in which the client is located. Since the segments in this example use different IP address ranges, this scenario can only be implemented by managing the APs directly with the central WLC via layer 3 and across the boundaries of the VLANs.

! The configuration corresponds to the example *Overlay network: Separating networks for access points without using VLAN* on page 55.

WLAN controller with Public Spot

This scenario is based on the first scenario (overlay network) and enhances it to include specific settings for user authentication.

The configuration of a Public Spot can be greatly simplified if the payload data sent from the WLAN to the WLC is routed through a WLC tunnel. A Public Spot can, for example, provide guests with Internet access in parallel with, but separated from, an internal wireless LAN.

In this example, the employees of a company have access to a private WLAN (SSID), while the guests use a Public Spot to access the Internet. In all areas of the building, the APs provide two SSIDs, 'COMPANY' and 'GUESTS'.

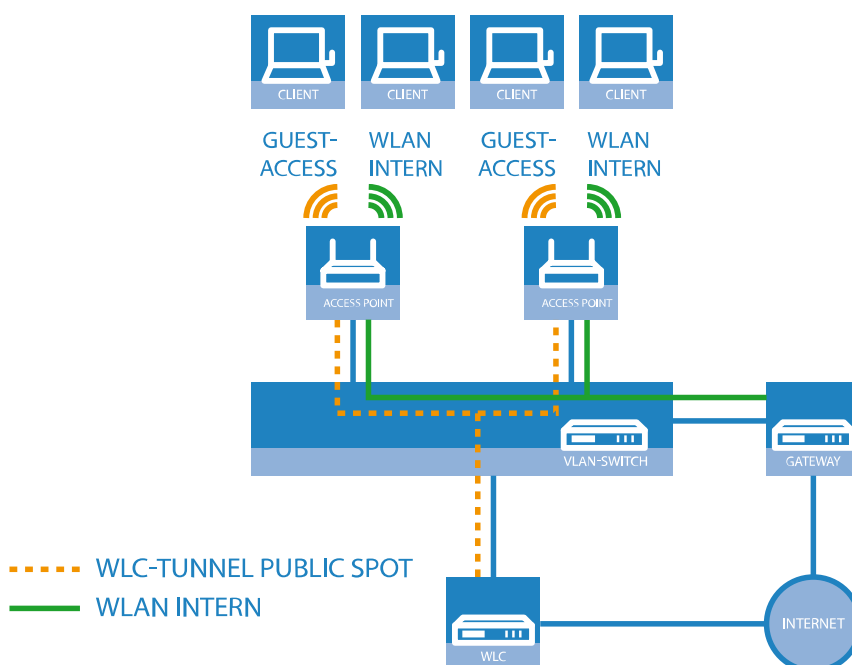


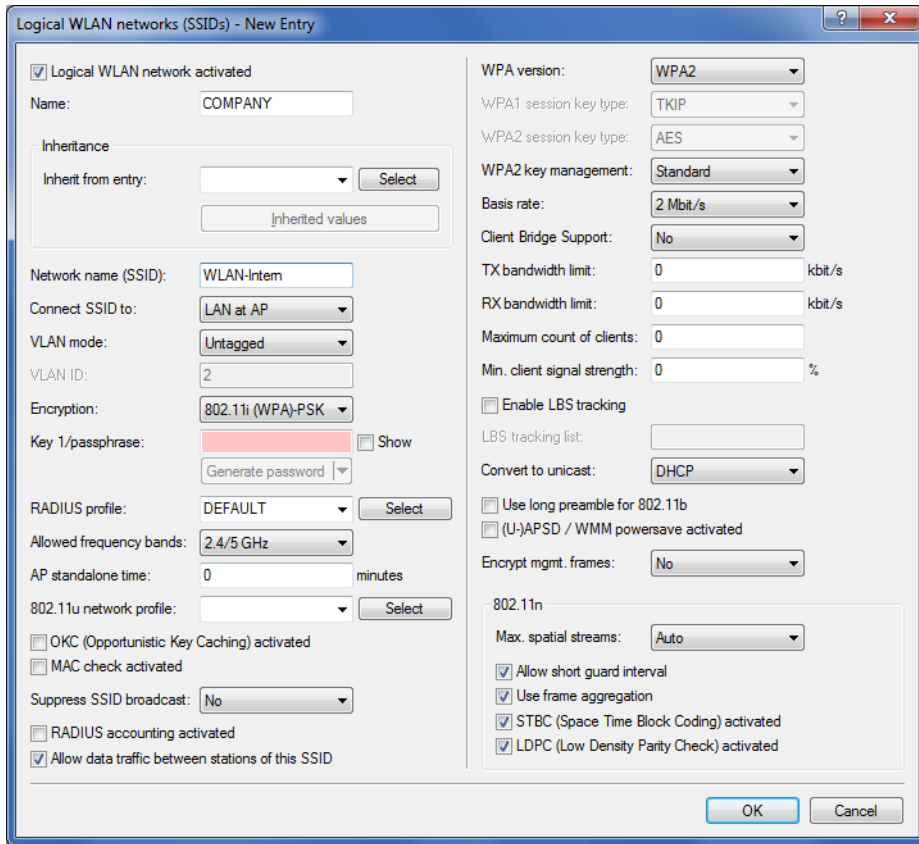
Figure 4: Example application: WLAN controller with Public Spot

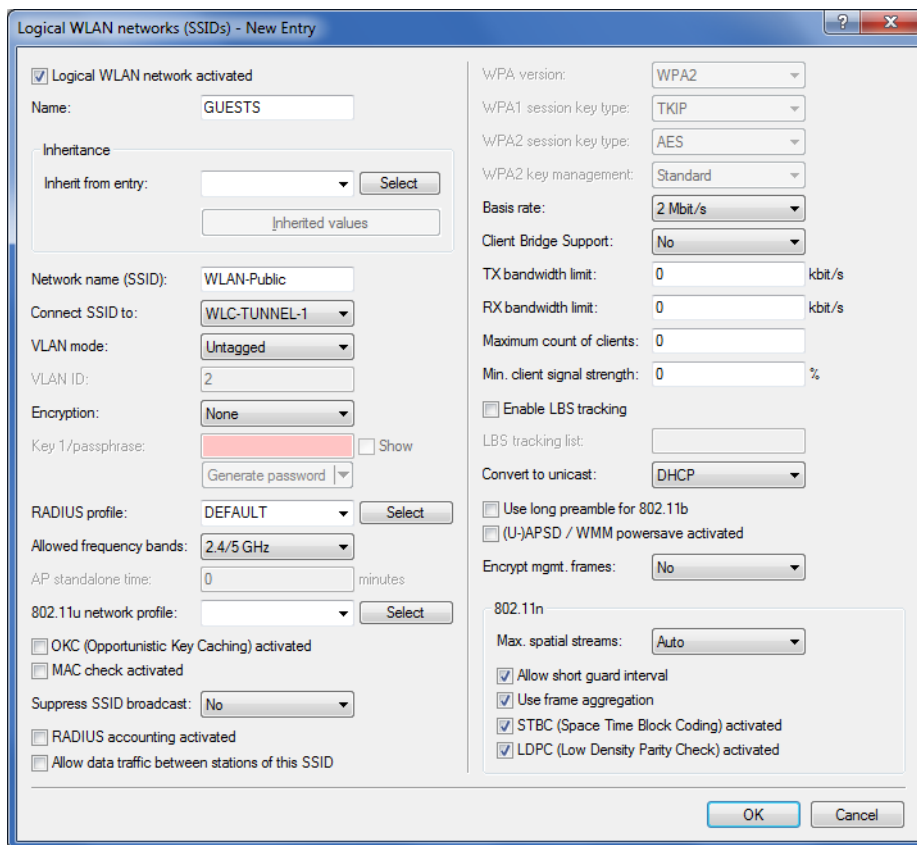
The aim of the configuration: A WLAN client that associates with the internal SSID should have access to all internal resources and the Internet via the central gateway. The APs break-out the payload data from the internal clients locally and pass it on directly to the LAN. The guests' WLAN clients associate with the Public Spot. The APs send the payload data from the guest clients through a WLC tunnel directly to the WLC, which uses a separate WAN interface for Internet access.

1. The internal WLAN and the guest WLAN each require an entry to be created in the list of logical networks, each with a suitable name and the corresponding SSID. Link the SSID for internal use with the 'LAN at AP', and the SSID for guests with (for example) 'WLC-TUNNEL-1'. Disable encryption for the guest network SSID so that the guests' WLAN

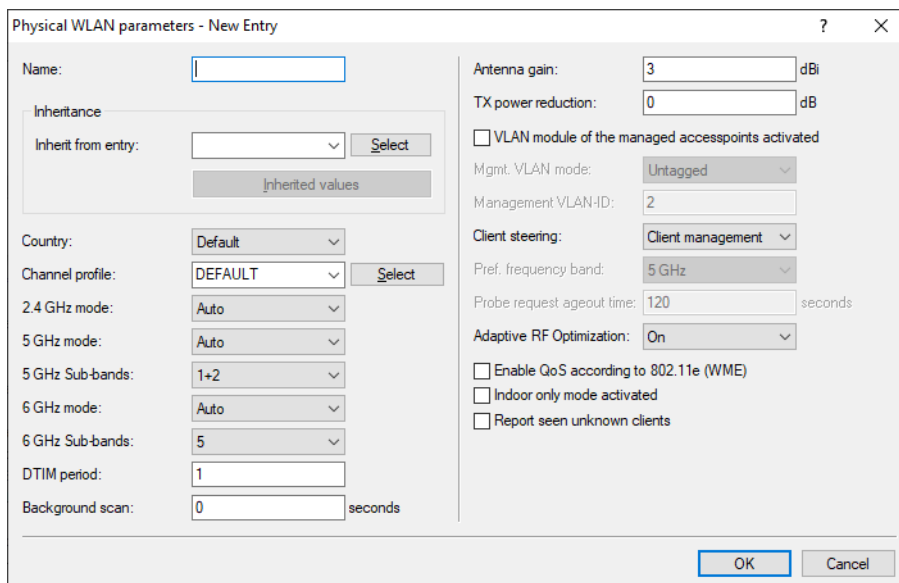
1 WLAN management

clients can associate with the Public Spot. You should also prevent inter-station traffic for this SSID. In LANconfig you find this setting under **Configuration > WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**.



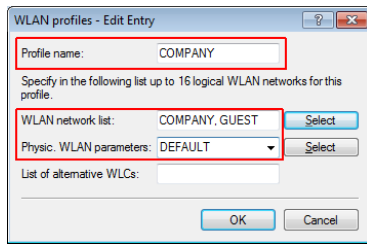


2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. In LANconfig you find this setting under **Configuration > WLAN Controller > Profiles > Physical WLAN parameters**.

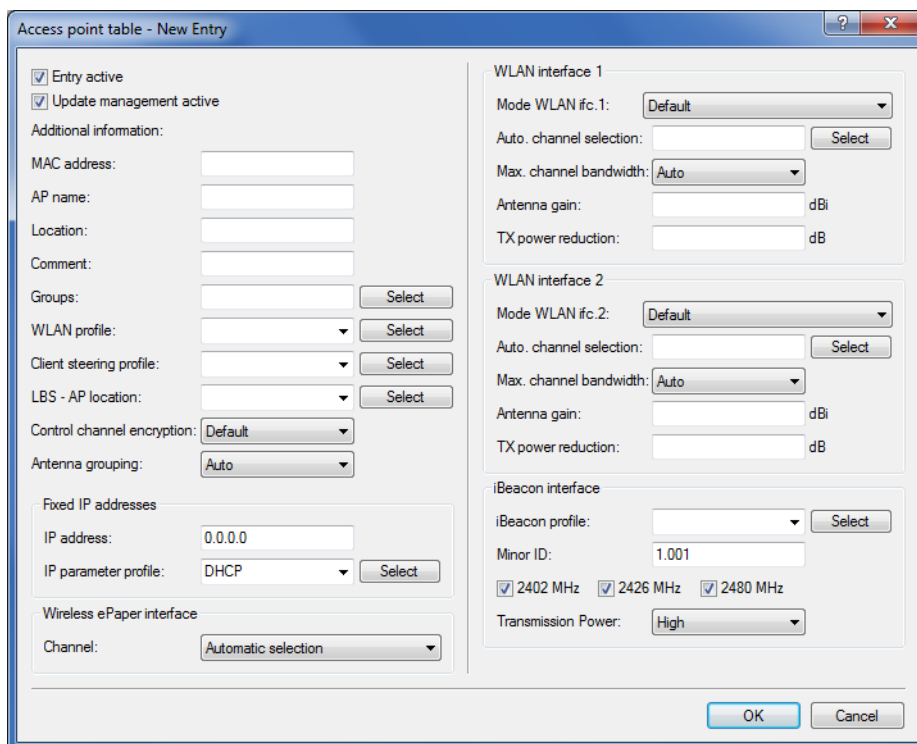


1 WLAN management

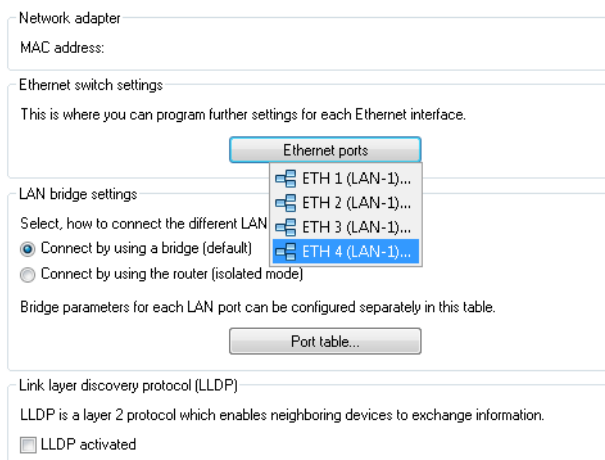
3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration > WLAN Controller > Profiles > WLAN profiles**.



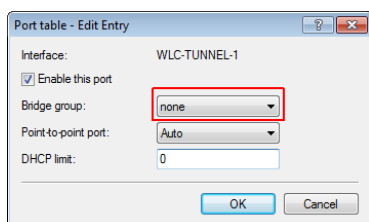
4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find this setting under **Configuration > WLAN Controller > AP config. > Access point table**.



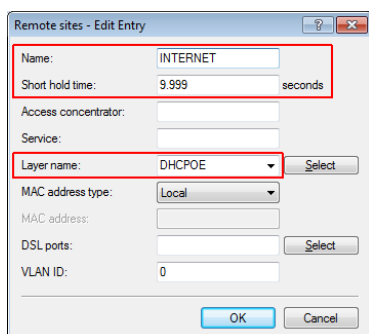
- Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical LAN interface 'DSL-1'. The WLC then uses this LAN interface for the guest network Internet access. In LANconfig you find this setting under **Configuration > Interfaces > LAN > Ethernet ports**.



- Verify that the logical LAN interface 'WLC-tunnel-1' is not allocated to a bridge group. This ensures that the other LAN interfaces do not transmit any data to the Public Spot. In LANconfig you find this setting under **Configuration > Interfaces > LAN > Port table**.



- For the guest Internet access, create an entry in the list of DSL remote sites with the hold time '9999' and the pre-defined layer 'DHCPOE'. This example assumes that Internet access is provided by a router with DHCP server. In LANconfig you find this setting under **Configuration > Communications > Remote sites > Remote sites**.



- For internal users, create the IP network 'INTRANET' with (for example) the IP address '192.168.1.100' and the interface tag '1'. For the guest access, create the IP network 'GUEST-ACCESS' with (for example) the IP address of

1 WLAN management

'192.168.200.1' and the interface tag '2'. The virtual router in the WLC uses the interface tags to separate the routes for the two networks. In LANconfig you find this setting under **Configuration > TCP/IP > General > IP networks**.

The screenshot shows the 'IP networks - Edit Entry' dialog box. The following fields are highlighted with red boxes: 'Network name' (INTRANET), 'IP address' (192.168.1.100), and 'Interface tag' (1). Other fields include Netmask (255.255.255.0), Network type (Intranet), VLAN ID (0), Interface assignment (Any), Address check (Loose), and Comment.

The screenshot shows the 'IP networks - Edit Entry' dialog box. The following fields are highlighted with red boxes: 'Network name' (GUEST), 'IP address' (192.168.200.1), and 'Interface tag' (2). Other fields include Netmask (255.255.255.0), Network type (Intranet), VLAN ID (0), Interface assignment (Any), Address check (Loose), and Comment.

- The WLC is able to act as a DHCP server for APs and the associated WLAN clients. To set this up, activate the DHCP server for the 'INTRANET' and the 'GUEST-ACCESS'. In LANconfig you find this setting under **Configuration > TCP/IP > DHCP > DHCP networks**.

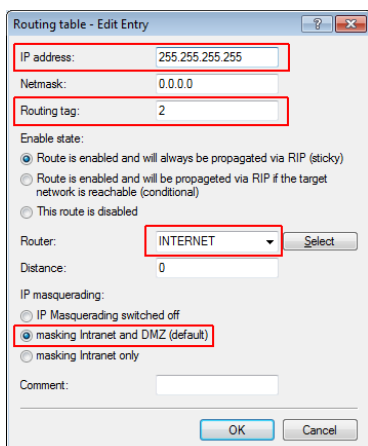
! Activation of the DHCP server is obligatory for the guest network and optional for the internal network. There are other ways of realizing a DHCP server for the internal network.

The screenshot shows the 'DHCP networks - New Entry' dialog box. It is divided into several sections:

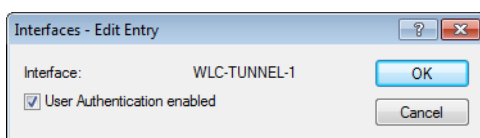
- Network name:** A dropdown menu with a 'Select' button.
- DHCP server enabled:** A dropdown menu set to 'Auto'.
- Options:** Checkboxes for 'Evaluate broadcast bit' and 'DHCP cluster'.
- Forwarding of DHCP queries:** Four input fields for server addresses (all set to 0.0.0.0) and a 'Source address (opt.)' dropdown with a 'Select' button. Below are checkboxes for 'Place server replies in intermediate storage' and 'Adapt server replies to the local network'.
- Lease time:** Input fields for 'Maximum lease time' and 'Default lease time', both set to 0 minutes.
- Addresses for DHCP clients:** Input fields for 'First address', 'Last address', 'Netmask', 'Broadcast', and 'Default gateway', all set to 0.0.0.0.
- Name server addresses:** Input fields for 'Primary DNS', 'Secondary DNS', 'Primary NBNS', and 'Secondary NBNS', all set to 0.0.0.0.

 The dialog box has 'OK' and 'Cancel' buttons at the bottom right.

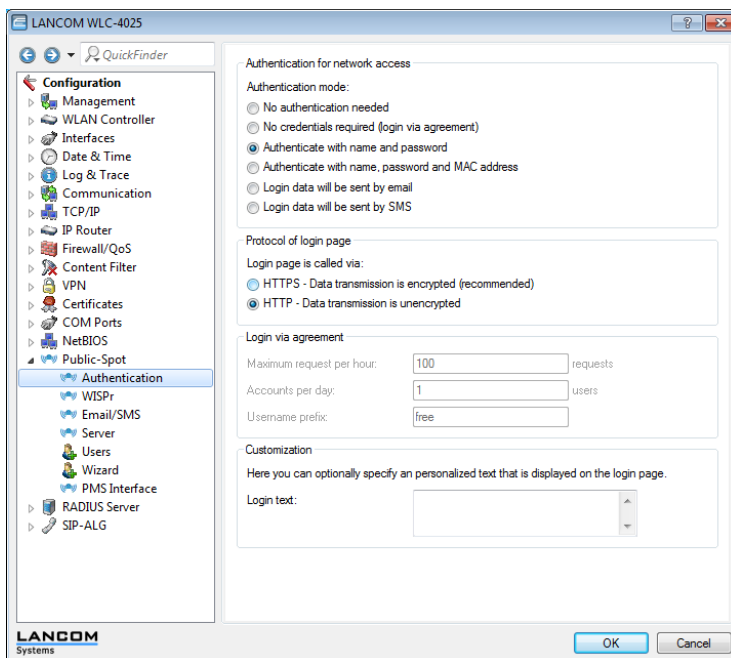
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLC. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under **Configuration > IP router > Routing > Routing table**.



11. Activate the Public Spot user authentication for the logical LAN interface 'WLC-Tunnel-1'. In LANconfig you find this setting under **Configuration > Public Spot > Server > Operational settings > Interfaces**.



12. The final step is to enable authentication via the Public Spot for the WLC. In LANconfig you find this setting under **Configuration > Public Spot > Authentication**.



In addition to configuring the WLC, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

1.4.4 IP-dependent auto configuration and tagging of APs


The easiest way to manage all of the APs that you add to a managed network is to use a flat hierarchy. However, in the largest installations with hundreds of APs across several locations, this type of organization quickly becomes confusing and creates a high level of administrative effort. Setting up **Assignment groups** can help to simplify the management of distributed APs. The WLC can automatically to configure each new AP based on the IP addresses it receives. Manual assignment of an IP parameter profile, a WLAN profile and a Client-steering profile by an administrator is no longer required.

The following describes how an assignment group is used when an unassociated AP registers with a central WLC: After the new APs are installed on site (e.g. at a company or branch network), they try to establish a connection to the specified WLC and obtain a configuration via CAPWAP. The WLC detects the connection requests and, for each new AP, it checks the AP table for a suitable AP profile (e.g., the default profile) and/or whether a suitable assignment group has been defined. If one or more configuration options are available, the WLC checks them for the following states:

1. For a new AP there is an assignment group but no AP profile. In this case, the WLC assigns the profile specified in the assignment group to the new AP.
2. For a new AP there is both an assignment group as well as an AP profile. In this case, the WLC ignores the assignment group and assigns the profile defined in the AP profile to the new AP.
3. For a new AP, there is an AP profile but no assignment group. The behavior is the same as point (2).

If a new AP has neither an AP profile nor an assignment group, the WLC issues an alarm to notify the administrator of the incorrect configuration.

After successful group assignment, the WLC automatically creates an AP profile for every new AP in the access point table. In the **Groups** field, the WLC references the assignment group used when it added the new AP.

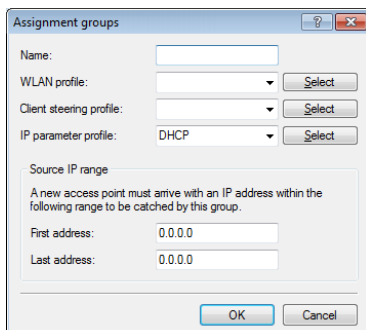
 An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups overlap, LCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status > WLAN-Management > AP-Configuration**.

The group field also gives you the the option of assigning individually definable tags to an AP. For example, these **Tag groups** can be used to act as filter criteria in order for the WLC to restrict the actions it performs to a selection of APs.

Setting up assignment groups for IP-dependent auto configuration

The following tutorial shows you how you setup assignment groups on a WLC for the IP-dependent automatic configuration of new APs.

1. Open the configuration dialog for your device and select **WLAN controller > AP configuration > Assignment groups**
2. Click on **Add** to create a new group.



3. Enter under **Name** a unique descriptor for the assignment group, for example, `Berlin_branch`.
4. Select the **WLAN profile** that the WLC automatically assigns to a new AP if the IP address of the new AP is within the source IP range.

5. Enter the **IP parameter profile** if the new AP should receive a manual network configuration. Otherwise, leave the value as **DHCP**, whereby the AP automatically gets a network configuration from the DHCP server. The DHCP server must be configured to do this.

If you wish to assign a manual network configuration in which a new AP receives a different IP address, you specify the corresponding address range in the **IP parameter profile** under **Address assignment pool**.

6. **Optional:** Specify a **Client-steering profile** in order to forward future WLAN clients to the ideal AP in case there are several new APs within transmission range.

! If you activate client steering, this must be activated for every AP in the managed infrastructure. Refer to section [Client steering by WLC](#) on page 106 for further information on this.

7. Enter the start and end of the **Source IP range** relevant to the assignment group.
A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.
8. Close all dialog windows with **OK** and save the configuration to your device.

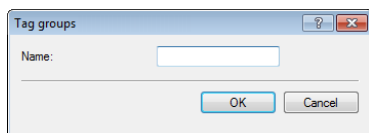
From now on, the WLC assigns the profiles referenced in the assignment groups to all new APs. The LCOS console can now provide you with information about the categorization, see [Overview of CAPWAP parameters with the show command](#) on page 126.

! Please ensure that the access point table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.

Setting up tag groups for the detailed selection of APs

The following tutorial shows you how a tag group can be added to an AP configuration on a WLC. To do this, you first create a tag group and then assign it to a WLAN profile.

1. Open the configuration dialog for your device and select **WLAN controller > AP configuration > Tag groups**
2. Click on **Add** to create a new group.



3. Under **Name** you enter the new tag and save the entry with **OK**.
4. Navigate to the dialog with **WLAN controller > AP configuration > Access point table**.
5. Select an existing AP profile with **Edit** or add a new one, if necessary.
6. Under **Groups** select the tag group(s) created earlier.
Multiple tag groups can be specified in a comma-separated list.

i The tag groups are independent of the assignment groups, the assignment of which is specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. The manual allocation of an assignment group has no effect on the AP configuration, which is in line with the state check described under [IP-dependent auto configuration and tagging of APs](#) on page 70. The only effects are on the filtering in the command `show capwap group` at the console

! The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

7. Close all dialog windows with **OK** and save the configuration to your device.

From now on the WLC gives the tags in the edited WLAN profile to those APs that received it.

1.5 Access point administration

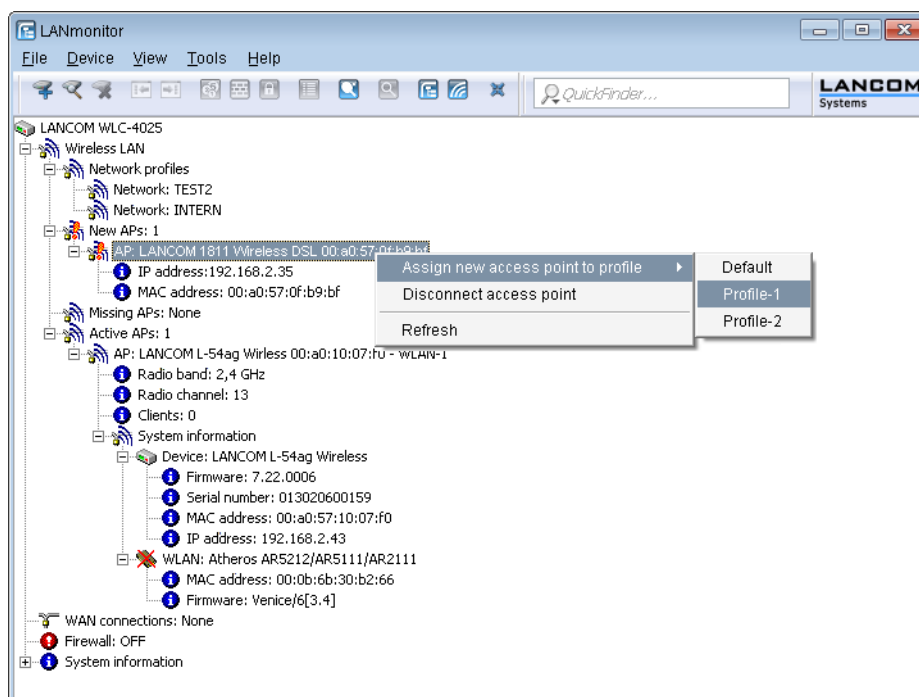
1.5.1 Accepting new access points into the WLAN infrastructure manually

If you prefer not to accept APs into the WLAN infrastructure automatically, you can also manually accept APs.

Using LANmonitor to accept access points

It is very easy to accept new APs with LANmonitor. A configuration is selected that will be assigned to the AP after transmission of a new certificate.

In LANmonitor, click on the new AP with the right-hand mouse key. From the context menu that pops up, you select the configuration which is to be assigned to the device.



! Assignment of the configuration causes the AP to be entered into the AP table in the WLC. It takes a few seconds for the WLC to assign a certificate to the AP and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted AP is briefly signaled as a "Lost AP" by the red Lost AP LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

Accepting access points via WEBconfig with provision of a certificate

New APs that do not have a valid certificate but do have an entry in the AP table can be manually accepted with WEBconfig.

1. Open the WLC configuration with WEBconfig.
2. Under **Extras > LCOS menu tree > Setup > WLAN-Management** select the action **Accept AP**.

- When requested for additional arguments, enter the MAC address of the AP to be accepted and confirm with **Execute**.

Accept-AP

Enter here any additional arguments for the command you are about to execute:

Arguments|00a005711111

Accepting access points via WEBconfig with provision of a certificate and configuration

New APs that do not have a valid certificate and do not have an entry in the AP table can be manually accepted by means of a wizard in WEBconfig. A configuration is selected that will be assigned to the AP after transmission of a new certificate.

- Open the WLC configuration with WEBconfig. Click on **Setup Wizards** and select the wizard **Assign access points to profiles**.

Setup Wizards **LANCOM**
Systems
... connecting your business

[Logout](#)

Please choose the desired wizard:

- [Set up Internet connection](#)
- [Selection of Internet Provider](#)
- [Connect Two Local Area Networks](#)
- **[Assign Access Points to Profiles](#)**
- [Check Security Settings](#)
- [Basic Settings](#)
- [Rollout](#)
- [Manage Public Spot Account](#)
- [Create Public Spot Account](#)

- Click on the link to start the wizard. Select the desired AP by means of its MAC address and choose the WLAN configuration that is to be assigned to it.

192.168.2.34 - Assign Access Points to Profiles **LANCOM**
Systems
... connecting your business

Step 3 of 4

Select the profile the new access point shall be assigned to:

Profile

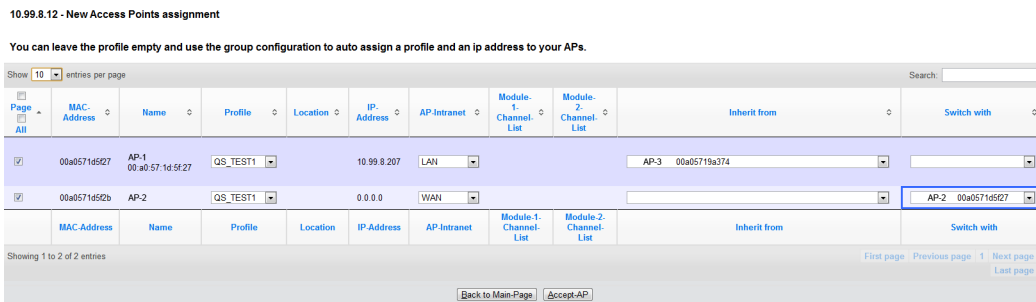
Previous Page Apply Reset Terminate this Wizard

- ! Assignment of the configuration causes the AP to be entered into the AP table in the WLAN controller. It takes a few seconds for the WLC to assign a certificate to the AP and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted AP is briefly signaled as a "Lost AP" by the red "Lost AP" LED, in the device's display, and in LANmonitor until assignment of the certificate is completed.

Adding new APs with the WEBconfig Setup Wizard

As of LCOS 9.00, WLCs have a revised Setup Wizard **Assign Access Points to Profiles**, which makes it easier to add new APs via WEBconfig. Just a few mouse clicks with the new Setup Wizard allows you to

- > Make a targeted search for a new AP;
- > Accept one or more new APs at the same time;
- > Assign a WLAN profile or a channel list to a new AP;
- > Allow a new AP to inherit the configuration from an accepted AP;
- > To exchange the configuration in a new AP for that of an accepted missing AP. When exchanging a configuration, the new AP receives the complete configuration of the accepted missing AP (except for its MAC address). When the new AP has been integrated, the WLC then deletes the configuration of the accepted missing AP.



Click **Accept AP** to include the new AP with its new settings into the network.

! If you have allowed an AP to be configured via assignment groups, there is no need for any further settings for this AP in the Setup Wizard. The WLC automatically assigns the settings for the appropriate groups to the AP.

1.5.2 Manually removing access points from the WLAN infrastructure

The following actions are required to remove an AP under management of the WLC from the WLAN infrastructure:

1. In the AP, switch the WLAN operating mode of the WLAN module from 'Managed' to 'Client' or 'Access Point'.
2. In the WLAN controller, delete the configuration for the AP and/or deactivate **Automatically provide APs with a default configuration** via **Extras > LCOS menu tree > Setup > WLAN-Management > Autoaccept-AP**.
3. Disconnect the AP in WEBconfig by selecting **Extras > LCOS menu tree > Setup > WLAN-Management** and the action **Disconnect AP**, or alternatively in LANmonitor.
4. When requested for additional arguments, enter the MAC address of the AP to be disconnected and confirm with **Execute**.

Disconnect-AP

Enter here any additional arguments for the command you are about to execute:


Arguments

1.5.3 Deactivating access points or permanently removing them from the WLAN infrastructure

Occasionally it is necessary to temporarily deactivate or even permanently remove a WLC-managed AP.

Deactivating an access point

To deactivate an AP, set its corresponding entry in the AP table to 'inactive' or delete the entry from the table. In the AP, the WLAN modules in managed mode are switched off and the corresponding SSIDs are deleted.

 The WLAN modules and the WLAN networks (SSIDs) are still switched off even if standalone operation is activated.

An AP deactivated in this way remains connected to the WLC and the certificates are retained. The WLC can reactivate the AP and its managed-mode WLAN modules at any time simply by activating the entry in the AP table or by making a new entry in the AP table along with the appropriate MAC address.

If the connection to a deactivated AP is broken (either unintentionally due to a failure or intentionally by the administrator) then the AP begins a new search for a suitable WLC. Although the former WLC can check the validity of the certificate, due to the fact that there is no (active) entry in the AP table the AP treats it as a secondary WLC. If the AP finds a primary WLC then it will register with it.

Permanently removing an access point from the WLAN infrastructure

In order to permanently remove an AP from a centrally managed WLAN infrastructure, the certificates in the SCEP client have to be either deleted or revoked.


- If you have access to the AP, the certificates are quickly deleted by resetting the device.
- If the device has been stolen and consequently needs to be removed from the WLAN infrastructure, then the certificates in the WLC's CA have to be revoked. This is done in WEBconfig by navigating to **Extras > LCOS menu tree > Status > Certificates > SCEP-CA > Certificates** and accessing the **Certificate status table**. Here you delete the certificate for the MAC address of the APs which are to be removed from the WLAN infrastructure. The certificates are not actually deleted, but they are marked as expired.

 In case of a backup solution featuring redundant WLCs, the certificates have to be revoked in all of the WLCs!

1.6 AutoWDS – wireless integration of APs via P2P connections

In a centrally managed WLAN network, access points (APs) are typically connected to the WLAN controller (WLC) via the LAN. The LAN connections simultaneously determine the topology of the managed network. Network extension by means of additional APs is restricted to the reach of the hard-wired network architecture and requires the extension of the corresponding infrastructure.

By means of **AutoWDS**, you have the option of extending a WLAN by means of point-to-point (P2P) connections for the cost-effective and fast installation of highly scalable networks. "AutoWDS" stands for "automatic wireless distribution system". This feature enables you to create a radio network from several APs, which are interconnected via wireless only: a logical connection is all you need. Potential applications include the seamless connection of smaller properties or even entire districts to the Internet, or the establishment of a company network where connections via LAN are impracticable.

 AutoWDS is not supported anymore as of LCOS 10.70. The functionality still remains intact in LANCOM devices (except in 18xx series routers) and therefore still can be used for existing installations. However LANCOM Systems will not provide any support regarding the configuration and troubleshooting of an AutoWDS scenario.

In the simplest case, all you need is a WLC connected via LAN to an AutoWDS-enabled AP. The AP supports the managed network and at the same time acts as an "anchor AP". Using this anchor AP, unassociated AutoWDS-enabled APs connect to the WLC, which transmits a configuration to them by means of CAPWAP. After obtaining the configuration and being incorporated into the managed WLAN, the individual APs use P2P links to forward user data, to communicate with one another, and to support the topology. Additional APs that join later are able to use the associated APs as their anchor APs. In this manner, several APs can be chained together to establish meshed networks, which can optionally feature

redundant connections via RSTP. From the perspective of an unassociated AP, associated APs are master APs. From the perspective of the master AP, unassociated APs are slave APs.

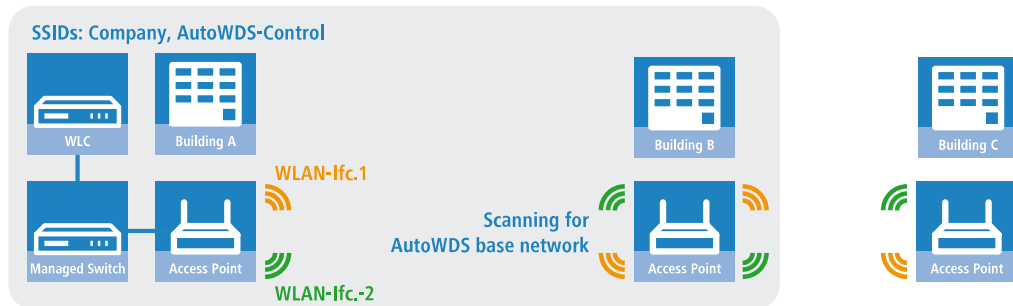


Figure 5: Phase 1 – unassociated AP in building B seeks AutoWDS base network and finds anchor AP in building A

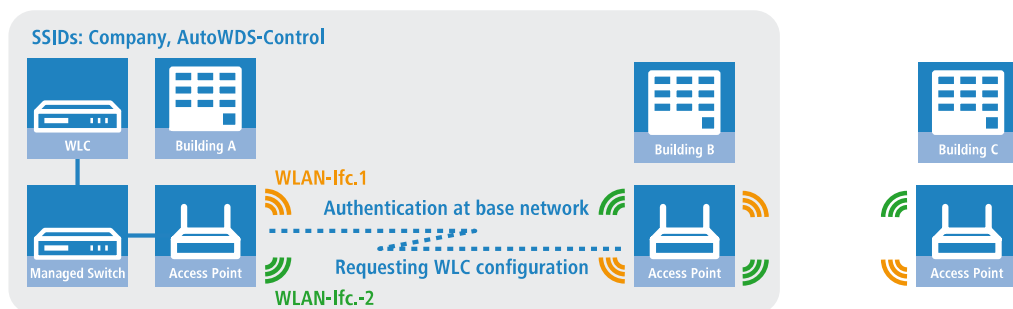


Figure 6: Phase 2 – unassociated AP in building B finds WLC and retrieves AP configuration via CAPWAP

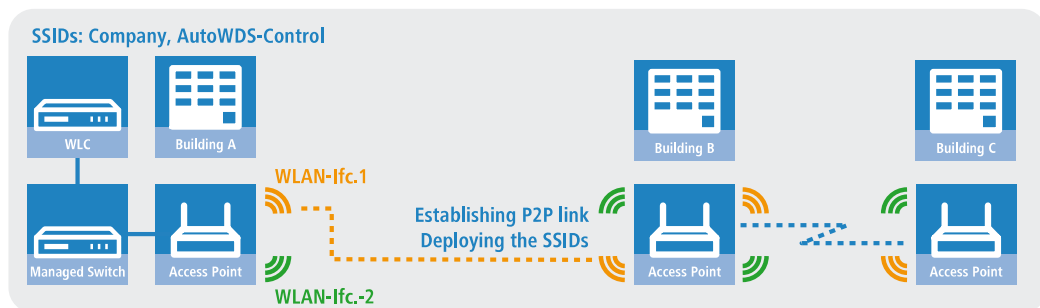


Figure 7: Phase 3 – unassociated AP in building B joins the managed WLAN. Unassociated AP in building C seeks AutoWDS base network and finds anchor AP in building B

Precise information about the integration process and the operating modes for topology management can be found in the following sections, which describe how AutoWDS functions.

- ! AutoWDS is suitable for static infrastructure only, not for mobile APs. If an AP should move out of range of its P2P partner and lose the connection to the network, there is a temporary downtime and a subsequent *reconfiguration*. However, the roaming of WLAN clients between individual AutoWDS APs is no different than the roaming between conventional APs.
- ! AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.
- ! The DFS processing by an AP in 5-GHz operation is unaffected by AutoWDS and has a higher priority. DFS radar recognition may cause the AP to suddenly change the channel during operation. It can even completely deactivate

the WLAN for a period if radar recognition is running on different channels and the available frequencies drop out. The impacted AP can cause interference to the entire AutoWDS group, and may not be able to deploy any SSIDs for some time. Within buildings you have the option of counteracting interference by enabling the indoor mode.



If you operate AutoWDS on a device with a single physical WLAN interface, its data rate will be reduced to just a third, since the device must send incoming/outgoing data multiple times: To the WLAN clients, to a master AP and, if applicable, to a slave AP. This effect is mitigated by operating only devices that have multiple WLAN physical interfaces and using these to divide up the data traffic. You do this by reserving one physical WLAN interface for connecting the APs and one physical WLAN interface for connecting the clients.

MultiHop on the same WLAN interface can be enabled in the AutoWDS profile configuration, if necessary. This is disabled by default due to the associated loss of performance.

1.6.1 Notes on operating AutoWDS

Owing to technical restrictions, the applications of AutoWDS are limited to certain specific application scenarios. Please carefully observe the general remarks in this chapter to avoid possible complications. The items listed here are intended to supplement the remarks elsewhere in the AutoWDS chapter, so some redundancies are possible.

- APs must switch channels when radar is detected (5-GHz band, outdoor and DFS). This can potentially lead to temporary interruptions to the WLAN due to necessary changes of channel.
- In general, we recommend a maximum of 3 hops for AutoWDS operations.
- When operating AutoWDS on one radio channel only, problems with multiple transfers and hidden stations can occur. For this reason we recommend the use of APs with two physical WLAN interfaces (dual radio) operating on separate radio channels.
- AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.



If you are operating DFS in combination with AutoWDS, you should set the continuation time for autonomous operation of the AutoWDS profile to at least 2 minutes. After the downtime of a P2P connection, this extra minute allows for the one-minute DFS scan, after which the CAPWAP layer restores the CAPWAP connection to the WLC via the P2P connection.



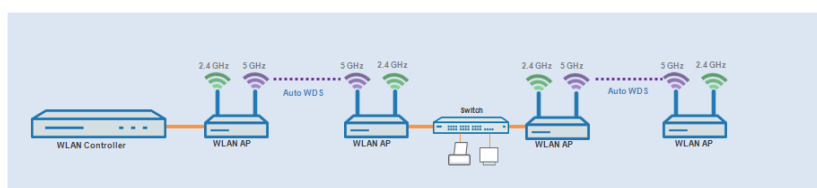
If possible, ensure that all APs on each physical WLAN interface (WLAN-1, WLAN-2) consistently use the same frequency band (2.4 GHz or 5 GHz) to exclude any potential problems with the automatic topology configuration.

The following is an overview of the **suitability of AutoWDS** for certain application scenarios.

Suitable:

Use of a **dedicated** physical WLAN interface for the P2P links.

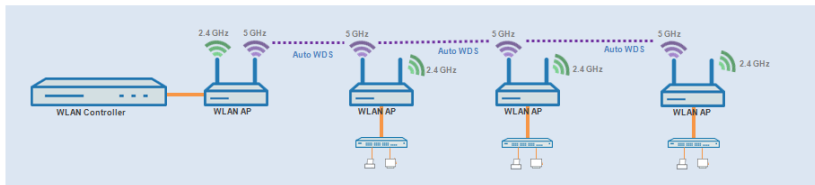
- Use of different channels for the P2P links (indoor)
- Use of AutoWDS with up to 3 hops



Partly suitable:

Use of single physical WLAN interface **simultaneously** for the AutoWDS uplink and downlink (repeater mode) where all P2P links operate on the same radio channel.

- > Use for operation without DFS (indoor)
- > Use of AutoWDS with up to 3 hops



Difficulties can arise from the hidden station problem or throughput loss due to multiple transmissions.

- > **Hidden station problem:** Over larger distances, widely separated APs on the same network may not be able to "see" each other. In this case, several APs could end up transmitting simultaneously to cause interference for the APs between them. These collisions lead to multiple transmissions and performance losses.

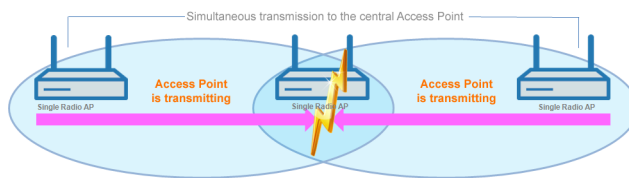


Figure 8: Simultaneous transmissions to the middle AP: The two outer APs are unaware of the collision.

- > **Throughput-loss due to multiple transmissions:** An AP transmitting data packets multiple times on the same channel leads to a reduction of the maximum available throughput (by half per hop).

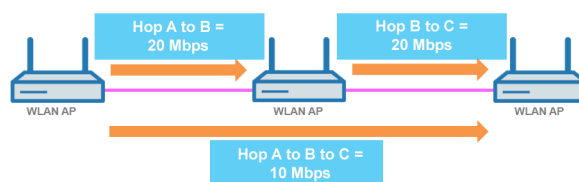
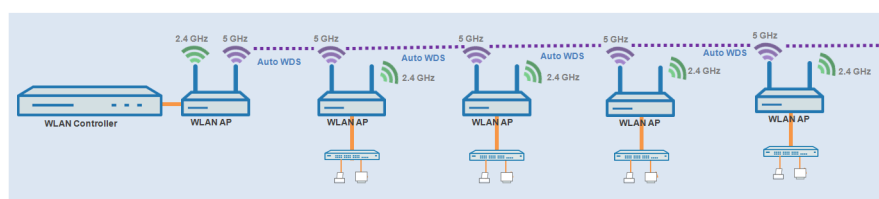


Figure 9: Transmission of data packets on every hop

Unsuitable:

Use of a physical WLAN interface **simultaneously** for AutoWDS uplink and downlink (repeater mode) during outdoor operations with more than one hop in the 5-GHz band.



In repeater mode, the physical WLAN interface has a dual role: In the direction of the WLC the interface operates as a master, while in the direction of neighboring APs it operates as a slave. For this purpose, all APs necessarily operate on the same radio channel. However, if the DFS feature detects signals, the APs are required to stop transmitting on the affected frequencies. This means that the APs cannot inform the WLC about the DFS event and the WLC cannot initiate a change of frequency for the network. As a result, the affected APs are potentially permanently separated from the network.

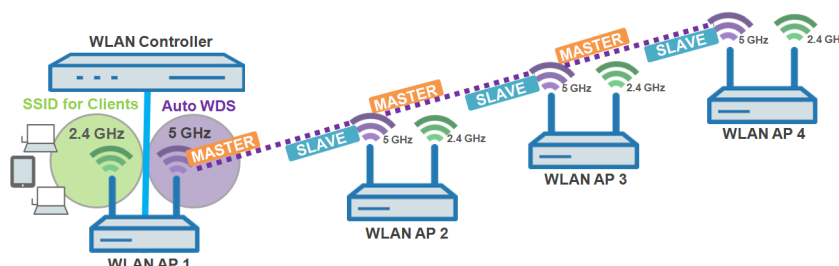


Figure 10: Connection lock after DFS detection

1.6.2 How it works

Deploying the AutoWDS base network

AutoWDS provides different integration modes for managing P2P links for meshed networks. The majority of the configuration is performed on the WLC which manages the individual logical WLAN networks. You link an active AutoWDS profile with an established WLAN profile of your managed wireless network. The AutoWDS profile groups the settings and limits to form the P2P topology and of the AutoWDS base network.

The AutoWDS base network and its associated SSID (default name: **AutoWDS-Rollout**) is a management network only. It serves two purposes: The first is to authenticate an AP during the preconfigured integration, and the second is to establish the WLC tunnel for configuration exchange. In this way, unassociated APs remain isolated from operations while they are being integrated into the managed WLAN. As soon as there is a P2P connection to a master AP, an unassociated AP is considered to be integrated and it processes further communications via the bridge on Layer 2. Similar to conventional P2P links, the P2P partners set up a management SSID, which they use to process the data traffic and the CAPWAP tunnel to the WLC (see [Updating the AP configuration and establishing the P2P link](#) on page 81).

i The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within the WLAN infrastructure.

After assigning an active AutoWDS profile to your managed WLAN, the corresponding anchor APs deploy the AutoWDS base network and transmit their beacons (assuming you have enabled 'SSID broadcast' in the AutoWDS profile) with an additional manufacturer-dependent identifier. This identifier, also known as an "AutoWDSInfoFlag", signals the general support of the feature to unassociated AutoWDS-capable APs and informs them...

- > whether AutoWDS is enabled/disabled for the detected SSID;
- > whether the AP of the corresponding SSID has an enabled/disabled WLC connection;
- > whether the WLC accepts or prohibits the express mode for unassociated APs; and
- > whether integration requires the APs to connect to the equivalent physical WLAN interface of the anchor AP (strict interface pairing, i.e. with WLAN-1 to WLAN-1 and with WLAN-2 to WLAN-2), or whether mixed interface pairs are allowed.

A managed AP will automatically work as an AutoWDS AP after it has been initially paired with a WLC via LAN cable and a valid certificate and an AutoWDS profile with the additional AP configuration has been transferred correctly. A configured AutoWDS AP will automatically function as an unassociated AP after it has failed to establish a CAPWAP connection to a WLC after a predefined time, for example if there is no wired LAN connection. This access point then temporarily switches its operating mode to **Client** mode and scans each WLAN until it detects a suitable anchor AP. The scan is carried out in the 2.4-GHz and 5-GHz frequency bands.

If your device has two physical WLAN interfaces and both are enabled, both WLAN interfaces simultaneously scan for a suitable AutoWDS base network. If a physical WLAN interface detects a suitable SSID, then it associates with the anchor AP, assuming that the interface pairing mentioned above permits this. The other physical WLAN interface continues to scan in case the already associated physical WLAN interface loses the connection again. Until then, this physical WLAN interface does not connect to any other AutoWDS base network. Once your device has received the WLC configuration, the two physical WLAN interfaces behave as specified in the profile, i.e. they deploy the SSIDs assigned to them and the AutoWDS base network.

The procedure for searching for an AutoWDS base network is identical with that of the reconfiguration in the case that the WLAN connection is lost (see [Connectivity loss and reconfiguration](#) on page 82).

Differences between the integration modes

When integrating unassociated APs into your managed WLAN, you have the choice of two different integration modes. The integration mode determines the conditions under which your WLC accepts an unassociated AP:

- **Preconfigured integration** is the controlled and preferred method to integrate an unassociated AP into a managed WLAN over a point-to-point link. In this mode, the WLC only allows the integration of APs that have a local, preconfigured SSID and a valid WPA2 passphrase for the AutoWDS base network.

This mode is suitable for all productive environments, and is used to create a predefined relationship between an unassociated AP and an AutoWDS base network. As soon as the AP obtains a configuration from the WLC, the AP gives this configuration a higher priority than its own local AutoWDS configuration. This remains so until the WLC revokes the configuration via CAPWAP or you reset the device.

- **Express integration** is the quick way to integrate an unassociated AP into a managed WLAN via a point-to-point link. In this mode, the WLC allows both the integration of preconfigured devices as well as devices that are not configured at all. Unconfigured APs have neither a registered SSID nor an individual WPA2 passphrase for the AutoWDS base network. Instead, APs can authenticate with any AutoWDS base network by using a pre-shared key hard-coded in the firmware.

This mode is suitable for the easy integration of new APs into a managed WLAN. The choice of AutoWDS base network is automatic and is outside your control. As soon as the corresponding APs obtain configurations from the WLC, these devices save the settings as default values until the WLC revokes the configuration via CAPWAP, the device executes the express [reconfiguration](#) after an interruption in the connection, or you reset the device.

⚠ For the express integration make sure that no other AutoWDS base network is in range. Otherwise it is possible for an external WLC to take control of your AP and revoke your remote access. Having the express mode enabled increases the vulnerability to attack. For this reason it is advisable to disable the express mode if it is not absolutely necessary.

⚠ For the security reasons name above, LANCOM recommends a preconfigured integration. Through the pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. Learn more about this in section [Accelerating preconfigured integration by pairing](#) on page 87.

After successful authentication on the AutoWDS base network and retrieval of an IP address, the unassociated APs scan the network for a WLC. As soon as they have detected a WLC, they attempt to connect with it and retrieve a configuration. In LANmonitor, these APs are shown as unassociated devices. To include these in the managed WLAN, the administrator must still confirm them and assign WLAN profiles to them. Assigning profiles in this way is no different from accepting normal APs. Alternatively, assignment can be handled by the WLC if you

- set up a default WLAN profile and activate its automatic assignment; or
- enter the associated AP into the access point table and link it with a WLAN profile.

⚠ By simultaneously setting the automatic acceptance of unassociated APs by the WLC ("Auto Accept"), the integration of unassociated APs can be fully automated. However, for express integration you should ensure that you disable this setting in order to maintain a minimum level of security and hinder rogue AP intrusion.

-
- i The procedures for certificate generation, certificate checks, and the automatic acceptance or rejection of connection requests by the WLC are identical to a WLAN scenario with cable-connected APs. Refer to the section [Communication between access point and WLAN controller](#) on page 8 for further information on this.

Designing the topology

When the WLAN profile is assigned by the WLC, the slave APs simultaneously receive information about how their P2P links in the meshed network are to be established. The topology results directly from the hierarchy of the P2P connections established between the APs. The WLC offers the following management modes for this:

- > **Automatic:** The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.
- > **Semi automatic:** The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.
- > **Manual:** The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Normally, the WLC handles the automatic calculation of the topology, where a slave AP generally connects with the closest master AP. Calculated in real-time, the topology is recorded by the WLC in the status table **AutoWDS-Auto-Topology**. If you use semi-automatic or manual management, you define the static P2P links in the setup table **AutoWDS-Topology**. To achieve this, you specify the relationships between the individual master APs and slave APs in a similar manner to a normal P2P connection. For more on this, see the section [Manual topology management](#) on page 88.

-
- i The automatic generation of a P2P configuration (e.g., for initial connection or reconnection of an AP) replaces any existing entry in the AutoWDS-Auto-Topology table.
-
- i The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.
-
- i For manual topology configuration, it is important for a configured P2P master AP within the topology to be closer to the WLC than a corresponding P2P slave AP. This is because a brief interruption to the P2P connection will cause the slave AP to scan for the master AP.

Updating the AP configuration and establishing the P2P link

If an unassociated AP has received the full WLAN profile with all its settings from the WLC via CAPWAP, as a slave it attempts to establish a P2P link to the master AP assigned to it. The AP simultaneously changes its WLAN operation mode from **Client** back to **Managed**.

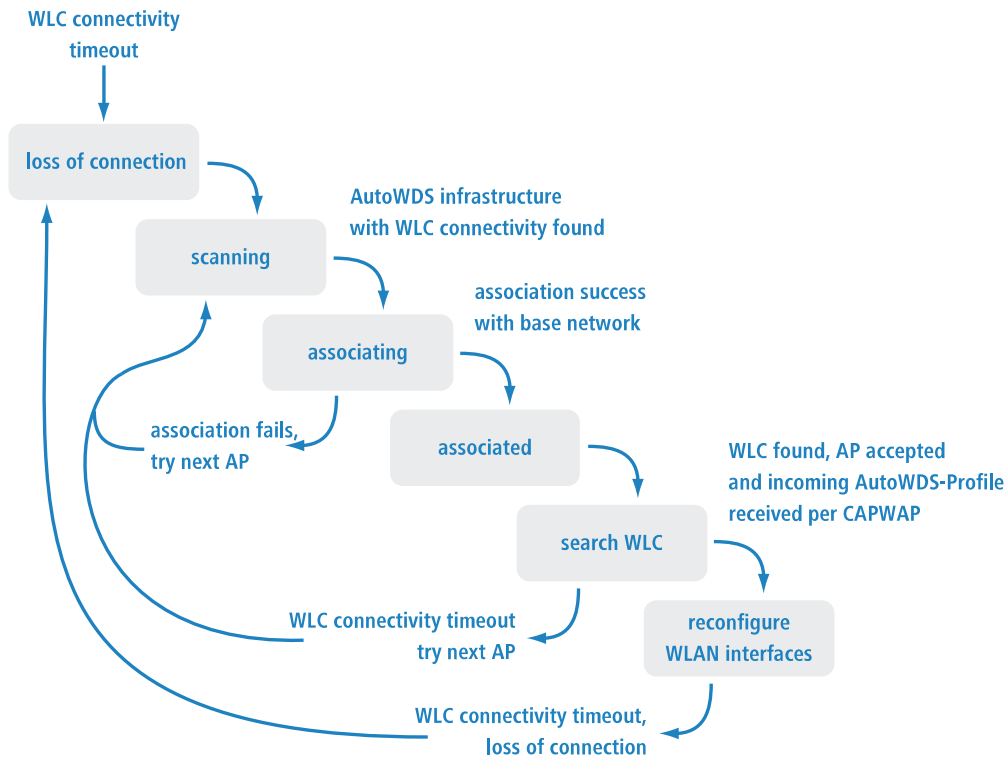
Since the master AP is already in managed mode, it obtains only an update to its P2P configuration from the WLC via CAPWAP. This informs the AP of the WPA2 passphrase and the peer identification of the AP. For an automatically generated P2P configuration, the peer identification corresponds to the MAC address; for a manual P2P configuration, it corresponds to the name of the slave AP. The master AP labels the SSIDs with ***** P2P Info *****.

Once both APs are successfully interconnected over a P2P link, the AutoWDS integration process is concluded. The unassociated AP can then be used by clients (smartphones, laptops, other APs in client mode looking for a master, etc.).

-
- i As long as the unassociated AP is in client mode, bridging between a physical WLAN interface and a LAN interface or another physical radio interface is disabled throughout the integration process. The device automatically puts all physical WLAN interfaces on different bridges. Not until successful creation of a P2P connection does the AP switch the bridging back to the original state.

Connectivity loss and reconfiguration

An automatic process of (re-)configuration is triggered as soon as you enable AutoWDS on an unassociated AP, if authentication at an anchor AP fails, or if an associated AP loses contact to the WLC. This process follows the scheme shown here:



An AP does not run the (re-)configuration process if it is in client mode and can connect to an anchor AP but not to the WLC. The AP waits for 5 minutes after connecting to the AutoWDS base network to see whether the WLC performs a configuration of the device. If no configuration is performed by the WLC by then (e.g., because no administrator accepts the AP), the AP disconnects from the AutoWDS base network and scans for further suitable SSIDs. If there is only one SSID in range, the AP contacts it again to repeat the integration process.

! If there is a connection to a LAN, the AP tries to reach the WLC by broadcast over the LAN for the duration of the downtime. If the AP finds the WLC via LAN, then no new P2P link is set up and the WLC deletes all automatically generated P2P links that set the AP to be a slave.

Configuration timeouts

The initial configuration and the reconfiguration of an unassociated AP are triggered by various timeouts, which together control the behavior of the device. This includes, if specified:

1. The duration of standalone P2P-link operation if the CAPWAP connection is lost (except for reconfiguration);
2. The wait time until the start of the automatic (re-)configuration for the preconfigured integration; as well as
3. The wait time until the start of the automatic (re-)configuration for the express integration.

The continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards the P2P part of the WLC configuration. If the standalone continuation time is specified as 0, the AP discards this part of the configuration immediately.



Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the wait times for the preconfigured and express integration—as a basis to count down the preset time

until the start of the (re-)configuration for the preconfigured integration. After this wait time expires, the device switches its physical WLAN interface(s) into client mode and scans the available SSIDs for the last detected AutoWDS base network. At the same time, the timer starts the countdown to the start of the automatic (re-)configuration for the express integration.

If the device has not found the expected AutoWDS base network when the express timer expires, the device automatically switches to express integration. It then searches for any AutoWDS-enabled network until a suitable anchor AP is detected.

By adjusting the interaction between the various wait times, you can allow the device to react flexibly to unforeseen events. This facilitates the implementation of a fallback solution, for example in the case that you change the pre-shared key for the AutoWDS base network. If the change should fail on an unassociated AP, the device becomes inaccessible as it has an invalid configuration. Please observe the notes under *Differences between the integration modes* on page 80.

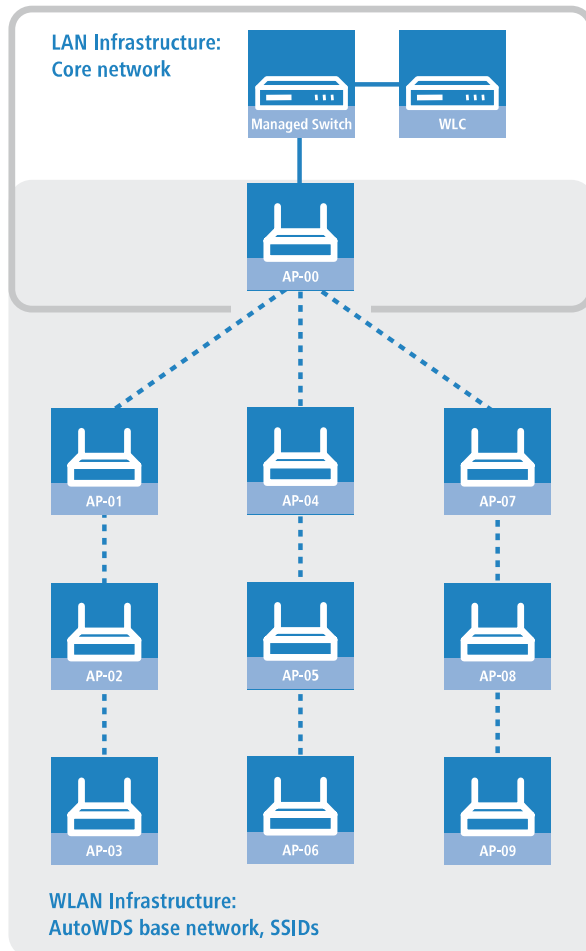
The relevant counters are configured on the AP (e.g. via LANconfig) and also on the WLC (Setup menu only). The counters are only observed by the AP if no WLC configuration (initial configuration) is available. As soon as a configuration is available, then the values specified in the AutoWDS profile apply (reconfiguration). Learn more about the setting the priorities for configurations under *Differences between the integration modes* on page 80.

-
-  If you disable the express timer or the preconfiguration timer, the device skips the corresponding integration step. The automatic reconfiguration can be switched off by disabling both timers. This means that, after being disconnected for long enough, the device can no longer be reached by AutoWDS. However, the device remains accessible over the LAN interface and searches the LAN for a WLC.
 -  The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to 0.
-

Example: Failure of an AP

Each AP maintains its CAPWAP connection by issuing echo requests to the WLC at a specified interval. If an AP fails or its connection is interrupted, these requests will be lost. If the APs repeat the echo request and receive no response from

the WLC, the CAPWAP connection is considered to be lost and the APs start the reconfiguration process described under *Connectivity loss and reconfiguration* on page 82.



For the infrastructure illustrated above, a failure of AP-01 would have the following impact, assuming that automatic topology management is enabled:

1. AP-01 is defective.
2. AP-02 and AP-03 repeat their echo-requests; all repeats fail.
3. AP-02 and AP-03 start the standalone operation of their P2P link (if configured) and continue to try to reach the WLC (over wireless and LAN, assuming connectivity exists).
4. AP-02 and AP-03 stop their autonomous operation of P2P connections.
5. AP-02 and AP-03 count down the wait time until the start of the preconfigured integration.
6. After the wait time expires, AP-02 and AP-03 switch into client mode and scan the WLAN for the last known AutoWDS base network.
7. AP-02 and AP-03 find a new anchor AP (e.g. B. AP-05 or AP-06) and login as clients.
8. AP-02 and AP-03 restore the CAPWAP connection via the **WLC-TUNNEL-AUTOWDS** and inform the WLC about the new anchor AP and the physical WLAN interfaces they are using.
9. The WLC generates a P2P link for the corresponding physical WLAN interfaces and delivers the configuration to the APs by CAPWAP.
10. The APs set up the new P2P link to the master APs assigned to them and stop communicating with the WLC via the **WLC-TUNNEL-AUTOWDS**; they are bridged to the LAN instead.

1.6.3 Setup by means of preconfigured integration


The following sections show you how to set up an AutoWDS network by means of the preconfigured integration. Configuration relies on the automatic topology management of the WLC.

In this scenario, a company is expanding its business premises into a new building. The company wants to integrate the new business premises into its existing managed WLAN. The relevant APs should be connected exclusively via point-to-point link. Between building A (old) and B (new), no wired network connection can be installed.

To keep the configuration simple, a single WLC is used to configure all of the APs. The exact number of APs in building A and building B is immaterial. Particular features, such as multiple physical WLAN interfaces, are automatically taken into account by the WLC topology management.


The configuration itself is divided into two parts:

1. Configuration of the WLC in building A
2. Configuration of all APs in building B

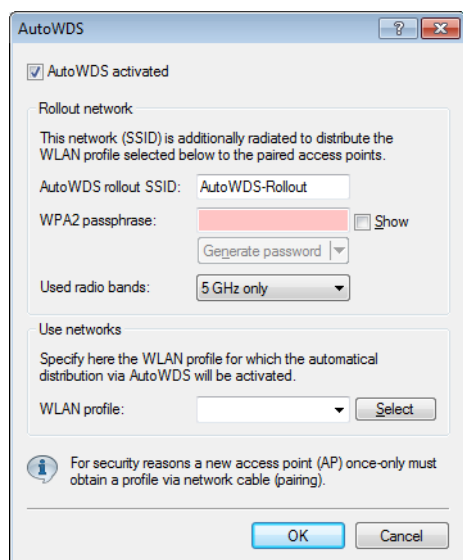
 The example application requires a valid WLAN configuration with valid certificates in the WLC. Just how to set up a managed WLAN is described in the chapter on WLAN management.

Configuring the WLC

The following instructions describe how to configure the AutoWDS of a central WLC for preconfigured integration.

 Ensure that the AutoWDS APs, which integrate with the network as WLAN clients, are able to reach a DHCP server via the WLC-TUNNEL-AUTOWDS interface. Without an IP address, the APs do not search for the WLC and thus do not receive a configuration from it.

1. Open the configuration dialog in LANconfig and click on **WLAN controller > Profiles > AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Enter the name of the AutoWDS base network under **AutoWDS-Rollout-SSID**. By default LANconfig uses the identifier `AutoWDS-Rollout`.

The SSID specified here acts as the management network for all APs that are searching for the AutoWDS network and, apart from the passphrase, it offers no further options for configuration. The WLC internally connects the specified SSID automatically using a WLC tunnel (**WLC-TUNNEL-AUTOWDS**). Normal WLAN clients are unable to use this management network.

! In this case, enter a custom AutoWDS rollout SSID that is different from the LANconfig default.

i Setting up this AutoWDS base network reduces the maximum number of SSIDs that your device can support on a physical WLAN interface by 1.

- Under **WPA2 passphrase** you enter a key to secure the AutoWDS base network.

Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

- Under **Used radio bands** you specify the frequency band used by the APs for the AutoWDS base network.

- Select the **WLAN profile** with the SSID which is to be enhanced with AutoWDS.

The APs with this WLAN profile serve as anchor APs and support the AutoWDS base network. At the same time, associated APs receive this WLAN profile via AutoWDS as a default configuration, which they use to transmit the corresponding SSID.

- Close the dialog window with **OK** and save the configuration to the device.

The WLC now assigns the AutoWDS settings to all managed AutoWDS-capable APs in your WLAN. These now form the basis for your AutoWDS base network. For future reconfiguration processes, the APs use only the SSID and passphrase stored here, unless configured otherwise (see *Differences between the integration modes* on page 80).

This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for preconfigured integration. The configuration steps are identical for all unassociated APs.

i There is no need to configure an AP that is already paired with a WLC. If devices are out of range of the WLC, thus making pairing impossible, then the SSID and passphrase can optionally be entered manually.

- Open the configuration dialog in LANconfig and click on **Wireless LAN > AutoWDS** to access the AutoWDS dialog.

- Click on **AutoWDS activated** to enable the feature on the device.
- Under **Network name (SSID)** enter the name of the AutoWDS base network that you configured on the WLC (e.g. AutoWDS-Rollout).
- Enter the key for the AutoWDS base network under **WPA2 passphrase** that you have configured on the WLC (e.g. AutoWDS-Control).
- Change the timeout values for the **Time till search mode 'Preconfig'** to 1 and for the **Time until search mode 'Express'** to 0.
- Under **Wireless LAN > General > Physical WLAN settings**, make sure that at least one physical WLAN interface is in **Managed** mode. Otherwise the device will never search for an AutoWDS base network.
- Close the dialog window with **OK** and save the configuration to the device.


After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for the specified AutoWDS base network. To learn more about the procedure, refer to the [chapter about the function](#).

1.6.4 Accelerating preconfigured integration by pairing

Through the one-time pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. For pairing, you reset an AP and connect it via LAN to the WLC used for running your managed WLAN including AutoWDS. In the reset state, the AP is automatically in managed mode after being switching on. Once the AP finds the WLC and the WLC accepts the AP, the AP automatically receives all relevant certificates and partial configurations required to configure the parameters in the device. Pairing is then complete. On location, a coworker installs the AP and switches it on. Your device then searches for the preconfigured AutoWDS base network.

The following steps summarize the pairing procedure. They also include the steps for automatic configuration assignment, which further simplifies the pairing of a high number of APs.

1. Start LANconfig and, on your WLC, set up a managed WLAN with a valid WLAN profile, if you have not already done so. In LANconfig you configure this type of profile under **WLAN controller > Profiles > WLAN profiles**.
2. Activate AutoWDS for this WLAN profile as described in [Configuring the WLC](#) on page 85.
3. Create a profile that is valid for all APs under **WLAN controller > AP configuration > Access point table** with the button **Default**. Assign the **WLAN profile** you created earlier to this profile
4. Enable the option **Automatically provide APs with a default configuration** under **WLAN controller > General**.
5. **Optional:** To avoid having to manually accept unassociated APs in LANmonitor by allowing the WLC to do this automatically, you should additionally select the option **Automatically accept new APs (auto-accept)**.

 For security reasons, you should only enable this option if you have connected the unassociated APs to the WLC via a LAN interface. To exclude the possibility of rogue AP intrusion, make sure that no other devices are connected with the WLC.


6. Send the configuration to the WLC.
7. Reset the unassociated AP and connect the device to the WLC via the LAN. The device automatically starts to search for a WLC.
8. In LANmonitor, you accept the new AP under **Wireless LAN > New APs**, unless you have set up automatic acceptance. The WLC sends the device those parts of the configuration that it needs for its future operation in managed mode. After successful configuration, LANmonitor lists the device in the **Active APs**.


This completes the pairing and the AP is ready for AutoWDS operation.

1.6.5 Express integration

The following sections show you how to set up an AutoWDS network by means of the express integration. Configuration relies on the automatic topology management of the WLC.

The initial scenario is similar to the [preconfigured integration](#).

 By default, AutoWDS is disabled on a reset AP and you must first use a wired access to activate the feature. However, an exception is made for devices that are explicitly setup with this feature at the customer's request: In this case, AutoWDS is enabled by default. The [second part of the configuration](#) is eliminated and the devices in express-integration mode can be commissioned directly.

 Express configuration has certain characteristics that are relevant to security. We recommend that you read the section [Differences between the integration modes](#) on page 80 carefully.

Configuring the WLC

The following instructions describe how to configure the AutoWDS of a central WLC for express integration.

1. Carry out each step under [Configuring the WLC](#) on page 85 for the preconfigured integration.
2. Log on to your device via WEBconfig or the console.

3. In the setup menu, switch to the table **WLAN Management > AP Configuration > AutoWDS Profiles**.
4. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
5. Change the **Allow-Express-Integration** parameter to **Yes** and save the settings by clicking on **Send**.

This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for express integration. The configuration steps are identical for all unassociated APs.

1. Open the configuration dialog in LANconfig and click on **Wireless LAN > AutoWDS** to access the AutoWDS dialog.

2. Click on **AutoWDS activated** to enable the feature on the device.
3. Under **Wireless LAN > General > Physical WLAN settings**, make sure that at least one physical WLAN interface is in **Managed** mode.
Otherwise the device will never search for an AutoWDS base network.
4. Close the dialog window with **OK** and save the configuration to the device.

After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for any AutoWDS base network. For further information on this procedure please refer to [Deploying the AutoWDS base network](#) on page 79.

1.6.6 Switching from express to preconfigured integration

Following a network rollout and the express integration, the switch to a preconfigured integration is implemented by disabling the express integration on the WLC. There is no need to change anything on the APs because they have already received an AutoWDS configuration during the express integration, and this pre-configures an AutoWDS network for subsequent re-configuration procedures.


1. Log on to your device via WEBconfig or the console.
2. In the setup menu, switch to the table **WLAN Management > AP Configuration > AutoWDS Profiles**.
3. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
4. Change the **Allow-Express-Integration** parameter to **No** and save the settings by clicking on **Send**.

You have now disabled the express integration of further unassociated APs.

1.6.7 Manual topology management

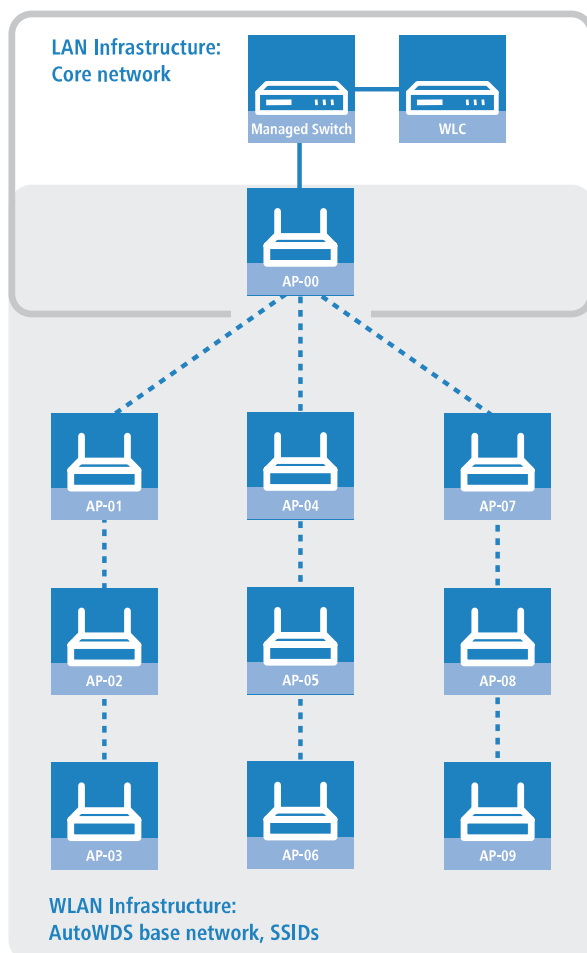
The examples of AutoWDS installation rely upon automatic topology management by the WLC, which simplifies the configuration. Depending on the usage scenario, it may be necessary to setup individual or all of the P2P links manually.

The following section shows you how to disable the automatic topology management on the WLC and create a manual P2P configuration. To configure the P2P links, you first assign unique names to each of the APs. Then link these names with the topology configuration and the physical WLAN interfaces being used. The chapter assumes that you have already performed the steps for the WLC under [Setup by means of preconfigured integration](#) on page 85, so that you can complete the basic configuration and enable AutoWDS on the WLC.

 In general, we recommend a maximum of 3 hops for AutoWDS operations.

Changes to the initial scenario

The initial scenario is similar to the preconfigured integration. The entire infrastructure is based on dual-radio APs, which are arranged according to the illustration below. The managed WLAN initially consists of a single AP, which serves as the initial anchor AP for the unassociated APs.

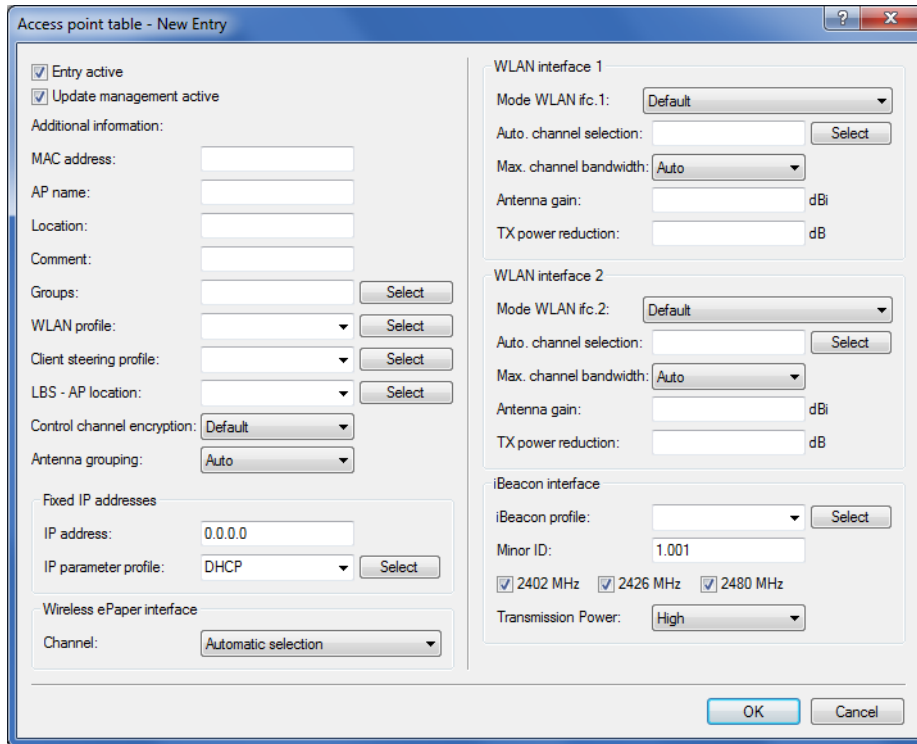


Configuring the WLC

The following instructions describe how to disable the automatic topology management and the configuration of manual P2P links according to the scenario described under [Manual topology management](#) on page 88.

1 WLAN management

1. Open the configuration dialog in LANconfig and click on **WLAN controller > AP configuration > Access point table** to access the list of managed access points.




2. For each unassociated AP, enter the **MAC address** and a unique identifier under **AP name**. You will reference this name later in the topology configuration.

For the example scenario, the individual configuration entries are as follows:

Table 1: Configuring the unassociated APs in the access point table

Entry	MAC address	AP name
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

 The table entry AP-00 refers to your existing AP, which the unassociated APs use as an anchor AP.

3. Select the **WLAN profile** for which you have enabled AutoWDS. By means of the corresponding WLAN profile, the APs automatically receive the settings for AutoWDS and hence for the P2P configuration.

4. Close the dialog window with **OK** and save the configuration to the device.
5. Log on to your device via WEBconfig or the console.
6. In the setup menu, switch to the table **WLAN Management > AP Configuration > AutoWDS Profiles**.
7. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
8. Change the **Topology-Management** parameter to **Manual** and save the settings by clicking on **Send**.
9. Navigate to the table **WLAN-Management > AP-Configuration > AutoWDS-Topology** and click on **Add**.
10. For each P2P pair, create a manual P2P configuration. The specified P2P link is always considered from the perspective of the slave AP.
 - a) In the field **AutoWDS-Profile**, specify the AutoWDS profile that applies for the manual P2P configuration, for example **DEFAULT**.
 - b) Set the **Priority** of the P2P configuration to 0 (highest priority).
 - c) For the **Slave-AP-Name** and **Master-AP-Name**, enter the names of the APs according to your hierarchy.

For the example scenario, the individual configuration entries in the case of strict interface pairing are as follows:

Table 2: Configuring the P2P pairs in the AutoWDS-topology table

Entry	Slave-AP-Name	Slave-AP-WLAN-Ifc.	Master-AP-Name	Master-AP-WLAN-Ifc.
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2
09	AP-09	WLAN-1	AP-08	WLAN-1

- d) Under **Key** specify the WPA2 passphrase used by the P2P partners to encrypt the P2P link.
Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength. If you leave the field empty, the device automatically generates a passphrase with a length of 32 characters.
- e) Switch the entry **Enabled** to **Yes**.
- f) Save the entries by clicking on **Send**.

If APs were already connected, the WLC sends the new configuration to these APs, which triggers the reconfiguration procedure for each one. If no APs were connected, the WLC transmits the P2P configuration when the unassociated APs connect for the first time.

1.6.8 Redundant paths by means of RSTP

In combination with the rapid spanning tree protocol (RSTP), manual topology management allows you to set up redundant P2P links to improve the failover reliability of your entire AutoWDS base network. To do this, you must first enable RSTP in the Setup menu of each AP, because the WLC management settings do not include this part of the configuration. You can reduce the work involved by transmitting a script to all of the APs by means of the WLC script management.

The following steps show you how to do this. These steps assume that you have successfully set up an AutoWDS base network. After activation, RSTP automatically performs the path search.

1 WLAN management

1. Create a text file with the name `WLC_Script_1.lcs`.
2. Copy the following lines of code into the text file and save it.

```
# Script (9.000.0000 / 15.07.2014)

lang English
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version      Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating           yes

flash Yes

# done
exit
```

3. Login to the WEBconfig interface of your WLC and navigate to **Extras > File management > Upload certificate or file**.
4. In the **File type** selection list, select **CAPWAP - WLC_Script_1.lcs** and use the **Browse** button to locate your script file. Then click on **Start upload**.
You can check if the file was successfully uploaded to the WLC in the Status menu under **File system > Contents**.
5. Navigate to the Setup menu item **WLAN management > Central firmware management > Script management** and click on **Add**.
6. For the **Profile** enter the corresponding WLAN profile and under **Name** enter `WLC_Script_1.lcs` in order to link the AutoWDS profile with the script name and to roll it out to the APs.
7. As described in section [Configuring the WLC](#) on page 89, assign unique names to the APs in the WLC and set up the manual P2P links.

You have now successfully completed the configuration.

1.7 Central firmware and script management

WLCs allow the configurations of multiple LANCOM WLAN routers and APs to be managed from a central location in a consistent and convenient manner. With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

To achieve this, the firmware and script files are stored on a Web server (firmware as *.upx files, scripts and *.lcs files). The WLC checks once daily, or when prompted by a user, to compare the available files with those on the devices. Alternatively, this procedure can be handled by a cron job—overnight, for example. If an update can be carried out, or if the AP is not running the desired firmware version, then the WLC downloads the file from the Web server and uploads it to the appropriate WLAN routers and APs.

The configuration of firmware and script management provides precise control over the distribution of the files. It is possible, for example, to limit certain firmware versions to certain device types or MAC addresses.

An update can be carried out in two possible states:

- > When a connection is established; the AP subsequently restarts automatically.
- > If the AP is already connected, the device does not restart automatically. In this case the AP is manually restarted with the menu action **Setup > WLAN-Management > Central-Firmware-Management > Reboot-updated-APs** or by a timed cron job.

- The action **Setup > WLAN-Management > Central-Firmware-Management > Update-Firmware-and-Script-Information** updates the script and firmware directories.

The parameters for configuration can be found under the following paths:

LANconfig: **WLAN controller > AP update**

WEBconfig: **Setup > WLAN-Management > Central-Firmware-Management**

1.7.1 General settings for firmware management

➤ Firmware-URL

The path to the directory with the firmware files.

- Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
- Default: Blank



Note that the Web server specified must permit directory listing. The firmware management uses this to retrieve information about the available firmware.

➤ Simultaneously loaded FW

The number of firmware versions loaded simultaneously into the main memory of the WLC.



The firmware versions stored here are downloaded from the server just once and then used for all update processes.

- Possible values: 1 to 10
- Default: 5

➤ Firmware loopback address

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

Possible values:

- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'.
- 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- Name of a loopback address.
- Any other IP address.

Default:

- Blank



If the list of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Firmware management table

This table is used to store information about which firmware versions are to be operated with which devices (MAC address) and device types.

Device types

Select here the type of device that the firmware version specified here is to be used for.

- > Possible values: All or a selection from the list of available devices.
- > Default: All

MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

- > Possible values: Valid MAC address
- > Default: Blank

Version

Firmware version to be used for the devices or device types specified in this entry. If necessary, an update for the specified devices or device types will be made to this firmware version. This is stated in the form: "xx.yy", e.g. 10.40. Default: Blank

Date

The date allows you to downgrade to a specific firmware version within a release, for example from a Release Upgrade (RU) on an earlier upgrade.

- > Possible values: 8 characters from 0123456789. The entry must match the format of the UPX header, e.g. "01092014" for the September 01, 2014.
- > Default: Blank

General settings for script management

> Script URL

The path to the directory with the script files.

Possible values:

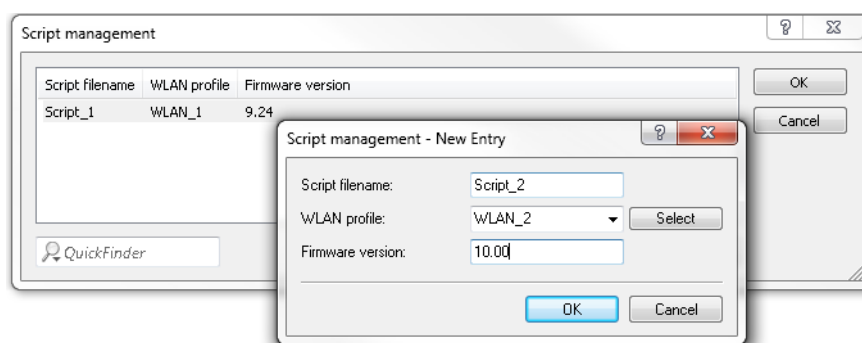
- > URL in the form `Server/Directory` or `http://Server/Directory`
- > Default: Blank

Script management table

In this table, scripts are assigned to a WLAN profile depending on the name of the script file.

Configuring a WLAN router and Access Point in the Managed mode is handled via WLAN profiles. A script can be used for setting those detailed parameters in managed devices that are not handled by the pre-defined parameters in a WLAN profile. Distribution is also handled by WLAN profiles to ensure that the wireless routers and APs with the same WLC configuration also use the same script.

As only one script file can be defined per WLAN profile, versioning is not possible here. However, when distributing a script to a wireless router or Access Point, an MD5 checksum of the script file is saved. This checksum allows the WLC to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.



Script filename

Enter the CAPWAP slot you selected for the script upload to the WLAN controller (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs). If the WLAN controller obtains the script from a web server, the script name on the web server has to be entered. Possible values: File name in the form *.lcs. Default: Blank.

WLAN profile

Select here the WLAN profile that the script file specified here should be used for. Possible values: Selection from the list of defined WLAN profiles. Default: Blank

Firmware version

By specifying a firmware version, you determine the LCOS version set in the script that is rolled out.


⚠ Please enter the firmware version in the form "xx.yy", e.g. 10.00 or 9.24.

Internal script storage (script management without HTTP server)

In contrast to firmware files, script files are very small. The WLC's internal script storage allows the storage of up to three scripts of up to 64KB each. If script requirements do not exceed this volume, an HTTP server does not need to be configured for this purpose.

Script files are simply loaded from the designated storage location using WEBconfig. After upload, the list of available scripts must be updated with **Setup > WLAN-Management > Central-Firmware-Management > Update Firmware and Script Information**.

The internal scripts can be referenced from the script management table using the relevant names (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs).

 Please be careful with upper and lower case letters when entering script names.

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])

File Name/Location: SSL - Certificate (*.pem, *.crt, *.cer [BASE64])

Passphrase (if required):

Caution: Files are not performed by the interface can be seen in the VPN

Replace existing

- SSL - Private Key (*.key [BASE64 unencrypted])
- SSL - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
- SSL - Container as PKCS#12-File (*.pfx, *.p12)
- SSH - RSA Key (*.key [BASE64])
- SSH - DSA Key (*.key [BASE64])
- SSH - ECDSA Key (*.key [BASE64])
- SSH - accepted public keys
- VPN - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
- VPN - Device Certificate (*.pem, *.crt, *.cer [BASE64])
- VPN - Device Private Key (*.key [BASE64 unencrypted])
- VPN - Container (VPN1) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN2) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN3) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN4) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN5) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN6) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN7) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN8) as PKCS#12-File (*.pfx, *.p12)
- VPN - Container (VPN9) as PKCS#12-File (*.pfx, *.p12)

1.8 RADIUS

RADIUS stands for “Remote Authentication Dial-In User Service” and is referred to as a “triple-A protocol”. The three “A”s stand for

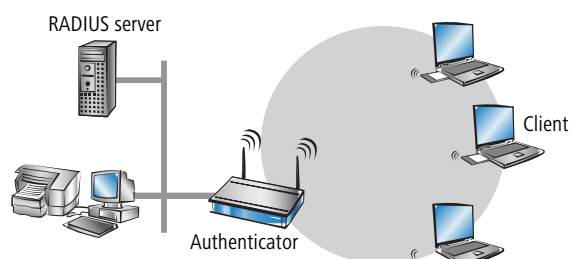
- > Authentication
- > Authorization
- > Accounting (billing)

This protocol allow you to grant users access to a network, to assign them certain rights and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

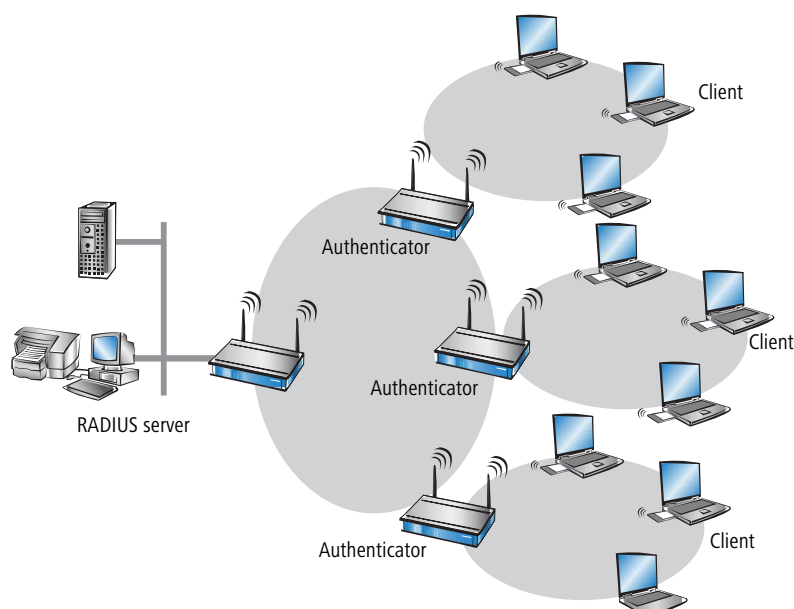
3 different devices are required for RADIUS to work.

- > Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.

- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by an access point, for example. The authenticator is referred to as the Network Access Server (NAS).



- Authentication server: RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of an access point for this task.



The authenticator has no initial information on the clients wanting to register. This is all stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database there and can vary from network to network. The authenticator has just the one task, that of transferring the information between the client and the RADIUS server.

Access to a RADIUS server can be configured in several ways:

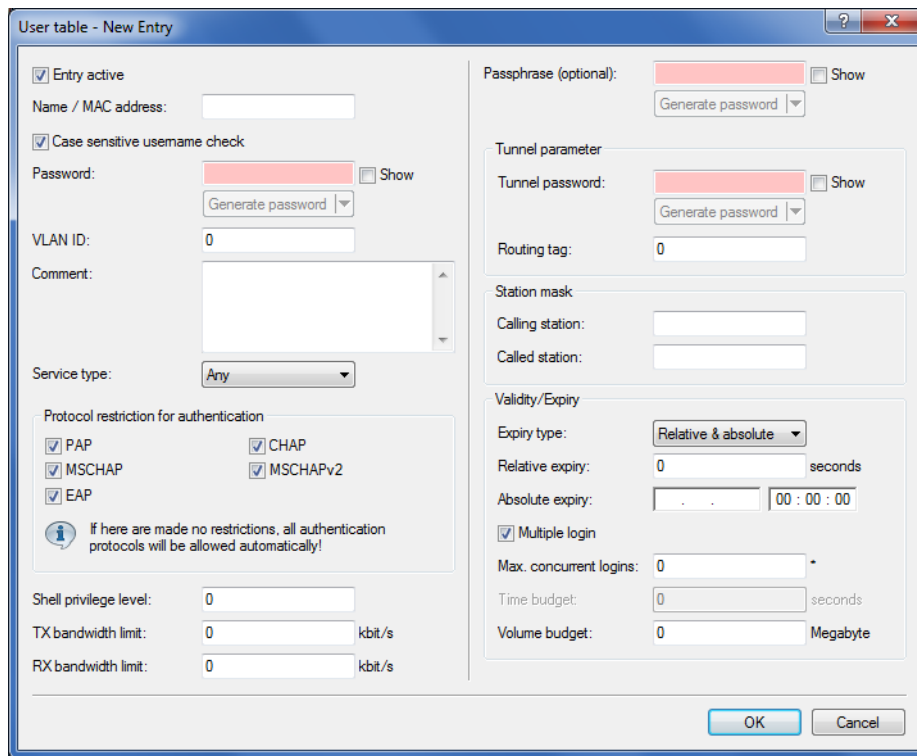
- Using PPP when dialing into a network
- Via WLAN
- Via a public spot for users who register using a browser
- Via the 802.1X protocol

1.8.1 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to authenticate WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal user table in the WLC.

1 WLAN management

In LANconfig enter the approved MAC addresses into the RADIUS database in the configuration section **RADIUS > Server** on the **General** tab. Enter the MAC address as **Name** and as **Password** and select the authentication method **All**.



1.8.2 External RADIUS server

By default the WLC forwards account and access management requests to a RADIUS server. In order for APs to contact the RADIUS server directly, the necessary server information has to be specified here. This ensures that the RADIUS application continues to function even if the WLC is unavailable. However, this means that the RADIUS server requires

settings for each and every AP, and the managed APs must be able to access the RADIUS server from their management network. If the RADIUS server is on another IP network, then it is vital that the gateway is set in the IP parameter profile.

LANconfig: **WLAN controller > Profiles > RADIUS profiles**

Name

Specify an identifier for this entry.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

Authentication server

IP address

Enter the IP address of authentication server.

Port

Enter the port used by the authentication server.

Secret

This entry contains the shared secret used for authorization.

Show

Enables / disables the display of the key.

Source address (optional)

Enter the loopback address of the device, where applicable.

Protocol

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Accounting server**IP address**

Enter the IP address of accounting server.

Port

Enter the port used by the accounting server.

Secret

This entry contains the shared secret used for authorization.

Show

Enables / disables the display of the key.

Source address (optional)

Enter the loopback address of the device, where applicable.

Protocol

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.


1.8.3 Dynamic VLAN assignment

Larger WLAN infrastructures often require individual WLAN clients to be assigned to certain networks. Assuming that the WLAN clients are always within range of the same APs, then assignment can be realized via the SSID in connection with a particular IP network. If on the other hand the WLAN clients frequently change their position and logon to different APs then, depending on the configuration, they may find themselves in a different IP network.

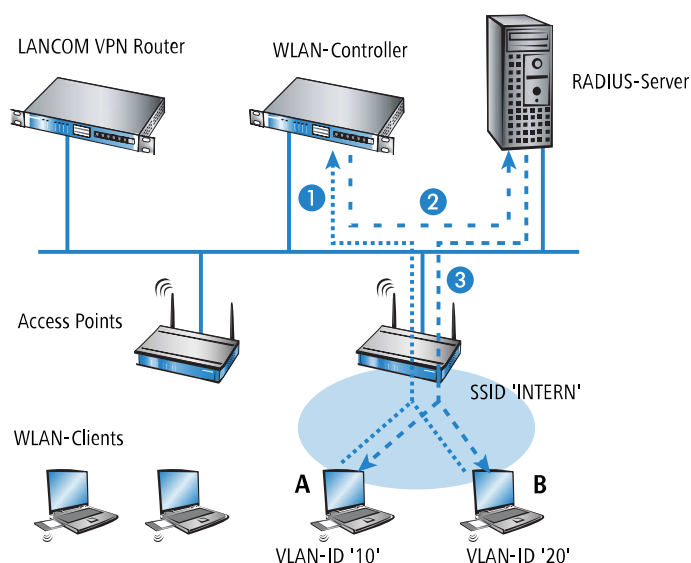
For WLAN clients to remain within a certain network **independent** of their current WLAN network, dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID, in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

Example:

- > The WLAN clients of two employees log into an AP in the WPA2-secured network with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the AP. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests are automatically forwarded to the WLC. This forwards the request in turn to the defined RADIUS server. The RADIUS server can check the access rights of the WLAN clients. It can also use the MAC address to assign a certain VLAN ID, for example for a certain department. The WLAN client in Marketing, for example, receives the VLAN ID '10' and WLAN client from Research & Development receives '20'. If no VLAN ID is specified for the user, the SSID's primary VLAN ID is used.
- > The WLAN clients of the guests log into the same AP in the unsecured network with the SSID 'PUBLIC'. This SSID is statically bound to the VLAN ID '99' and leads the guests into a certain network. Static and dynamic VLAN assignment can be elegantly operated in parallel.

 Assignment of the VLAN ID by the RADIUS server can be controlled by other criteria, such as a combination of user name and password, for example. In this way the unknown MAC address of a visitor to a company can be assigned a VLAN ID that permits guest access for Internet access only, for example, but that prohibits access to other network resources.

- ! As an alternative to an external RADIUS server, WLAN clients can be assigned with a VLAN ID via the internal RADIUS server or the stations table in the WLC.



1. Activate VLAN tagging for the WLC. This is done in the physical parameters of the profile by entering a value greater than '0' for the management VLAN ID.
2. For authentication via 802.1x, go to the encryption settings for the profile's logical WLAN network and choose a setting that triggers an authentication request.
3. To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

- ! For the management of WLAN modules with a WLC, a RADIUS server is required to operate authentication via 802.1x and MAC-address checks. The WLC automatically defines itself as the RADIUS server in the APs that it is managing—all RADIUS requests sent to the AP are then directly forwarded to the WLC, which can either process the requests itself or forward them to an external RADIUS server.

4. To forward RADIUS requests to another RADIUS server, use LANconfig to enter its address into the list of forwarding servers in the configuration section 'RADIUS servers' on the **Forwarding** tab. Alternatively, external RADIUS servers can be entered in WEBconfig under **Menu tree > LCOS Setup > RADIUS > Server > Forward servers**. Also, set the standard realm and the empty realm to be able to react to different types of user information (with an unknown realm, or even without a realm).
5. Configure the entries in the RADIUS server so that WLAN clients placing requests will be assigned the appropriate VLAN IDs as based on the identification of certain characteristics.

- ! Further information about RADIUS is available in the documentation for your RADIUS server.

1.8.4 Activating RADIUS accounting for logical WLANs in the WLAN controller

The configuration for logical WLAN networks is to be found in the following menu:

LANconfig: **WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**

RADIUS accounting activated


This is where you can activate RADIUS accounting for this logical WLAN network.

Possible values:

- > Yes, No

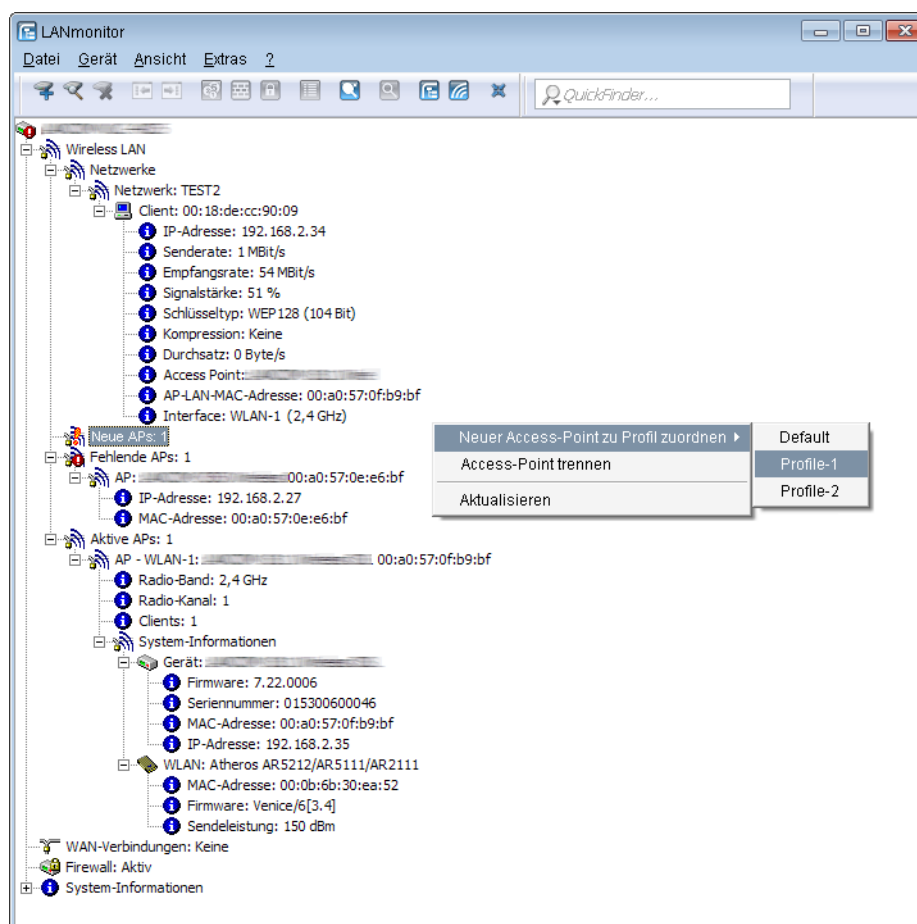
Default:

- > No

 The APs supporting the logical WLAN network as configured by the WLC must have a LCOS version 8.00 or higher.

1.9 Displays and commands in LANmonitor

LANmonitor gives you a quick overview of the WLCs in your network and the APs within the WLAN infrastructure. LANmonitor displays the following information, among other things:



- Active WLAN networks with the logged-in WLAN clients and the descriptor of the APs that they are associated with.
- Display of new APs with IP and MAC address
- Display of missing APs with IP and MAC address
- Display of managed APs with IP and MAC address, the utilized frequency band, and the channel

i For APs with an older firmware version and unable to transmit this data, the WLC takes the channel and frequency information from the **Active radios** status table under **Status > Active-Radios > WLAN-Management > AP-Status**.

Using the right-hand mouse key, a context menu can be opened for the APs and the following commands are available:

- **Assign new access point to profile**
Enables a new AP to be allocated to a profile and accepted into the WLAN infrastructure.
- **Disconnect access point**
Terminates the connection between AP and WLC. The AP then carries out a new search for a suitable WLC. This command can be used after a backup event to disconnect APs from a backup WLC and to redirect them to the correct WLC.
- **Refresh display**

Updates LANmonitor's display.

1.10 RF optimization

Selecting the channel from the channel list defines a portion of the frequency band that an AP uses for its logical wireless LANs. All WLAN clients that need to connect to an AP have to use the same channel on the same frequency band. The 2.4-GHz band works with channels 1 to 13 (depending on the country) and the 5-GHz band works with channels 36 to 64. On each of these channels, only one AP can actually transfer data. In order to operate another AP within radio range with maximum bandwidth, the AP must make use of a separate channel—otherwise all of the participating WLANs have to share the channel's bandwidth.

! With a completely empty channel list, the APs could automatically select channels which overlap in some areas, so reducing signal quality. Similarly, the APs might select channels which the WLAN clients cannot use due to the country settings. To steer APs towards certain channels, the non-overlapping channels 1, 6, 11 can be activated in the channels list.

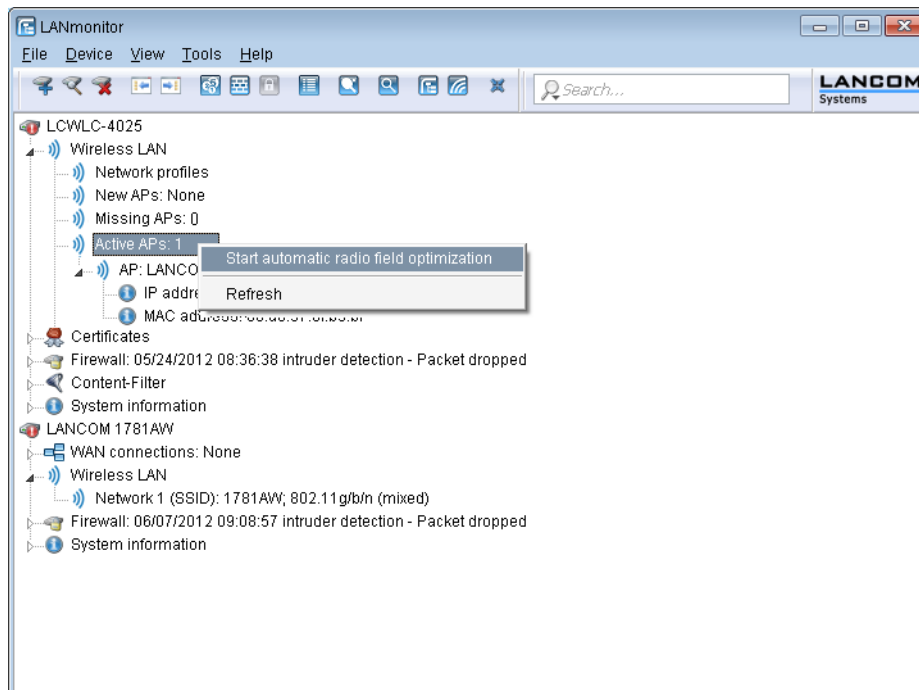
In larger installations with several APs it can be difficult to set a channel for every AP. With automatic radio-field (RF) optimization, the WLCs provide an automatic method of setting the optimum channels for APs that work in the 2.4-GHz band and 5-GHz band.

! You should ensure that APs transmitting in the 5-GHz band are set to the "indoor only" mode.

Command line: **Setup > WLAN-Management > Start-automatic-radio-field-optimization**


i You can invoke optimization for a particular AP by entering its MAC address as a parameter for the action.

LANmonitor: Right-click on the list of active APs or on a specific device, and in the context menu select **Start automatic RF optimization**.



Optimization is then carried out in the following stages:

1. The WLC assigns the same channel to all APs. The selected channel is the one being used by the majority of APs.
2. The APs carry out a background scan and report the results to the WLC.
3. Based on the devices found by the background scan, the WLC sets an interference value for each AP.
4. It then deletes the AP channel list for all APs. With the channel list now empty, each AP receives a configuration update with a new channel list for its respective profile.
5. The WLC disables the radio modules of all APs.
6. The individual APs now go through the following sequence. This begins with the AP with the highest interference value being the first to select a channel.
7. In the order of the interference values the WLC enables the radio modules in the APs, which then start their automatic calibration. Each AP automatically searches for the best channel from the channel list assigned to it. To determine which channel is the best, the AP scans for interference in order to allow for the signal strengths and channels occupied by other APs. Because the former list in the WLC configuration was deleted, this is now the profile channel list. If the profile channel list is empty, then the AP has freedom of choice from the channels that are not occupied by other radio modules. The selected channel is then communicated back to the WLC and entered into the AP channel list there. For this reason, the AP receives the same channel the next time a connection is established. The AP channel list has a higher weighting than the profile channel list.

 If an AP has multiple radio modules, each module goes through this process in succession.

 Radio-field optimization is a component of the LANCOM Active Radio Control (ARC).

1.10.1 Group-related radio field optimization

A WLC allows the grouping of APs by location information, device properties or network structure. This grouping can also be used as a basis for radio field optimization. Instead of performing a radio field optimization either for all APs or just for one of them, you can address all of the APs within a building tract, with a particular name, or with a particular firmware version.

Groups can be addressed via WEBconfig and also via the console by means of the Group parameters:

```
do /Setup/WLAN-Management/start optimization <Group>
```


The APs can be filtered with the following group-parameter options:

-g <Group name>

APs, which belong to the group. Multiple group names can be separated by commas.

-l <Location>

APs with the corresponding location setting.

 The combination of **-l** and one of the location options **-c** to **-r** is not useful.

-c <Country>

APs with the corresponding country setting.

-i <City>

APs with the corresponding city setting.

-s <Street>

APs with the corresponding street setting.

-b <Building>

APs with the corresponding building setting.

-f <Floor>

APs with the corresponding floor setting.

-r <Room>

APs with the corresponding room setting.

-d <Device name>

APs with the corresponding device name.

-a <Antenna>

APs with the corresponding number of antennas.



A combination of the options `-d` and `-a` is not useful.

-v <Firmware>

APs with this firmware version only.

-x <Firmware>

APs with a firmware version less than that specified here.

-y <Firmware>

APs with a firmware version less than or equal to that specified here.

-z <Firmware>

APs with a firmware version greater than that specified here.

-t <Firmware>

APs with a firmware version greater than or equal to that specified here.



Combinations are possible, e.g. to address APs with a firmware version between two versions.

-n <Intranet-Address>

APs located on the intranet with the address specified here.

-p <Profile name>

APs included in the WLAN profile specified here.

1.11 Client steering by WLC


With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLC. Managed APs constantly report the current values to the WLC, which uses these criteria to decide which APs may respond to requests from WLAN clients. For this reason, client steering is only possible with APs that are centrally managed by a WLC.


In managed networks a WLC centralizes the client steering for all connected APs. In this case, client steering works as follows:


1. The WLC collects the data about the associated WLAN clients from the APs connected to it. These data are the basis for the WLC to control the client steering.
2. All APs are configured so that client steering is handled by the WLC.
3. An unassociated WLAN client sends a probe request to the APs within its range.
4. Using CAPWAP, the APs transmit the request and the signal strength of the WLAN client to the WLC.
5. For each AP within range of the WLAN client, the WLC calculates a value from three factors:
 - > Signal strength value
 - > A value calculated from the number of clients associated at the AP
 - > Frequency band value

The WLC weights these factors and multiplies them together to derive the final value.

6. APs with the highest value, or a value that deviates from it within a specified tolerance level, receive a message from the WLC that they may accept the WLAN client at the next login attempt.
7. WLAN clients attempting to connect to an AP before it has received the response from the WLC are rejected.
8. If a WLAN client is acting "sticky", i.e. it does not attempt to connect to another AP with a good connection quality even though its current connection is of a lower quality, the WLC can prompt the current AP to log off the WLAN client. The WLAN client is then forced to connect with the AP offering the better connection.

 If an AP loses connection to the WLC which is responsible for client steering, the AP accepts all connections from authenticated WLAN clients.

 In order to optimize managed client steering, all APs require the installation of LCOS9.00 or later. If you have mixed operations with APs using earlier versions of LCOS, your WLAN will not be capable of optimizing the distribution of clients.

 In scenarios with time-critical roaming, such as with VoIP phones, you should not use client steering, as this can delay the client's login process.

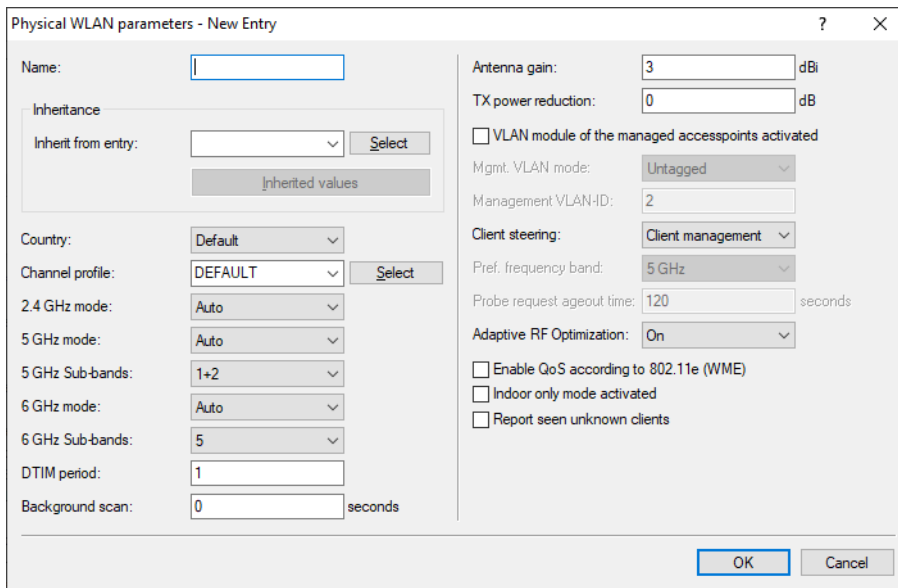
1.11.1 Configuration

You configure client steering with LANconfig as follows:

1. First, in the WLC you activate client steering for an AP under **WLAN controller > Profiles > Physical WLAN parameters** using the selection list **Client steering**.
 - > **Off**: Client steering is deactivated.
 - > **AP-based band steering**: The AP independently steers the WLAN client to a preferred frequency band.

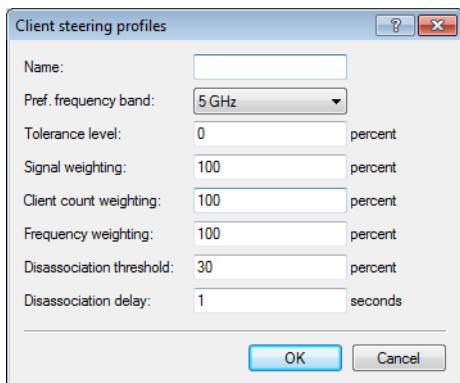
1 WLAN management

> **On:** The AP lets the WLC handle the client steering.



2. The menu **WLAN-Controller > AP-Configuration > Client steering profiles** contains two preconfigured default profiles (high density, default), which are sufficient for most use cases. Optionally, you create a new client steering profile by clicking on **Add**.

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.



The items have the following meanings:

Name

Name of the client-steering profile.

Pref. Frequency band

Specifies the frequency band to which the WLC steers the WLAN client.

- > **2.4GHz:** The WLC steers the WLAN client to the 2.4-GHz frequency band.
- > **5GHz:** The WLC steers the WLAN client to the 5-GHz frequency band.

Tolerance level

The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

Signal-Strength-Weighting

Specifies the percentage weighting of the signal-strength value used to calculate the final value.

Associated-Clients-Weighting

Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Frequency-Band-Weighting

Specifies the percent weighting of the value for the frequency band used to calculate the final value.

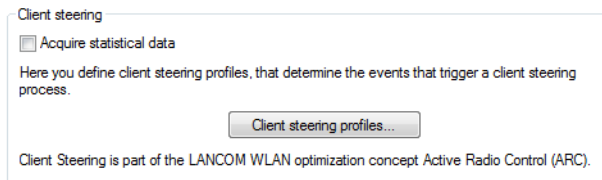
Disassociation threshold

Specifies the percentage of the maximum signal strength. If the current signal strength falls below this value, the client is disconnected.

Disassociation delay

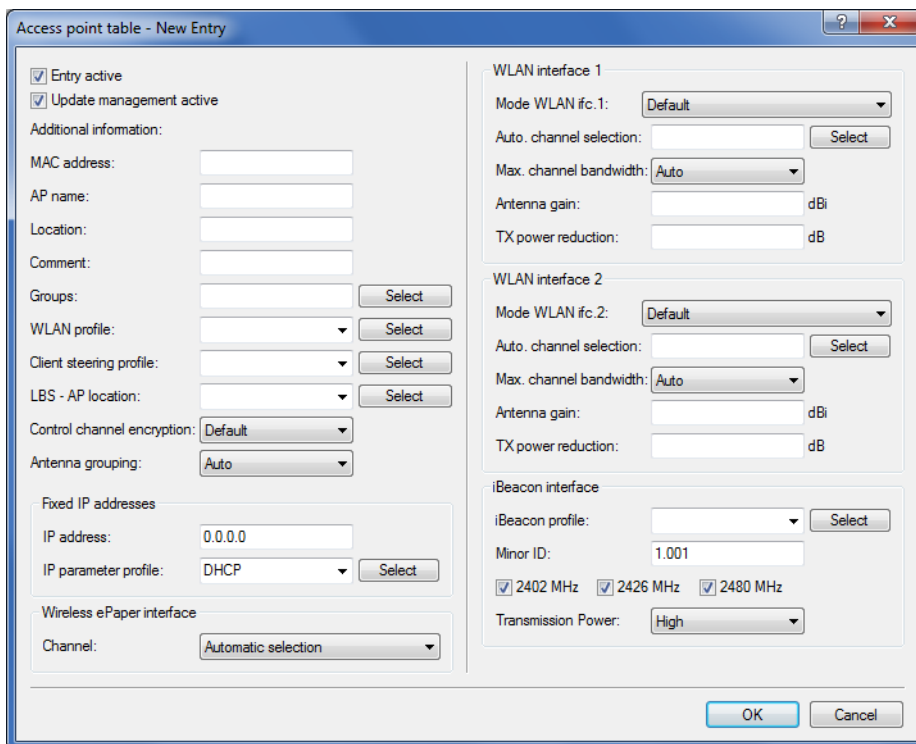
Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

- 3. Optional: Enable the capture of client-steering statistics with the parameter **Acquire statistical data**. This statistical data is suitable for analysis by LANmonitor, for example.

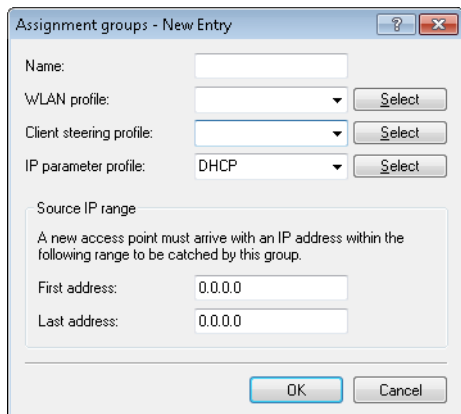


i Statistics capture increases the load on the WLC. LANCOM does not recommend the permanent recording of statistics.

- 4. Now assign one of the client-steering profiles to the corresponding AP in the AP table under **WLAN controller > AP configuration > Access point table**.



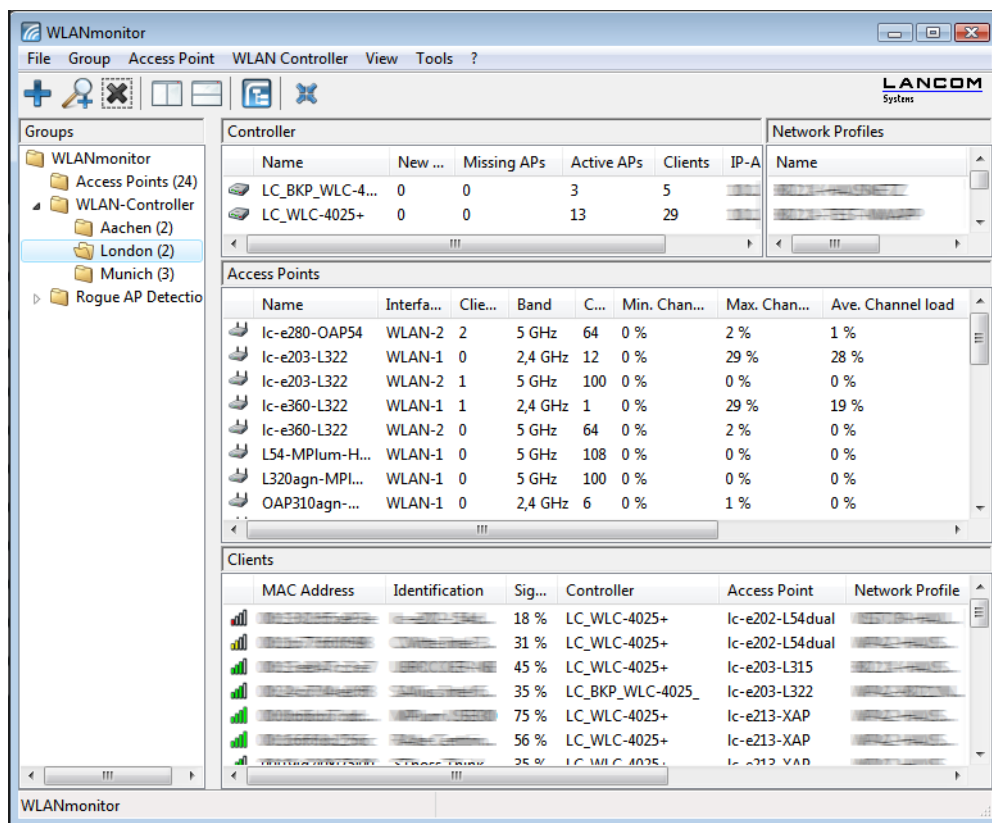
- Optional: If necessary, assign a suitable client-steering group to the defined assignment groups.



You have now completed the configuration of the client steering.

1.12 Channel-load display in WLC mode

The loads on the various channels used by each AP which is managed by a WLC are displayed as three values, the minimum, maximum and average channel load. The values displayed are measured every three minutes. Consequently, the first values are displayed after three minutes at the earliest.



1.13 Backing up the certificates

At system startup, a WLC generates the basic certificates for the assignment of certificates to the APs, including the root certificates for the CA (Certification Authority) and the RA (Registration Authority). Based on these two certificates, the WLC issues device certificates for the APs.

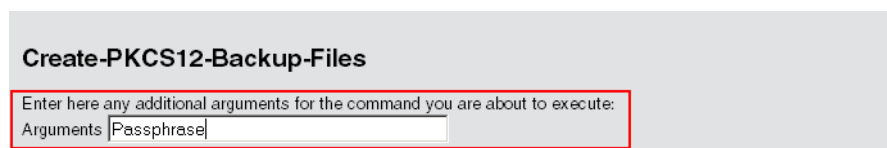
If multiple WLCs are employed in parallel in the same WLAN infrastructure (for load balancing) or if a device is being replaced or reconfigured, the same root certificates should always be used to avoid problems operating the managed APs.

1.13.1 Create backups of the certificates

To restore the CA or RA, the relevant root certificates with private keys will be required as generated automatically when the WLC was started. Furthermore the following files with information on issued device certificates should also be backed up. To ensure that this confidential information remains protected even when exported from the device, it is initially stored to a password-protected PKCS12 container.

WEBconfig

1. Open the configuration of the WLC in WEBconfig and go to **Extras > LCOS menu tree > Setup > Certificates > SCEP-CA > CA-certificates**.
2. Select the command **Create PKCS12 backup files** and enter the passphrase for the PKCS12 container as the additional argument.



Create-PKCS12-Backup-Files

Enter here any additional arguments for the command you are about to execute:

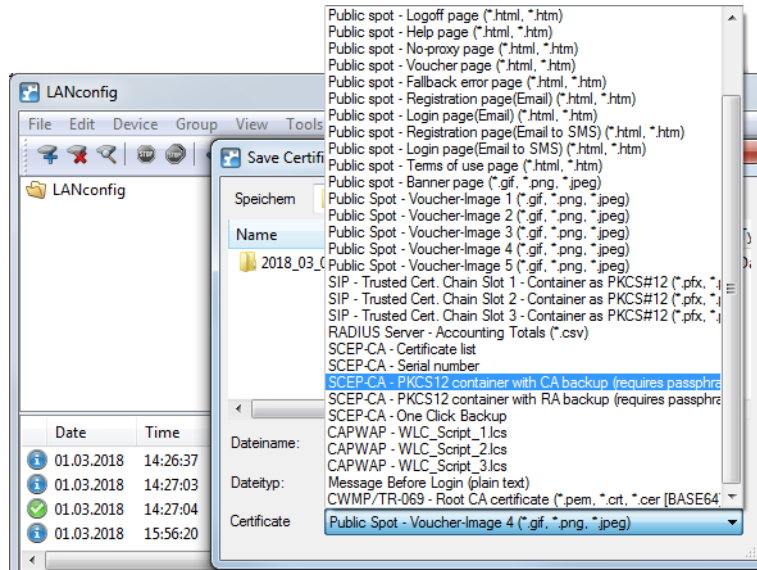
Arguments |Passphrase|

This command backs up the certificates and private keys to the PKCS12 files and these can then be downloaded from the device.

LANconfig

1. Highlight the WLC in the device view section and in the menu **Device > Configuration management** select the item **Save certificate as file**.

2. Set the **Certificate type** to PKCS12 container and click **Save**.



1.13.2 Uploading a certificate backup into the device

1. Click on **Extras > File management > Upload certificate or file**.
2. Select the two entries for SCEP-CA as data type one after the other:
 - > PKCS12 container with CA backup
 - > PKCS12 container with RA backup
3. For each upload, enter the file name, storage location, and the passphrase that was defined when the backup file was created. Confirm with **Start upload**:

Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type:

File Name/Location:

Passphrase (if required):

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

4. After loading the CA backup, the file `controller_rootcert` in the directory **Status > File-System > Contents** must be deleted.
Enter the following commands in the console:

```
cd /Status/File-System/Contents
del controller_rootcert
```

5. After restoring the backup, delete all files that start with `controller_` or `eaptls_`.
6. After that, access the directory **Setup > Certificates > SCEP-Client** and execute the command `Reinit`:

```
cd /Setup/Certificates/SCEP-Client
do Reinit
```


1.13.3 Backing up and restoring further files from the SCEP-CA

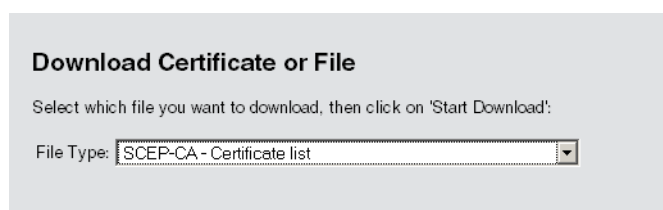
To be able to fully restore the SCEP-CA, it is important to have the information on the device certificates issued for the individual APs by the SCEP-CA.

! If the root certificates only were backed up, then any issued device certificates can no longer be revoked!

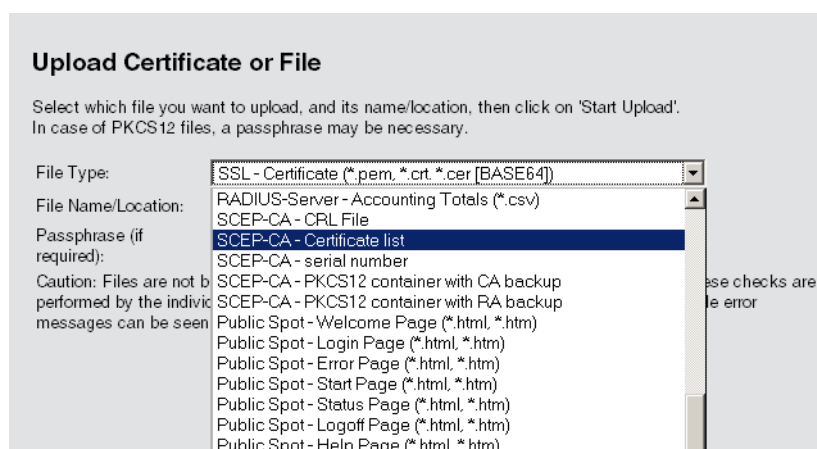
For this reason the following files have to be saved in addition to the certificates themselves:

- > SCEP certificate list: List of all certificates ever issued by the SCEP-CA.
- > SCEP serial numbers: Contains the serial number for the next certificate.

1. Click on **Extras > File management > Download certificate or file**.
2. Select the entries listed above as data type one after the other and then confirm with **Start download**:



3. To upload these files to the device, go to the entry page of WEBconfig and select the command **Upload certificate or file**.
4. Select the entries listed above as data type one after the other, enter each file name and storage location and confirm with **Start upload**:



! After installing a new certificate list, expired certificates are removed and a new CRL is created. Furthermore, the CA reinitializes itself automatically if certificates and keys are successfully extracted after loading the certificate backup.

1.13.4 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.

These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in LCOS. If you cannot wait until the individual services request


new certificates, a manual resolution requires deleting the SCEP files from the LCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, LCOS performs the necessary steps automatically.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup > Certificate > SCEP-CA > CA certificate**. This action generates a ZIP file within the LCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password, unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **Extras > File management > Download certificate or file > SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **Extras > File management > Upload certificate or file > SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.

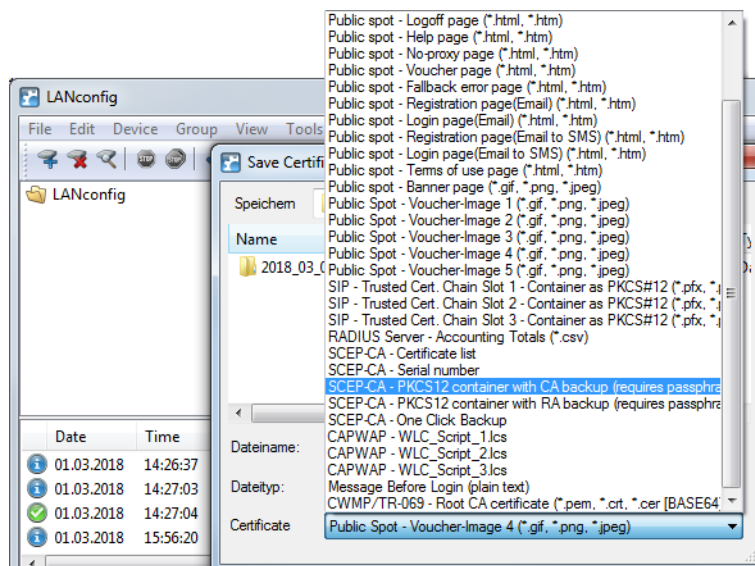
 If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action [2.39.2.2.11 Restore-certificates-from-Backup](#) in order for the device to restore the certificate record.

1.13.5 Using LANconfig to backup and restore certificates

Certificates are stored and uploaded with LANconfig as follows:

Save

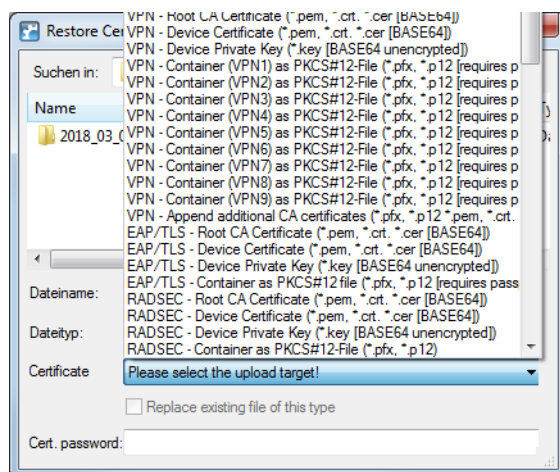
1. Highlight the WLC in the device view section and in the menu **Device > Configuration management** select the item **Save certificate as file**.
2. Set the **Certificate type** to PKCS12 container and click **Save**.



Upload

1. Highlight the WLC in the device view section and in the menu select **Device > Configuration management** and the item **Upload certificate or file**.
2. Set the **Certificate type** to PKCS12 container.

- Now navigate to the desired file, enter the password if necessary and click **Open**.



One Click Backup

For the One Click Backup, select the entry "SCEP-CA - One Click Backup" from the dialog list.

1.14 Backup solutions

WLCs manage a large number of APs, which in turn may have a large number of WLAN clients associated with them. WLCs thus play a crucial role in the functioning of the entire WLAN infrastructure—for which reason the organization of a backup solution in case of temporary WLC failure is in many cases indispensable.

In case of a backup event, a managed AP should connect to an alternative WLC. Because this connection will only function if the certificate in the AP has been authorized by the backup controller, it is essential that all WLCs sharing a backup solution have identical root certificates.

1.14.1 WLC cluster

If you are operating multiple WLCs in your network, you can collect these devices into a cluster. The APs in a managed WLAN are no longer managed by a single, central WLC but by multiple, synchronized WLCs. For large networks in particular, a WLC cluster provides numerous advantages:

- Automatic network "load balancing" between the individual APs and WLCs;
- Increased failover reliability through the provision of backup WLCs ("hot standby") and automatic redistribution of the APs in the case of a WLC failure;
- Setting up a certificate hierarchy: Management of certificates by a central certification authority (CA), represented either by a master WLC or an external station (such as a server).

As of LCOS 9.00, the cluster function received numerous enhancements described below.

Enabling/disabling CAPWAP in the WLC

In order to operate multiple WLCs in a cluster, they must all have identical configurations. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master WLC's configuration.

Learn more about mirroring a configuration in the section [Config-Sync](#).

WLC tunnel for internal communication

The use of WLC tunnels is essential for a WLC cluster. The WLCs in the WLC cluster use this tunnel to communicate with one another and keep their status information aligned. With the feature extensions as of LCOS 9.00, the way that LCOS deals with WLC tunnels is also improved:

- WLCs are able to find one another automatically.
- You have the option to statically configure WLC tunnels.
- WLCs disconnect a WLC tunnel only after a timeout.
- WLC tunnels can be switched on or off globally.

The settings for the WLC tunnels and other WLCs (remote WLCs) are located in the section **WLAN controller > General > WLC cluster**. The setting **WLC tunnel active** allows you to disable the usage of WLC tunnels, which in effect causes the clustering feature to be switched off.

Finding the ideal WLC

The algorithms implemented in LCOS ensure that the APs are intelligently distributed between the individual WLCs. This allows the APs to equally distribute the network load between all of the WLCs in a cluster, or to select an alternative WLC if one should fail. For this, an AP first sends out a discovery request on the network to identify all available WLCs. The WLCs then respond with a discovery response which an AP uses to create a prioritized list of WLCs. This AP prioritizes the list based on various criteria.

An AP works through the different criteria sequentially: If multiple WLCs appear to be ideal candidates after applying a criterion, the AP uses the next criteria to prioritize. This process ends when a WLC finally identifies just one WLC as being ideal after the prioritization described in the following.

Criteria for prioritization

- **Specificity of the AP configuration:** An AP evaluates whether a WLC can provide it with a configuration, and whether this contains a specific AP profile or a default profile. The AP prioritizes a specific AP profile as highest, followed by a default profile. If a profile is missing, it is given the lowest priority.
- **The preference value:** The AP evaluates the preference value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

If there still remain several WLCs which are considered to be ideal, the prioritization process continues by evaluating the connection status and the type of selection process (automatically vs. manually initiated):

- When the **calculation is triggered for the first time**, an AP calculates a weighted value for each of the remaining WLCs by taking the number of APs connected to each WLC and comparing this with the maximum possible number of APs (**license usage**). Ultimately, the ideal WLC is taken as that with the lowest license usage.



If a WLC has reached the maximum possible number of AP connections (license quota exhausted), an AP no longer considers the affected WLC for the current selection.

- In the case of **automatic checking** of the ideal AP distribution, an AP stays with the WLC it is connected to if this WLC is included in the list of the remaining WLCs. Otherwise, a **randomized algorithm** causes the AP to select an arbitrary AP.
- In the case of a **manually triggered check**, a **randomized algorithm** ensures that the APs distribute the available license quotas as evenly as possible across the network.

Determining the ideal AP distribution

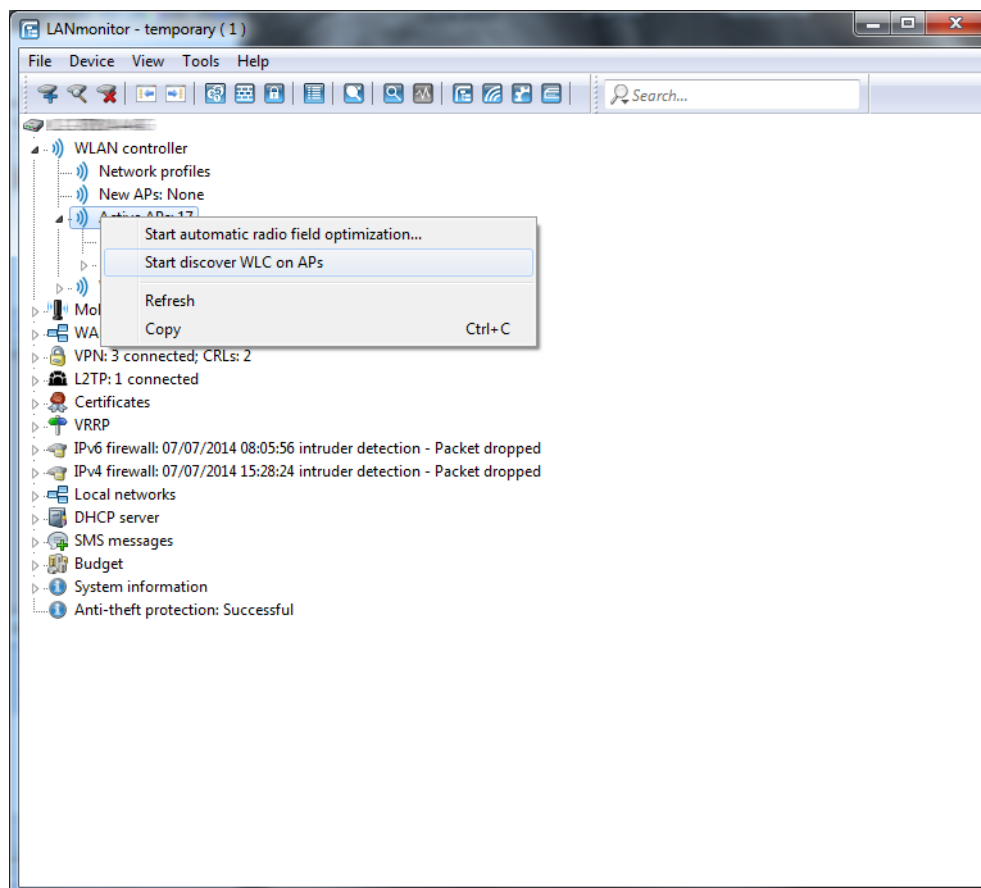
The identification of the ideal AP distribution in a WLC cluster and any redistribution that may be triggered by it occur automatically. Every AP automatically performs the *Finding the ideal WLC* process at irregular intervals between 30 and 60 minutes. If the result of the process is positive for the WLC which is already connected, no redistribution takes place. If a different WLC has a higher priority, the AP attempts to connect to this WLC.

However, as an administrator you can use LANmonitor to manually trigger a calculation of the ideal AP distribution and the resulting redistribution of the APs (see *Manually initiate ideal AP distribution* on page 117).

Manually initiate ideal AP distribution

The following steps show you how to start the recalculation of an ideal distribution, and if necessary to trigger a redistribution.

1. Start LANmonitor and select a WLC.
2. Navigate to the menu item **Wireless LAN > Active APs**.
3. Open the context menu on any AP and select **Start WLC search on APs**.



The access points each find their optimum WLC and distribute themselves across the WLC cluster according to the specifications.

Setting up a CA hierarchy

In order to operate multiple WLCs in a WLC cluster, they all need to have identical configurations. This also includes the certificates used within the WLC cluster. The solution lies in establishing a certificate hierarchy, also known as a CA hierarchy: This involves defining the CA of a WLC as the root-CA. The other WLCs retrieve this certificate for their (sub-) CA.

The following scenario shows you the configuration steps which are necessary for setting up a CA hierarchy. As examples, the configuration is done using two WLCs:

- WLC-MAIN represents the device with the root-CA;
- WLC-SUB is the device which obtains a certificate from the root-CA in order to issue further certificates as a sub-CA.

Configuring the root-CA

The following section describes how to set up a root CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup > Certificates > SCEP-CA > CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

Example: /CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE

3. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Operating** to **Yes**.

You have now completed the configuration of the root CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly.

Configuring the sub-CA

The following section describes how to set up a sub-CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Root-CA** to **No**.
3. Navigate to the menu **Setup > Certificates > SCEP-CA > CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

Example: /CN=WLC-SUB CA/O=LANCOM SYSTEMS/C=DE

4. Switch to the menu **Setup > Certificates > SCEP-CA > Sub-CA** and enter the distinguished name of the root-CA under the parameter **CADN**.

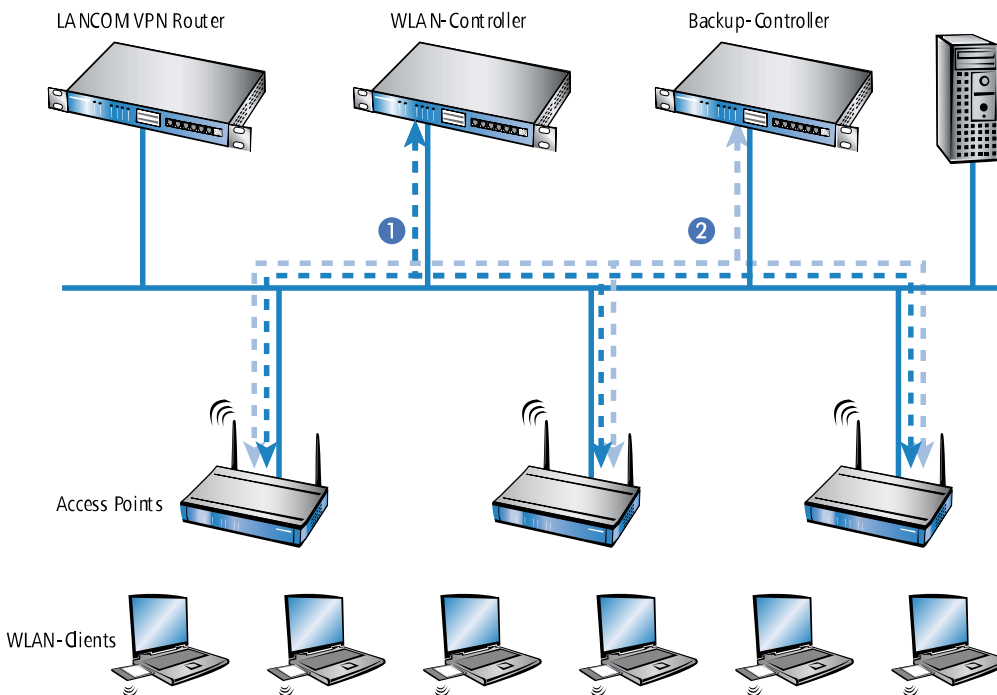
Example: /CN=WLC-MAIN CA/O=LANCOM SYSTEMS/C=DE

5. For the parameter **Challenge-Pwd**, enter the challenge password that is stored on WLC-MAIN under **Setup > Certificates > SCEP-CA**.
6. Enter the URL (address) to the root CA in the **CA-Url-address** parameter.
If another WLC with the LCOS operating system provides the root CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached. Example:
`http://192.168.1.1/cgi-bin/pkiclient.exe`.
7. Optional: Specify the **Ext-Key-Usage** and **Cert-Key Usage** to restrict the functions of the sub-CA. For more information, see the Menu Reference Guide.
8. Set the parameter **Auto-generated-request** to **Yes** to activate the sub-CA.
9. Navigate to the menu **Setup > Certificates > SCEP-CA** and set the parameter **Operating** to **Yes** to enable the CA server with SCEP.

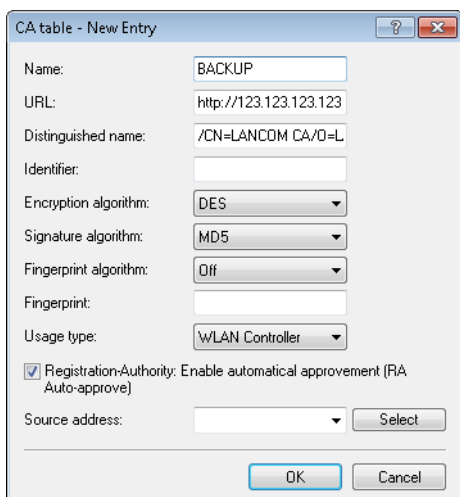
You have now completed the configuration of the sub-CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly. The hierarchy of certificates must be visible here: The WLC first displays the certificate of the root CA and then the certificate of the sub-CA.

1.14.2 Backup with redundant WLAN controllers

This is worthwhile for backing up a WLC with a second WLC, the aim being to maintain full control over all managed APs at all times. The backup WLC is configured in such a way that it obtains the necessary certificates from the backed-up primary WLC via SCEP.



1. Set the same time on the two WLCs 1 and 2.
2. Switch off the CA on the backup WLC (WEBconfig: LCOS menu tree > Setup > Certificates > SCEP-CA > SCEP-Operating).
3. In the configuration of the SCEP client in the backup WLC, create a new entry in the CA table (in LANconfig under **Certificates > SCEP client > CA table**). The CA of the primary WLC is entered here.



4. The URL is to be entered as the IP address or the DNS name of the primary WLC followed by the path to the CA /cgi-bin/pkiclient.exe. For example 10.1.1.99/cgi-bin/pkiclient.exe'.
 - > **Distinguished-Name:** Standard name of the CA (/CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE) or the name given on the primary Controller

1 WLAN management

- > Enable **RA auto-approve**
- > **Usage type:** WLAN controller

5. Then create a new entry in the certificate table with the following information:

- > **CA-Distinguished-Name:** The standard name under which the CA is entered, e.g. /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE
 - > **Subject:** Specification of the primary WLAN controller's MAC address in the form: /CN=00:a0:57:01:23:45/O=LANCOM SYSTEMS/C=DE
 - > **Challenge password:** The general challenge password of the CA on the primary WLAN controller or a password for the Controller specified manually.
 - > **Extended key usage:** critical,serverAuth,1.3.6.1.5.5.7.3.18
 - > **Key length:** 2048 bits
 - > **Usage type:** WLAN controller
6. If a SCEP configuration was previously active on the backup controller, the following actions must be executed under WEBconfig (**LCOS Menu Tree > Setup > Certificates > SCEP client**):
- > Clear-SCEP-Filesystem
 - > Update (2x: the first time, the SCEP client retrieves the new CA/RA certificates only; the second time the device certificate is updated)
7. Configure the first WLC **1** according to your requirements with all profiles and the associated AT table. The APs then establish connections to the first WLC. Each AP receives a valid certificate and a configuration for the WLAN module from the WLC.
8. Transfer the configuration from the first WLC **1**, for example using LANconfig, to the backup controller **2**. The profiles and the AP tables with the MAC addresses of the APs are transferred to the backup WLC at the same time. All APs remain logged on to the first WLC. Once the configuration is transferred, you need to give the backup controller a new IP address.

Should WLC **1** fail, the APs will automatically search for another WLC and they will find the backup WLC **2**. Because this has the same root certificate, it is able to check the validity of the APs' certificates. Because the APs are also entered into the backup WLC's AP table along with their MAC addresses, the backup WLC can fully take over the management of the APs. Changes to the WLAN profiles in the backup WLC will directly affect the managed APs.

-
- ! In this scenario, the APs remain under the management of the backup WLC until this itself becomes unavailable or is manually disconnected.
-
- ! If the APs are set up for standalone operation they will remain operational while searching for a backup WLC, and the WLAN clients will remain associated.

1.14.3 Backup with primary and secondary WLAN controllers

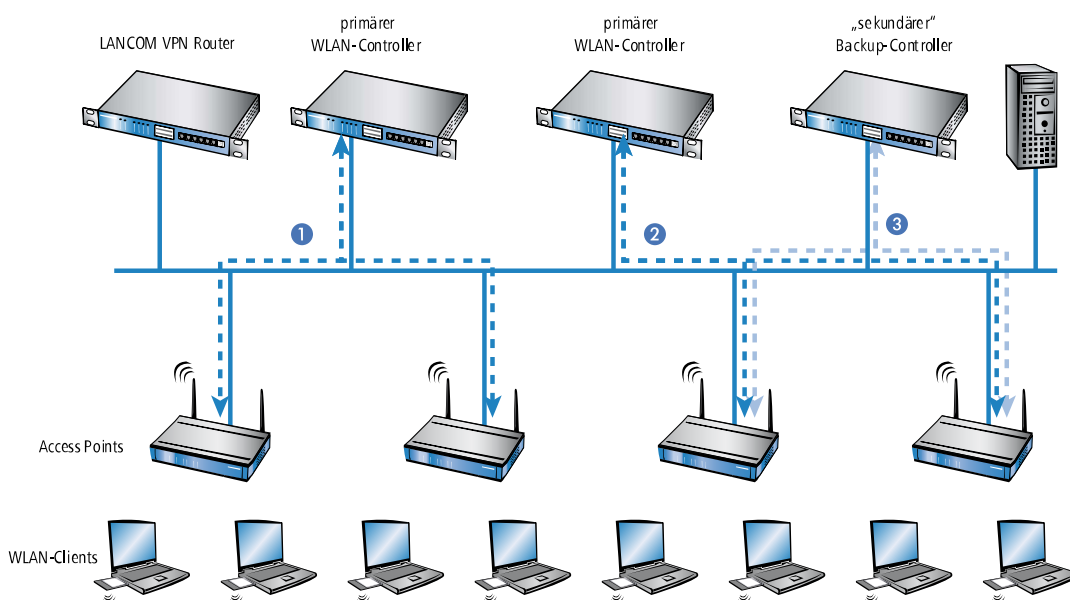
This second type of backup you can provide a larger number of "primary" WLCs with one common "secondary" backup WLC. In case a WLC should fail, the APs remain operational but they work with the current configuration of the WLAN modules. As a secondary WLC, the backup WLC cannot assign any configuration changes to the APs.

1.14.4 Primary and secondary controllers

The establishment of a WCL/AP connection is always initiated by the AP. An AP in managed mode will search the LAN for a WLC that will provide it with a configuration. During this search the AP may find various suitable WLCs:

- > The WLC can authenticate the **certificate** in the AP and it has a **configuration** stored for the MAC address of the AP. A WLC of this type is described as a "primary" WLC.
- > A WLC can authenticate the **certificate** of an AP, but it has **neither a configuration** stored for the MAC address of the AP, **nor does it have a default configuration**. A WLC of this type is described as a "secondary" WLC.

This is an example of a backup solution with three WLCs for 50 managed APs: Two of the WLCs each manage 25 APs and the third is available as a backup WLC:



! A WLC is now able to accommodate five times the maximum number of APs that it can manage by itself. For each five WLCs (identical models), just one additional WLC is sufficient to provide a full backup WLC in case of failure.


1. Set the same time on all of the WLCs **1**, **2** and **3**.
2. Transfer the CA and RA certificates from the first primary WLC **1** to the second primary WLC **2** and to the secondary "backup WLC" **3**.
3. Configure the first WLC **1** according to your requirements with the profiles and the associated AP table for one half of the APs. This WLC becomes the primary WLC for the APs entered into it.


! For a backup solution using a secondary WLC, be sure to set the time for standalone operations such that the AP has time to find a backup WLC. This is because the backup WLC is not able to provide a new configuration for the AP.

Once the AP has established a backup connection to a secondary WLC the countdown until expiry of standalone operation is halted. The AP and its WLAN networks remain active as long as there is a connection to a WLC.

1. Configure the second WLC **2** for the other half of the APs, which subsequently treat this WLC as their primary WLC.
2. For the backup WLC **3** the time and the root certificates are set up only. No further configuration is required.

3. After being started, the APs search for a WLC by emitting a discovery message. In this case, all three WLCs respond to this message—the APs select "their" primary WLC for the DTLS connection that follows. One half of the APs decides on WLC **1** and the other half chooses WLC **2**. Because WLC **3** does not function as primary WLC for any of the APs, none of the APs log on to it.
4. Should WLC **2** fail, the APs will automatically search for another WLC. They discover the WLC **A** and **C**, whereby **A** is already under full load with its 25 APs. Backup controller **C** is able to check the validity of the certificates, i.e. it can authenticate the APs and accept them as managed APs. However, because the APs are **not** entered with their MAC numbers into the backup WLC's AP table, the backup WLC cannot manage the APs any further; they simply continue to operate with their current WLAN configurations.

 If WLC **A** is not under full load, for example because some of "its" APs are switched off, then some of the searching APs could log on here. WLC **A** remains a "secondary" controller for these APs because it does not have their configuration profiles. If in this case one of the APs with an entry in the AP table of WLC **A** is switched on again, then **A** accepts this reactivated AP and, in exchange, it disconnects one of the backup-event APs.

 If the APs are set up for standalone operation they will remain operational while searching for a backup WLC, and the WLAN clients can continue to use all of their functions.

1.14.5 Automatic search for alternative WLCs

As of LCOS 9.00, an AP no longer attempts to reconnect to the last known WLC in case of a disconnection. Instead, the AP searches in the network for an available WLC which corresponds to the criteria for the [Finding the ideal WLC](#).

1.14.6 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.


These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in LCOS. If you cannot wait until the individual services request new certificates, a manual resolution requires deleting the SCEP files from the LCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, LCOS performs the necessary steps automatically.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup > Certificate > SCEP-CA > CA certificate**. This action generates a ZIP file within the LCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password, unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **Extras > File management > Download certificate or file > SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **Extras > File management > Upload certificate or file > SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.

 If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action [2.39.2.2.11 Restore-certificates-from-Backup](#) in order for the device to restore the certificate record.

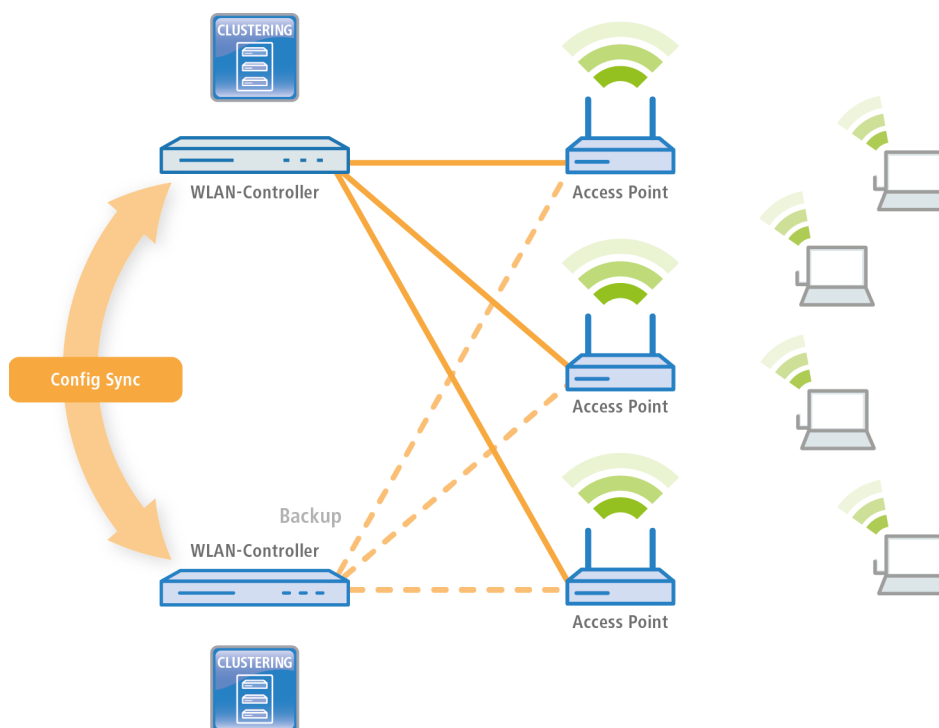
1.15 Automatic configuration synchronization (Config Sync) with the LANCOM WLC High Availability Clustering XL option

Example application, WLAN controllers:

WLAN infrastructures have become an integral part of modern corporate networks. In the age of the "all wireless office", the increasing demands on the availability of a WLAN solution make it essential to have a reliable backup and high-availability solution. In WLAN infrastructures with a single WLAN controller, any failures or maintenance downtimes (such as a firmware update) of the WLC until now caused the APs connected to it to switch to standalone operation. Consequently, the APs in standalone mode were no longer able to access the features that are provided centrally by the WLC such as a Public Spot, IEEE 802.1X authentication, or Layer-3 tunnels.

In order to avoid this and to maintain the full operation of all WLAN capabilities even if a WLC should be temporarily unavailable, one or more redundant or backup WLCs should be employed. In the backup event, the APs automatically switch from the temporarily unavailable WLC to a backup WLC. The backup WLC has the same configuration (e.g. AP table or WLAN profiles) as required by the primary WLC of the APs. The initial setup of the WLCs and any subsequent configuration changes must be carried out separately and identically on each device—a huge effort for the administrator. Manual maintenance of the configurations between multiple identical devices could lead to outdated or non-synchronous configurations on the backup WLCs, which in the case of a backup event could lead to a critical state for the entire WLAN infrastructure. The resulting troubleshooting usually turns out to be a real challenge. The users of the WLAN clients experience a loss of productivity, which could have major consequences company-wide.

New with the LANCOM WLC High Availability Clustering XL option: This software option allows multiple WLCs to be grouped into a highly-available cluster. In this way, configuration changes, features and enhancements made on one WLC are automatically transferred between the other WLCs in the cluster, without having to make manual changes on each individual device. Common parameters in a cluster (e.g. WLAN profiles, AP tables, or Public Spot settings) remain synchronized, individual parameters (such as the IP address of the WLC) are not exchanged.



The LANCOM WLC High Availability Clustering XL option offers greatly simplified administration and huge time savings because you only need to configure one WLC in the cluster. The WLC then transfers the changes to the other cluster devices automatically. In the case of maintenance downtime (e.g. for a firmware update) or even the failure of a WLC,

1 WLAN management

the APs automatically connect to another WLC which, thanks to Config Sync, already has the identical configuration without any intervention by the administrator. The result is a convenient way to high availability.

The prerequisites for a device to be a valid member of a cluster are:

- > The LANCOM WLC High Availability Clustering XL option (as of LCOS version 9.10) must be available.
- > IP communications must be available to all other devices, e.g. via LAN, WAN, or VPN.
- > It must be in the list of group members that is stored in each device.
- > A valid certificate must be available
- > It needs to authenticate itself by certificate as a member of the cluster.

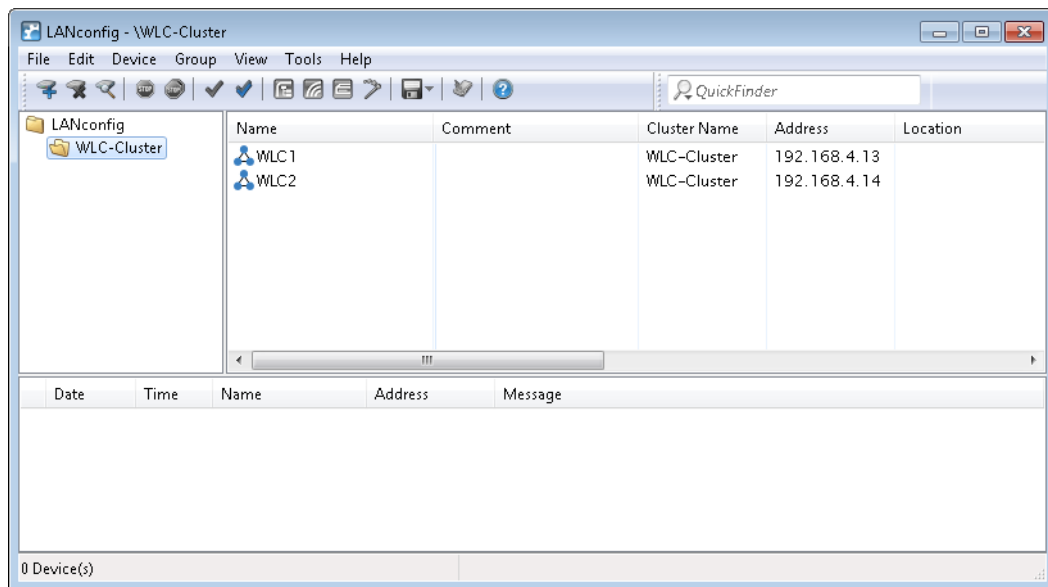
1.15.1 Special LANconfig icon for devices in a cluster or using Config Sync

LANconfig has a specific icon to mark devices that share their configuration via Config Sync. Furthermore, the **Config Cluster** column shows the configuration group for each device. LANconfig is thus able to sort and edit the device listing according to cluster name.

If you try to make changes to the configuration of a cluster member, you will receive following warning:

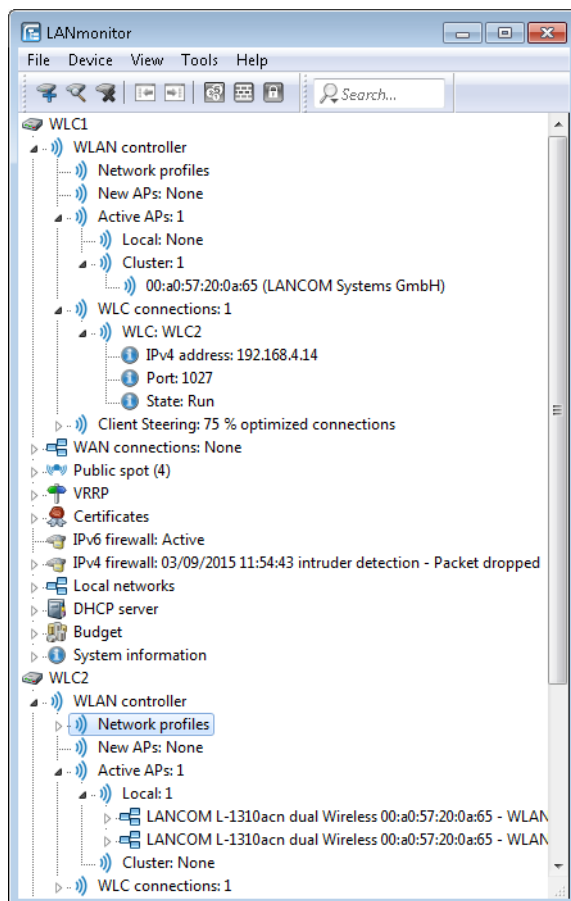
"This device belongs to the Config Cluster: [cluster name]. Editing this configuration also affects the following devices: [Listing of all devices in the same cluster]"

You can bypass this message if necessary. To do this, enable the option **Don't show again** in the displayed window.



1.15.2 Special LANmonitor icon for devices in a cluster or using Config Sync

LANmonitor has a specific icon to mark devices that share their configuration via Config Sync. Also, the name of the configuration group (cluster name) is shown after the device name. LANmonitor thus makes it easier to see which devices share the same configuration.



2 Appendix

2.1 Overview of CAPWAP parameters with the show command

The following information about the CAPWAP service can be viewed using the command line:

Table 3: Overview of all CAPWAP parameters with the show command

Parameters	Meaning
-addresses [<IfcNum>]	Shows the address tables of an individual or all WLC tunnels. In the case of an individual WLC tunnel, enter for the <IfcNum> the number of logical WLC tunnel interface, for example 10.
-groups	Shows the information for an individual or all available assignment/tag groups.

You can supplement the command `show capwap groups` with the parameters listed below, which control the scope of the displayed information:

Table 4: Overview of all CAPWAP group parameters with the show command

Parameters	Meaning
all	Shows the names configured in the setup menu and the device's internal names for all assignment/tag groups as well as the default groups that were set up. The default group represents an internal group which contains all APs.
<group1> <group2> <...>	Shows all APs of the respective assignment/tag groups.
-l <location>	Shows all APs of the respective location.
-c <country>	Shows all APs of the respective country.
-i <city>	Shows all APs of the respective city.
-s <street>	Shows all APs of the respective street.
-b <building>	Shows all APs of the respective building.
-f <floor>	Shows all APs of the respective floor.
-r <room>	Shows all APs of the respective room description.
-d <device>	Shows all APs that have the specified device name.
-v <firmware>	Shows all APs which have the specified firmware. To do this, enter the version number for <firmware> followed by the build number, e.g., 9.00.0001.
-x <firmware>	Shows all APs with a firmware version lower than the one installed on the current device.
-y <firmware>	Shows all APs with a firmware version the same or lower than the one installed on the current device.
-z <firmware>	Shows all APs with a firmware version higher than the one installed on the current device.

Parameters	Meaning
-t <firmware>	Shows all APs with a firmware version the same or higher than the one installed on the current device.
-n <intranet>	Shows all APs with an IP belonging to the specified Intranet address.
-p <profile>	Shows all APs that have been assigned with the specified WLAN profile.
rmgrp <group1 intern_name> <group2 intern_name> ...	Deletes the group(s) with the specified internal names from the memory of the device. Use this command to free up the main memory if too large a number of groups is degrading the performance of the device. The entry in the setup menu is unaffected by this action.
resetgrps	Deletes all groups except the default group.

For location information the device evaluates the information entered under **Location** in the access point table. The following field names are available:

- > co=Country
- > ci=City
- > st=Street
- > bu=Building
- > fl=Floor
- > ro=Room

For instance, the location entry `co=Germany, ci=Aachen` allows you to list all of the managed APs in Aachen from the console of the WLC with the command `+show capwap group -i Aachen`.

Example commands

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion ...
```