



... connecting your business

## Centralized WLAN Management

- LANCOM WLAN Controller
- LANCOM WLC Option for Router

**LANCOM**  
Systems

# Contents


1 Centralized WLAN Management.....	4
1.1 Starting position.....	4
1.2 Technical concepts.....	4
1.2.1 The CAPWAP standard.....	4
1.2.2 Smart controller technology.....	5
1.2.3 Communication between access point and WLAN controller.....	7
1.2.4 Zero-touch management.....	8
1.2.5 Split management.....	8
1.3 Configuration.....	9
1.3.1 Configuring the access points.....	9
1.3.2 Configuring the WLAN Controller.....	10
1.3.3 List of access points.....	22
1.3.4 Stations.....	23
1.3.5 Options for the WLAN controller.....	25
1.4 Tutorial: Virtualization and guest access accounts via the LANCOM WLAN controller.....	29
1 Wireless LAN configuration of the WLAN controllers.....	29
2 Configuring the switch.....	31
3 Configuring the IP networks in the WLAN controller.....	33
4 Configuring Public Spot access.....	35
5 Configuring the RADIUS server to operate a Public Spot.....	38
6 Configuring Internet access for the guest network.....	39
1.5 Access point administration.....	40
1.5.1 Accepting new access points into the WLAN infrastructure manually.....	40
1.5.2 Manually removing access points from the WLAN infrastructure.....	42
1.5.3 Deactivating access points or permanently removing them from the WLAN infrastructure.....	43
1.6 Central firmware and script management.....	44
1.6.1 General settings for firmware management.....	45
1.7 WLAN layer-3 tunneling.....	47
1.7.1 Introduction.....	47
1.7.2 Tutorials.....	48
1.8 RADIUS.....	60
1.8.1 Checking WLAN clients with RADIUS (MAC filter).....	60
1.8.2 External RADIUS server.....	61
1.9 Dynamic VLAN assignment.....	62
1.10 Activating 802.1x accounting for logical WLANs in WLAN controllers.....	64
1.11 Displays and commands in LANmonitor.....	65
1.12 Automatic RF optimization.....	66
1.13 Channel-load display in WLC mode.....	68
1.14 Backing up the certificates.....	68
1.14.1 Create backups of the certificates.....	68

1 Uploading a certificate backup into the device.....	69
2 Backing up and restoring further files from the SCEP-CA.....	69
1.15 Backup solutions.....	70
1 Backup with redundant WLAN controllers.....	71
1.15.1 Backup with primary and secondary WLAN controllers.....	72
1.15.2 Primary and secondary controllers.....	72

# 1 Centralized WLAN Management

LANCOM WLAN controllers and LANCOM routers with WLC option provide a centrally controlled WLAN management for larger-scale WLAN infrastructures. The WLAN controller centrally stores the configurations of individual access points as profiles and distributes these to the appropriate devices.

---

 This documentation will use "WLAN Controller" as a generic term for LANCOM WLAN controllers and LANCOM routers with WLC option.

## 1.1 Starting position

The widespread use of wireless access points 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 wireless access points must be configured and require appropriate monitoring in order to recognize unwelcome WLAN clients, etc. The administration of the access points, 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 access points 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 access points to avoid frequency interference and optimize network performance.
- In public places, access points 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 access points 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 access points is then no longer carried out in the devices themselves but by a central authority instead, the WLAN controller. The WLAN controller authenticates the access points 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 access points simultaneously. Optionally the configuration provided by the WLAN controller is **not** stored in the access point's flash memory but in RAM, so security-related data cannot fall into the hands of unauthorized persons in the event of theft of a device. 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 The CAPWAP standard

The CAPWAP protocol (Control And Provisioning of Wireless Access Points) introduced by the IETF (Internet Engineering Task Force) is a draft 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 WLAN controller and the access point.

ⓘ 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.

- Data channel, optionally also encrypted with DTLS. The payload data from the WLAN is transferred through this channel from the access point via the WLAN controller into the LAN—encapsulated in the CAPWAP protocol.

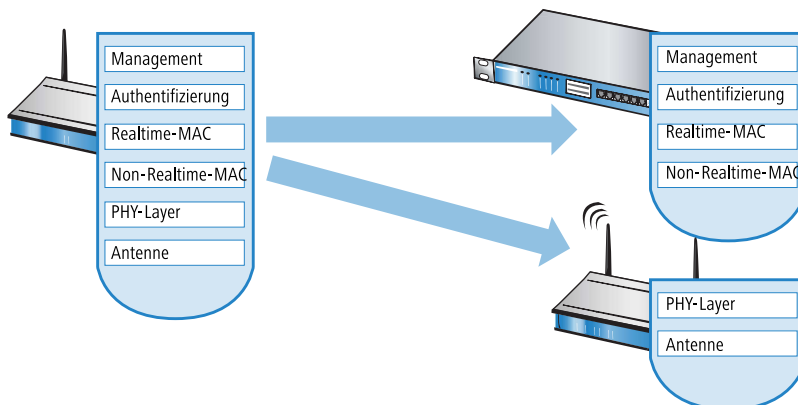
## 1.2.2 Smart controller technology

In a decentralized WLAN structure with stand-alone access points (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 access points. Centralized WLAN management divides these tasks among two different devices:

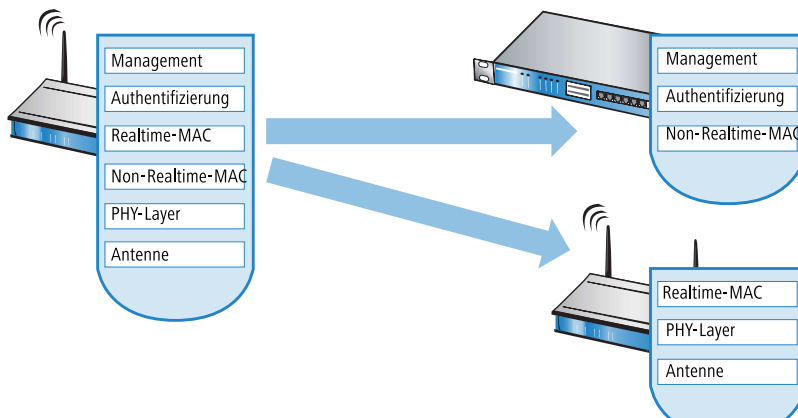
- The central WLAN controller assumes the administration tasks.
- The decentralized access points handle the data transfer at the PHY layer and the MAC functions.
- A RADIUS or EAP server can be added as a third component RADIUS or for authentication of WLAN clients (which can also be the case in stand-alone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

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

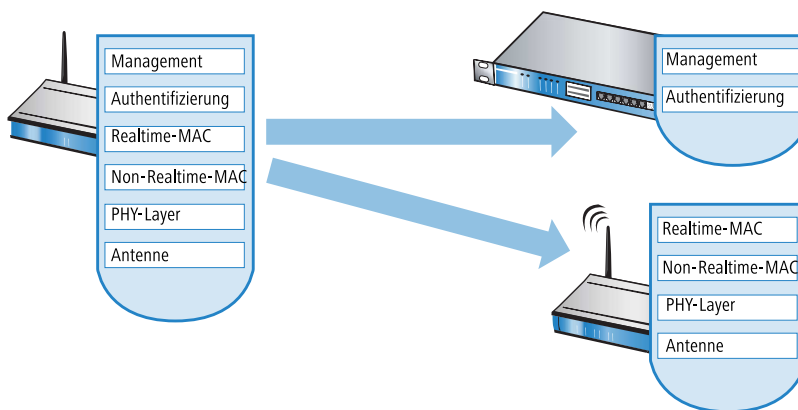
- Remote MAC: In this case, all of the WLAN functions are transferred from the access point to the WLAN controller. Here, the access points only serve as "extended antennas" without independent intelligence.



- **Split MAC:** With this variant, only a portion of the WLAN functions are transferred to the WLAN controller. Normally, real-time applications will continue to be processed in the access point; the non-real-time applications are processed via the central WLAN controller.



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



The technology from LANCOM Systems 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 WLAN controller 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 WLAN controller. In local MAC architectures the data can alternatively be broken out from the access points directly to the LAN to provide high-performance data transfer. WLAN controllers from LANCOM are also suitable for WLANs that work with the draft IEEE 802.11n standard, so offering much higher bandwidths than previous WLAN technologies. 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

LANCOM WLAN controllers also support the transfer of payload data through a CAPWAP tunnel.

- This allows selected applications such as VoIP to be routed via the central WLAN controller, 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 WLAN controller (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 WLAN controller.

## 1.2.3 Communication between access point and WLAN controller

ⓘ As of firmware version LCOS 7.20 there is a difference between LANCOM access points (e. g. the LANCOM L-54ag) and LANCOM wireless routers (e.g. the LANCOM 1811 Wireless) with regard to the ex-factory default settings in the WLAN modules. In the following specifications, the general term access point will be used for the most part.

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

- When shipped, the WLAN modules in LANCOM access points are set to the 'Managed' operating mode. In this mode, LANCOM access points search for a central WLAN controller that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLAN controller or until the operating mode of the WLAN module is changed manually.
- While searching for a WLAN controller, LANCOM access points switch off their WLAN module(s).
- Ex-factory, the WLAN modules in LANCOM wireless routers are set to the 'access point' operating mode. In this mode, LANCOM 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 LANCOM wireless routers has to be switched into the 'managed' mode.

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

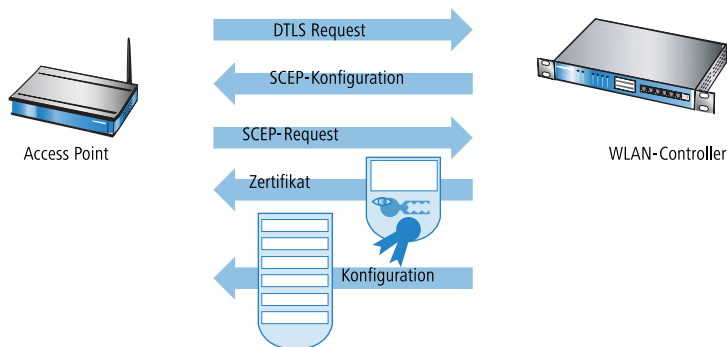
ⓘ The DNS names of WLAN controllers can also be resolved. All access points with LCOS 7.22 or higher have the default name 'WLC-Address' pre-configured so that a DNS server can resolve this name to a LANCOM WLAN controller. The same applies to the DHCP suffixes learned via DHCP. This also makes it possible to reach WLAN controllers that are not located in the same network, without having to configure the access points.

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

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

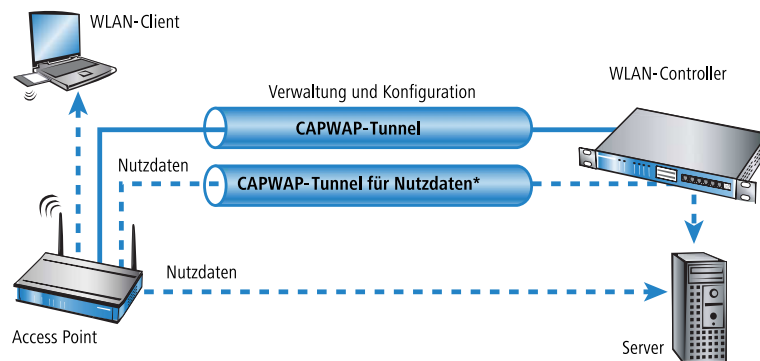
The access point is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the access point uses the SCEP to retrieve its certificate from the SCEP CA. Once this is done, the assigned configuration is transferred to the access point.

! 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 access point's MAC address in the AP table of the WLAN controller. If the access point'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).

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 access point directly into the LAN and transferred, for example, to the server.



## 1.2.4 Zero-touch management

With their ability to automatically assign a certificate and configurations to the requesting access points, LANCOM WLAN controllers implement true "zero-touch management". Simply connect new access points 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.

## 1.2.5 Split management

LANCOM access points can search for their WLAN controller in remote networks—a simple IP connection, such as via a VPN path, is all you need. As the WLAN controllers only influence the WLAN part of the configuration in the access point, all of the other functions can be managed separately. This division of the configuration tasks makes LANCOM WLAN controllers perfect 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.



## 1.3 Configuration

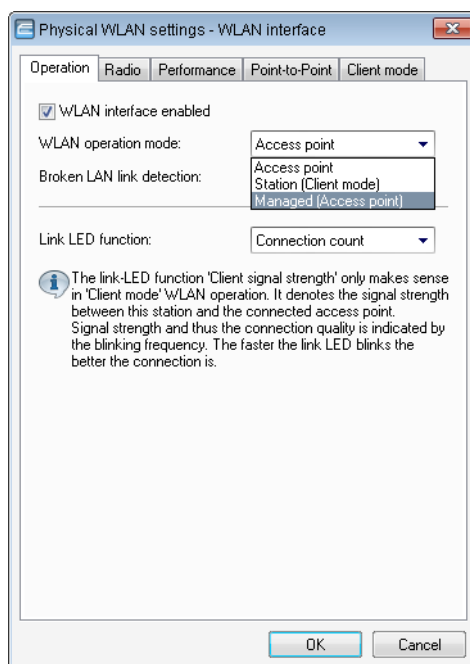
### 1.3.1 Configuring the access points

As of firmware version LCOS 7.20 there is a difference between LANCOM access points (e. g. the LANCOM L-54ag) and LANCOM wireless routers (e.g. the LANCOM 1811 Wireless) with regard to the ex-factory default settings in the WLAN modules.

- When shipped, the WLAN modules in LANCOM access points are set to the 'Managed' operating mode. In this mode, LANCOM access points search for a central WLAN controller that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLAN controller or until the operating mode of the WLAN module is changed manually.
- Ex-factory, the WLAN modules in LANCOM wireless routers are set to the 'access point' operating mode. In this mode, LANCOM 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 LANCOM 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 WLAN controller.

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
```

## 1.3.2 Configuring the WLAN Controller

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

### General settings

This area is for the basic settings of your WLAN controller.

- Automatically accept new APs (auto-accept)


Enables the WLAN controller to provide all new access points with a configuration, even those not in possession of a valid certificate.

Enables the WLAN controller to provide a certificate to all new access points **without** a valid certificate. One of two conditions must be fulfilled for this:

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

- Automatic provision of the default configuration

This enables the WLAN controller to assign a default configuration to every new access point (i.e. those **without** a valid certificate) even if no explicit configuration has been stored for it. In combination with auto-accept, the LANCOM WLAN controller can accept all managed-mode access points which are found in the WLAN infrastructure managed by it (up to the maximum number of access points that it can handle). Access points that are accepted by default are also entered into the MAC list.

 This option can potentially lead to the acceptance of unintended access points 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 access points:

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

### Basic configuration of the WLAN controller function

To get started, a LANCOM WLAN controller requires the following two pieces of information to carry out the mainly automated configuration of the access points:

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

Further optional examples for configuration include setting up redundant WLAN controllers, the manual disconnection and connection of access points, and backing up any necessary certificates.

### Setting the time information for the LANCOM WLAN controller

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

The LANCOM WLAN controller can only check the temporal validity of these certificates if it is set with the current time.

To set the time in the device start LANconfig, click on the entry for the WLAN controller 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, LANCOM WLAN controllers 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.

For LANCOM WLC-4006 models the time information must be obtained from a time server, as these devices do not have a battery-fed real-time clock.

As soon as the WLAN controller has valid time information it begins with the generation of the certificates (root and device certificate). Once the necessary certificates have been generated, the LANCOM WLAN controller 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](#))

### Creating a default configuration

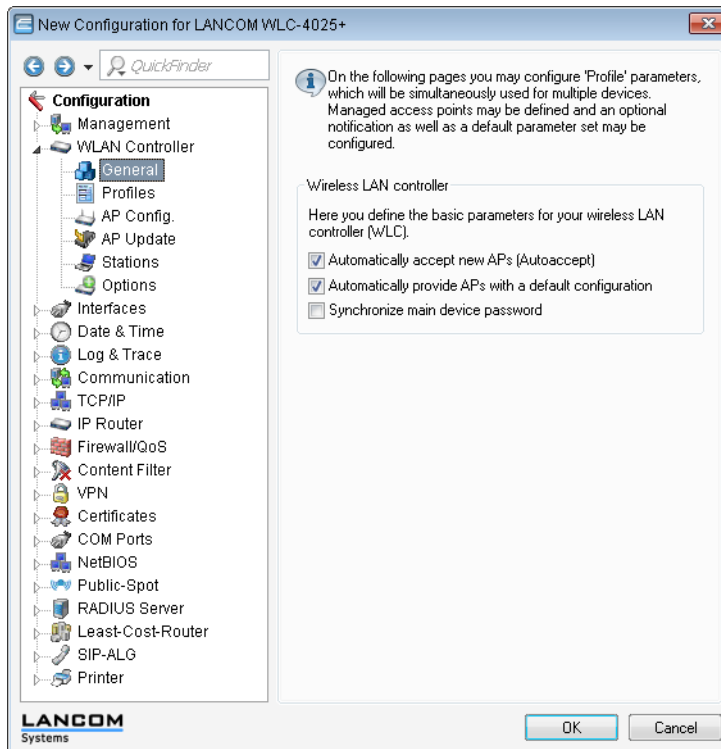
With the time information and the certificates, the LANCOM WLAN controller is ready for operations. If the LAN contains access points in managed mode (standard mode for ex-factory access points or after being reset with LCOS 7.20 or higher; for the manual setting see [Configuring the access points](#)), the WLAN controller soon displays these as "New access points" in LANmonitor. In addition, the New APs LED of the WLAN Controller will blink orange. In case the device comes with a display, it will show the number of new Access Points (New APs).

To be able to provide these new access points with WLAN settings, the LANCOM WLAN controller must contain at least one default configuration that can be provided to the access points that are searching for one.

### Example of a default configuration

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

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



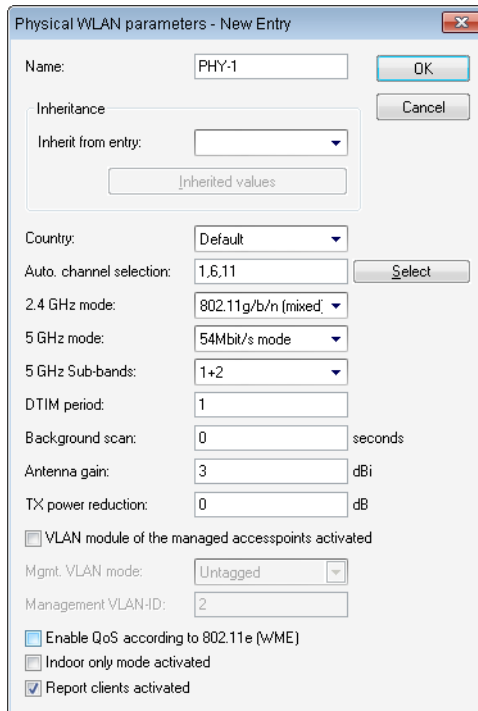
- **Automatically accept new APs (Auto-accept)** Enables the WLAN controller to provide a certificate to all new access points without a valid certificate. To this end, either a configuration for the access point has to be entered into the AP table, or 'Automatically provide APs with a default configuration'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

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

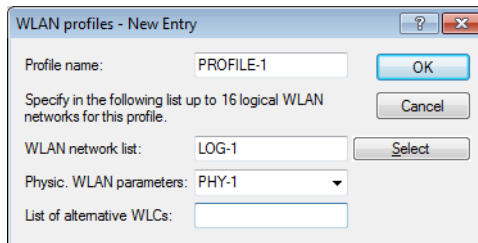
3. On the **Profiles** page, move to the logical WLAN networks. Add a new entry with the following values:

- **Name:** Give the WLAN a name. This name is used only for administrative purposes in the LANCOM WLAN controller.
  - **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 access point 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 an unique name, and assign the above logical WLAN network and physical WLAN parameters to it.



6. Change to the **AP config** 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 access point that is not explicitly listed with its MAC address in this table.

### Configuring the access points

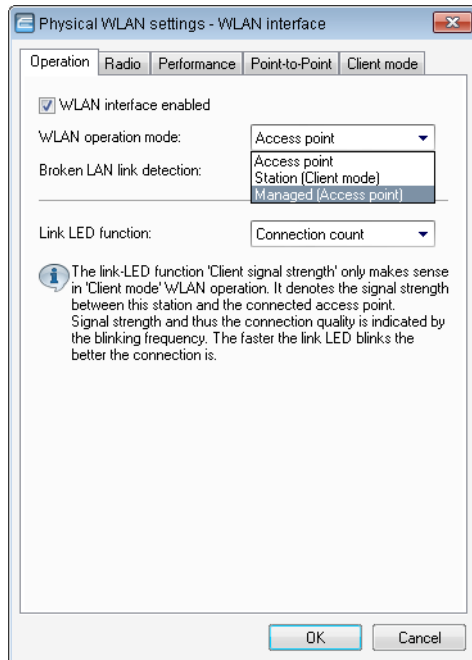
As of firmware version LCOS 7.20 there is a difference between LANCOM access points (e. g. the LANCOM L-54ag) and LANCOM wireless routers (e.g. the LANCOM 1811 Wireless) with regard to the ex-factory default settings in the WLAN modules.

- When shipped, the WLAN modules in LANCOM access points are set to the 'Managed' operating mode. In this mode, LANCOM access points search for a central WLAN controller that can provide them with a configuration, and they remain in "search mode" until they discover a suitable WLAN controller or until the operating mode of the WLAN module is changed manually.
- Ex-factory, the WLAN modules in LANCOM wireless routers are set to the 'access point' operating mode. In this mode, LANCOM 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 LANCOM 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 WLAN controller.

1 Centralized WLAN Management

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
```

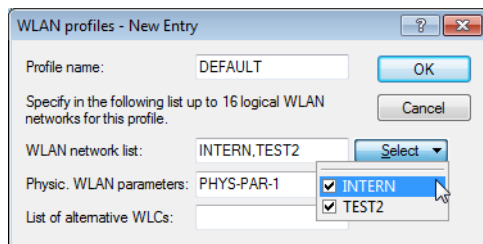
**Profiles**

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 access points. The allocation of WLAN profiles to the access points is set in the AP table.

The following parameters can be defined for every WLAN profile:



LANconfig: **WLAN Controller > Profiles > WLAN profiles**



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

- **Profile name**

Name of the profile under which the settings are saved.

- **WLAN network list**

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

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

- **Physical WLAN parameters**

A set of physical parameters to be used by the access point WLAN modules.

- **IP address of alternative WLAN controllers**

A list of WLAN controllers that the access points should attempt to connect with. The access point starts searching for a WLAN controller with a broadcast. Defining alternative WLAN controllers is worthwhile when a broadcast cannot reach all WLAN controllers (e.g. if the WLAN controller is located in another network).

### Logical WLAN networks

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

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

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

- **Network name**

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

- **Inheritance**

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

- **SSID**

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

- **VLAN-ID**

VLAN ID for this logical WLAN network



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

- **AP standalone time**

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

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

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

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



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



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



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

## Physical WLAN parameters

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

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

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

### ■ Name

Unique name for this combination of physical WLAN parameters.

### ■ Inheritance

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

### ■ Country

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

### ■ Automatic channel selection

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

### ■ Management VLAN ID

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

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

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

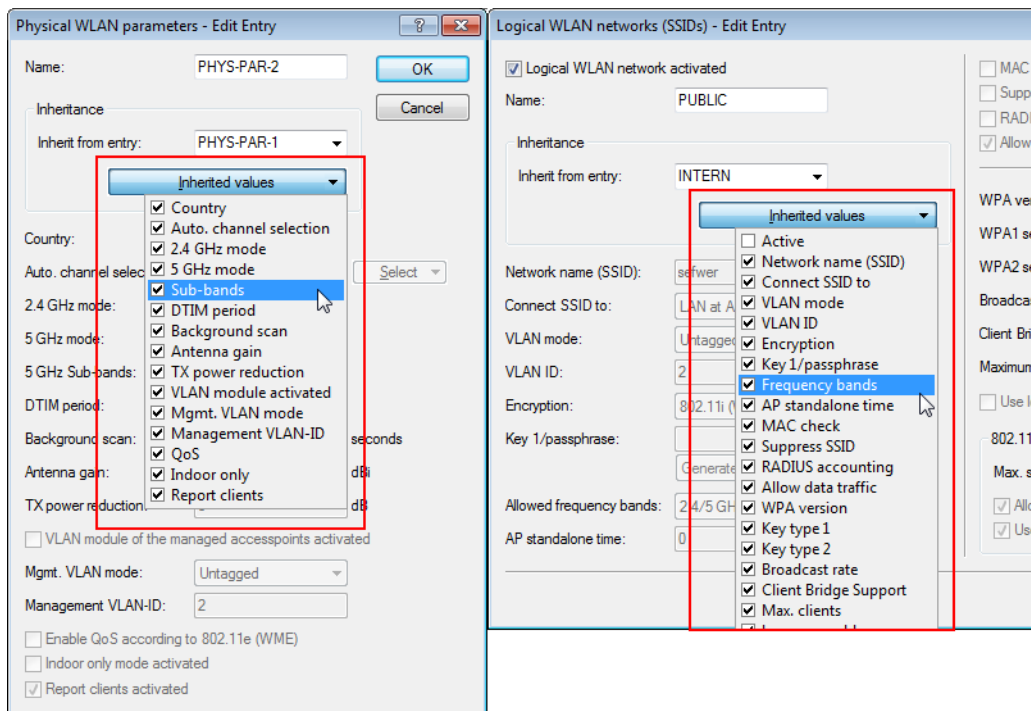
! All other physical WLAN parameters correspond to those for the standard configuration of access points.

### Inheritance of parameters

A LANCOM WLAN controller is capable of managing a large number of different access points at different locations. However, WLAN profiles include settings that are not equally suitable for every type of access point 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. You should initially generate the basic settings that are valid for the majority of the managed access points.
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.

## IP parameter profiles

The profiles defined in this dialog are assigned to access points which should not retrieve an IP address by means of DHCP. This allows you to define precisely the IP parameters to be used by an access point.

The screenshot shows a dialog box titled "IP parameter profiles - New Entry". It has a standard Windows-style title bar with a close button. The dialog contains the following fields and controls:

- Name:** A text input field containing "AP-INTRANET".
- Inheritance:** A section containing a dropdown menu labeled "Inherit from entry:" and a text input field labeled "Inherited values".
- Domain name:** A text input field containing "company.intern".
- Netmask:** A text input field containing "255.255.255.0".
- Default gateway:** A text input field containing "192.168.2.1".
- Primary DNS:** A text input field containing "80.123.254.1".
- Secondary DNS:** A text input field containing "0.0.0.0".
- Buttons:** "OK" and "Cancel" buttons are located on the right side of the dialog.

LANconfig: **WLAN Controller > AP Config. > IP parameter profile**

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

- **Name:** Name of the IP parameter profile

### Possible values

Maximum 31 characters

### Default

Blank

- **Inheritance:** Selection of an IP parameter profile defined earlier and from which the settings are to be inherited (*Inheritance of parameters*).

- **Domain name:** Name of the domain (DNS suffix) which is to use this profile.

### Possible values

Max. 63 characters

### Default

- **Netmask:** Netmask of the profile

### Possible values

Valid netmask

### Default

Blank

- **Default gateway:** The gateway to be used by the profile as standard.

### Possible values

Valid IP address

### Default

Blank

- **Primary DNS:** The DNS (Domain Name System) to be used by the profile.

### Possible values

Valid IP address

**Default**

Blank

- **Secondary DNS:** Second, alternative DNS if the first is unavailable.

**Possible values**

Valid IP address

**Default**

Blank

### 1.3.3 List of access points

The AP table is a central element of the configuration for WLAN controllers. Here, access points are assigned with WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) via their MAC addresses. Furthermore, the existence of an entry in the AP table for an access point affects its ability to connect to a WLAN controller. The following parameters can be defined for every access point:

LANconfig: **WLAN Controller > AP Config. > Access point table**

WEBconfig: **LCOS Menu Tree > Setup > WLAN management > AP configuration > Access points**

- **Update management active**

Activating update management for the access point enables the latest firmware and script versions to be uploaded automatically. All other settings are set under AP update.

- **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.

- **WLAN profile**

WLAN profile from the list of defined profiles.

- **WLAN interface 1**

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

- **Auto. channel selection Ifc 1**

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 just one channel is defined here, then only this channel will be used 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. Channels which are invalid for the frequency band are ignored.

- **WLAN interface 2**

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

- **Auto. channel selection Ifc 2**

Automatic channel selection for the second WLAN module.



Settings for the second WLAN module are ignored if the managed device has only one WLAN module.

- **Encryption**

Encryption of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

- **Double bandwidth**

LANCOM access points compliant with IEEE 802.11n optionally offer the activation of double the bandwidth.

- **Antenna grouping**

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

- **IP address**

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

- **IP parameter profile**

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

## 1.3.4 Stations

The Stations table is used to specify which WLAN clients can associate with the wireless networks provided by the LANCOM access points, which in turn are centrally managed by the WLAN controller. Furthermore, the method offers a convenient way to give each WLAN client an individual authentication passphrase and a VLAN ID.

To use the station table, it is imperative that the RADIUS server is activated in the WLAN controller. 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.

LANconfig: **WLAN Controller > Stations > Stations**

WEBconfig: **LCOS Menu Tree > Setup > WLAN management > Access list**

- **MAC address:** MAC address of the WLAN client for this entry.

**Possible values**

Valid MAC address

**Default**

Blank

- **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.

**Possible values**

Max. 32 characters

**Default**

Blank

- **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, then the passphrases used are those stored for each logical wireless LAN network in the **802.11i/WEP** section (for WLAN controllers, these are defined in the logical WLAN networks (SSIDs)).

**Possible values**

ASCII character string with a length of 8 to 63 characters

**Default**

Blank

- **TX bandwidth limit:** Bandwidth restriction for registering WLAN clients. A LANCOM WLAN device in client mode communicates its setting to the access point when logging on. The base station uses these values to set the minimum bandwidth.

**Possible values**

0 to 65535 kbps

**Default**

0

**Special values**

0: No limit

- **RX bandwidth limit:** Bandwidth restriction for registering WLAN clients. A client communicates its own settings to the base station when logging in. The base station uses these values to set the minimum bandwidth.



**Possible values**

0 to 65535 kbps

**Default**

0

**Special values**

0: No limit



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

- **VLAN-ID:** This VLAN ID is assigned to packets that are received from the client with the MAC address entered here.

**Possible values**

0 to 4096

**Default**

0

**Special values**

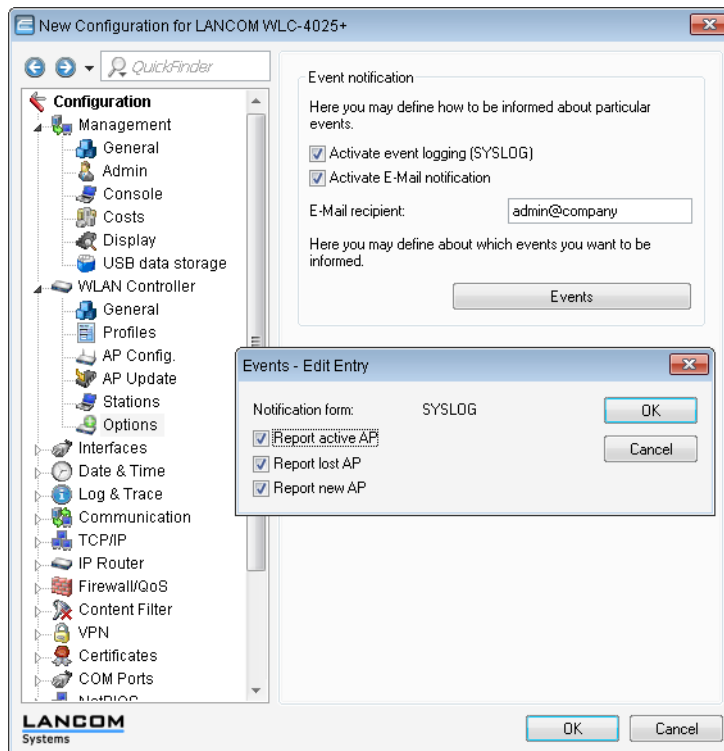
In case of VLAN-ID 0, the station is not assigned a specific VLAN ID. Instead, the VLAN ID for the radio cell (SSID) applies.

### 1.3.5 Options for the WLAN controller

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

## Event notification

Notification can take place via SYSLOG or e-mail. You can define the following parameters:



LANconfig: **WLAN Controller > Options > Event notification**

WEBconfig: **LCOS Menu Tree > Setup > WLAN management > Notification**

### ■ SYSLOG

Activates notification by SYSLOG.

- Possible values: On/off.

### ■ E-mail

Activates notification by e-mail.

- Possible values: On/off.

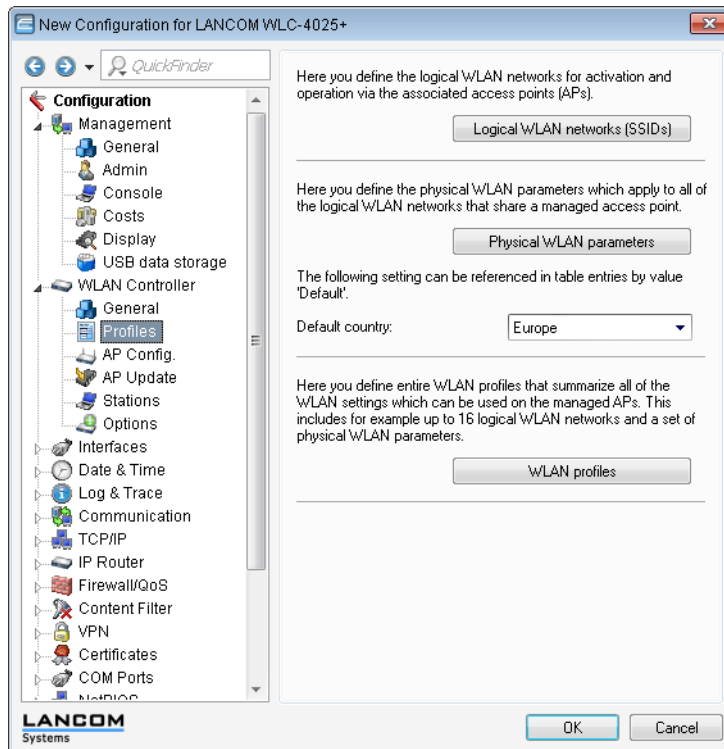
### ■ Events

Selects the events that trigger notification.

- Possible values:
  - ▶ Active access point
  - ▶ Missing access point
  - ▶ New access point

## Default parameters

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



LANconfig: **WLAN Controller > Profiles > Default country**

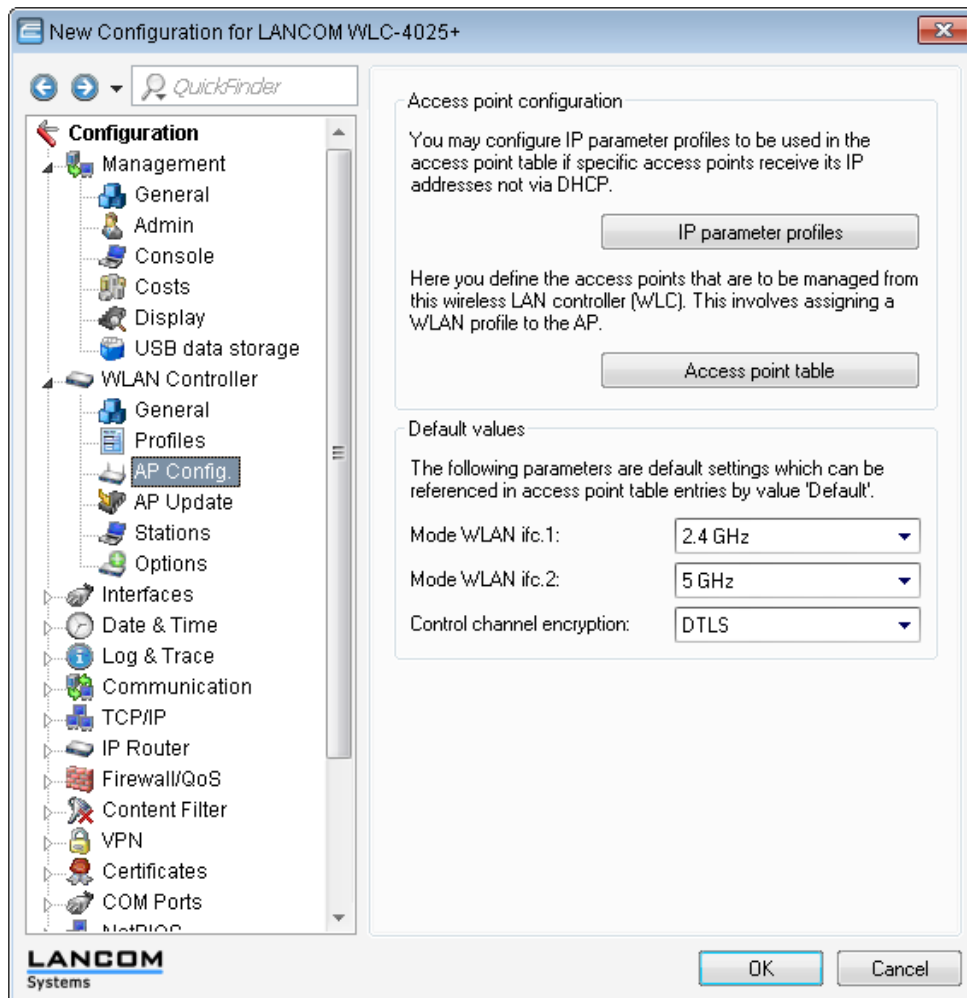
Webconfig: **LCOS Menu Tree > Setup > WLAN Management > AP-Configuration > Country-default**

### ■ 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:

- ▶ Germany



LANconfig: **WLAN Controller > AP config >**

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 of communications over the control channel. Without encryption the control data is exchanged as plain text. In both cases authentication is by certificate.

## 1.4 Tutorial: Virtualization and guest access accounts via the LANCOM WLAN controller

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.

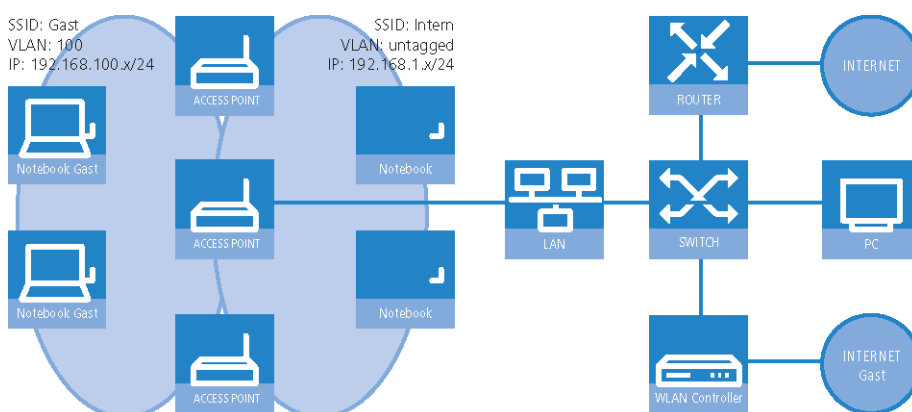
 The Public Spot Option is mandatory for this tutorial.

### Objectives

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



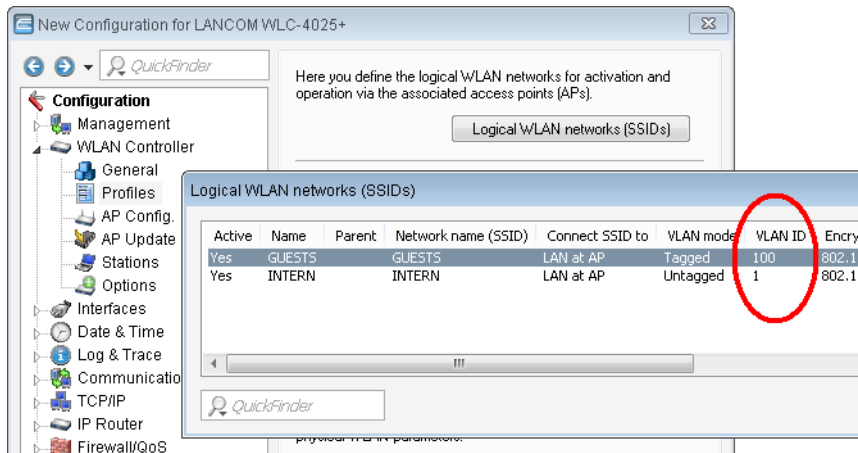
### 1 Wireless LAN configuration of the WLAN controllers

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.

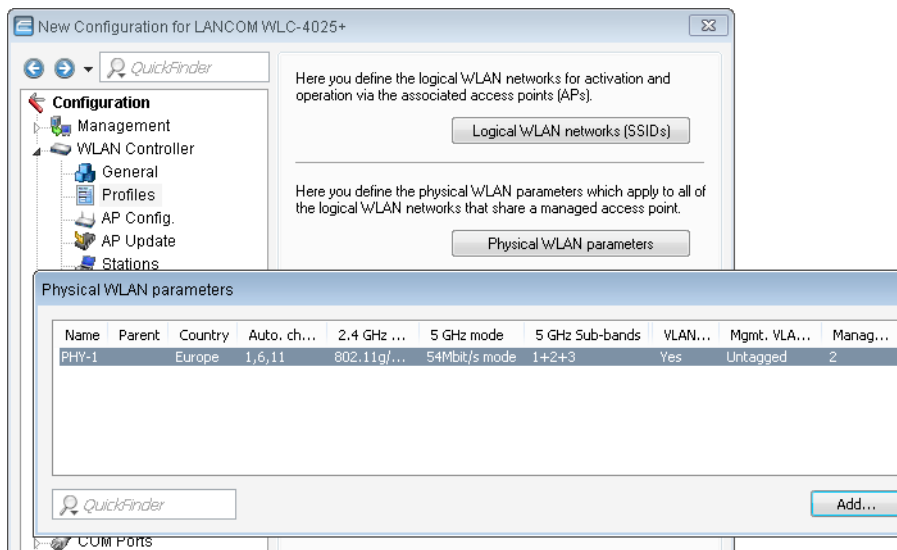
1. Create a logical WLAN for guests and one for the internal employees:

1 Centralized WLAN Management

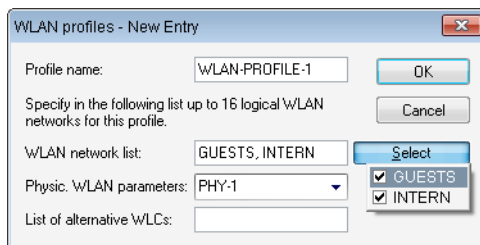
- The WLAN with the SSID 'GUESTS' uses the VLAN ID '100'. No encryption is employed here.
- The WLAN with the SSID 'INTERNAL' uses the VLAN ID '1' (i.e. transmitted to the Ethernet without a VLAN tag), and WPA encryption is employed.



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).



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



- Assign this WLAN profile to the access points managed by the controller. Do this either by entering the individual access points with their MAC addresses or, alternatively, you can use the default profile.

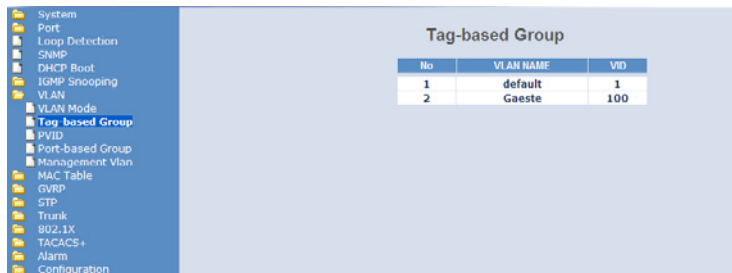
## 2 Configuring the switch

A switch configuration is demonstrated with the example of a LANCOM ES-2126+.

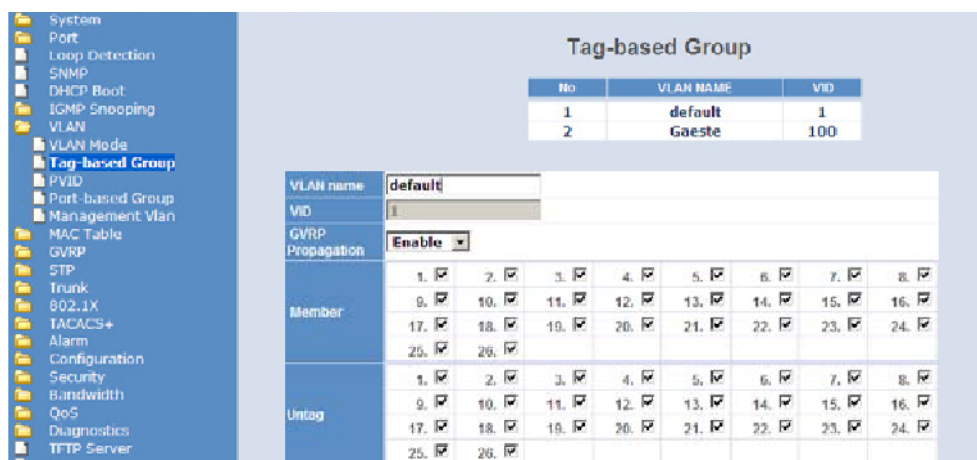
- Set the VLAN mode to &Tag based&, as the access points handle the assignment of VLAN tags.

1 Centralized WLAN Management

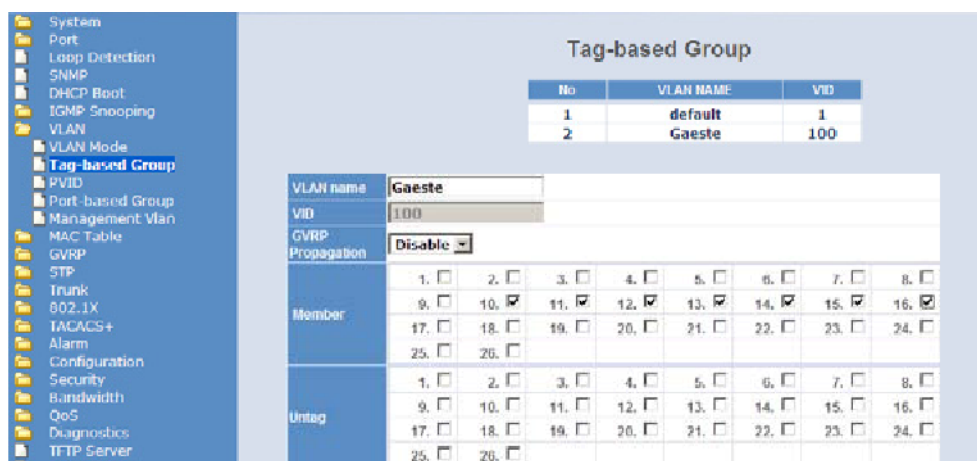
- To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the default group, and a dedicated group is set up for the guests. This is handled with the VLAN IDs entered into the controller when configuring the WLANs.



- The default VLAN is valid on all ports and remains untagged, i.e. the VLAN tags are removed from outgoing data packets from this group.

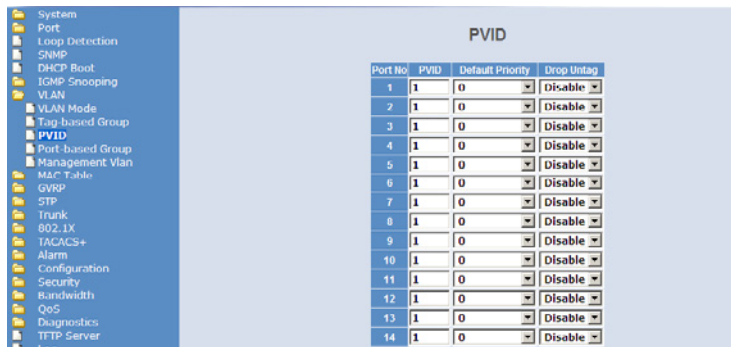


- The guests' VLAN group uses the VLAN ID '100' and is valid only for the ports connected to the WLAN controller and access points (ports 10 to 16 in our example). Tags are not removed from outgoing data packets.





- The port VLAN ID (PVID) is set to '1' for all ports, to assign the ports to the internal network. Untagged packets arriving at these port will be forwarded with the VLAN ID '1'.

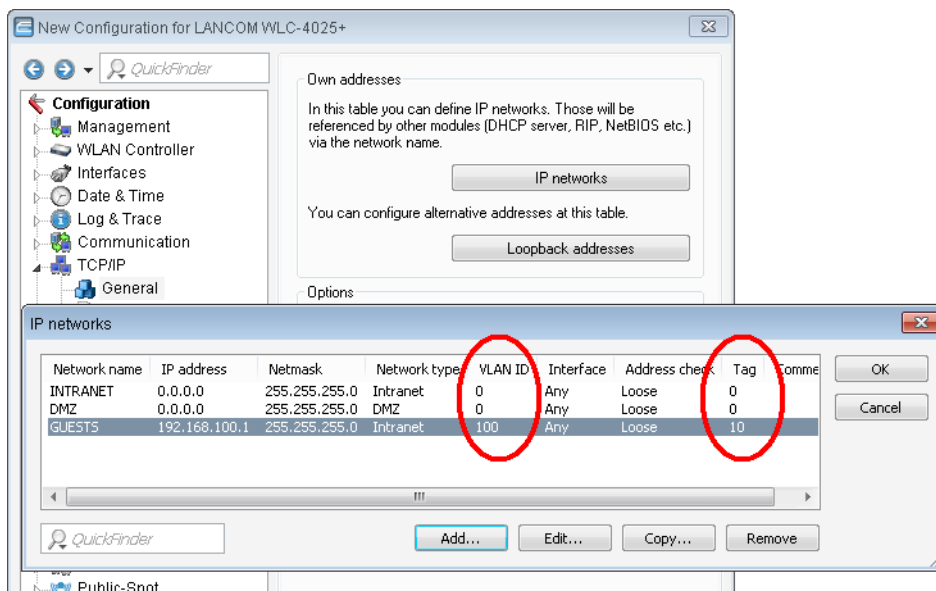


Port No.	PVID	Default Priority	Drop Untag
1	1	0	Disable
2	1	0	Disable
3	1	0	Disable
4	1	0	Disable
5	1	0	Disable
6	1	0	Disable
7	1	0	Disable
8	1	0	Disable
9	1	0	Disable
10	1	0	Disable
11	1	0	Disable
12	1	0	Disable
13	1	0	Disable
14	1	0	Disable

### 3 Configuring the IP networks in the WLAN controller

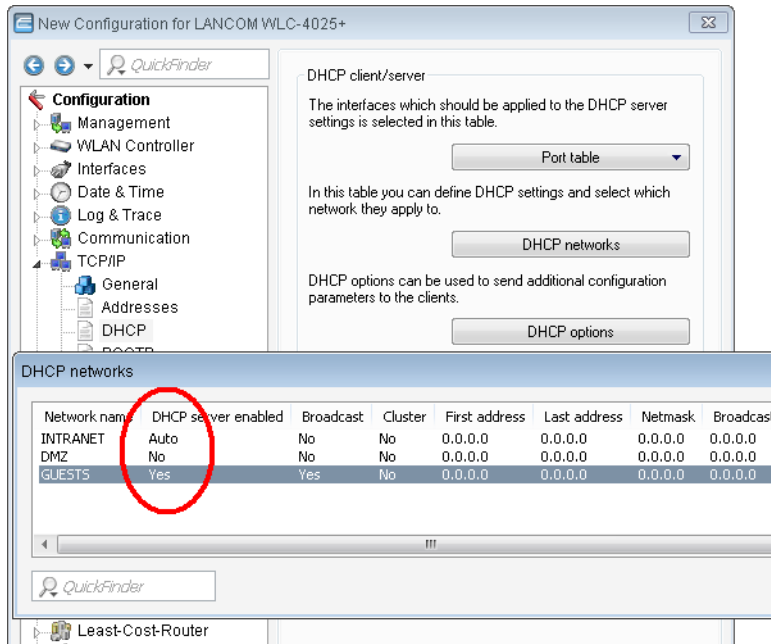
To separate the data streams on layer 3, two different IP networks are employed (ARF – Advanced Routing and Forwarding).

- Set the VLAN mode to &Tag based&, as the access points handle the assignment of VLAN tags.
  - 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.
  - For the guests, create a new IP network with the address '192.168.100.1'. This network uses the VLAN ID '100' so that data packets with this ID are assigned to the guest network. Here, too, the interface tag '10' is used later by the virtual router.

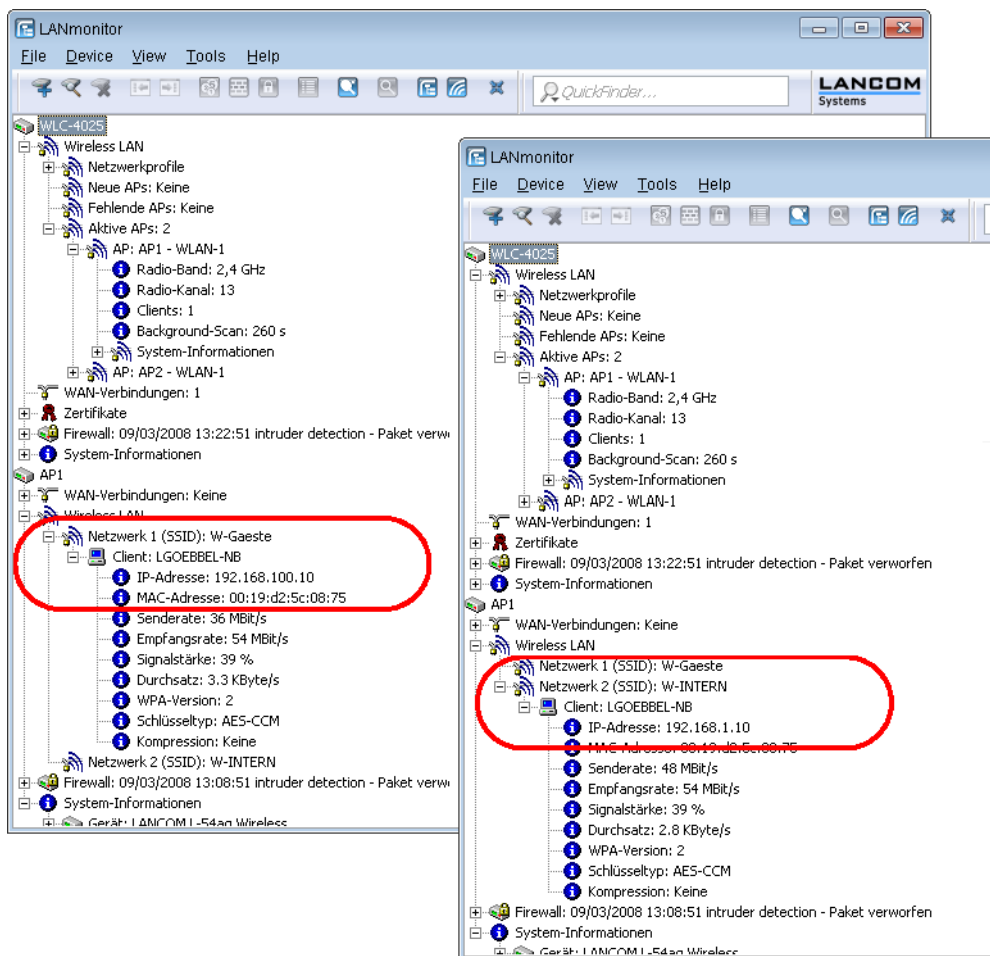


1 Centralized WLAN Management

- For both IP networks, an entry is created in the DHCP networks to permanently activate the DHCP server.



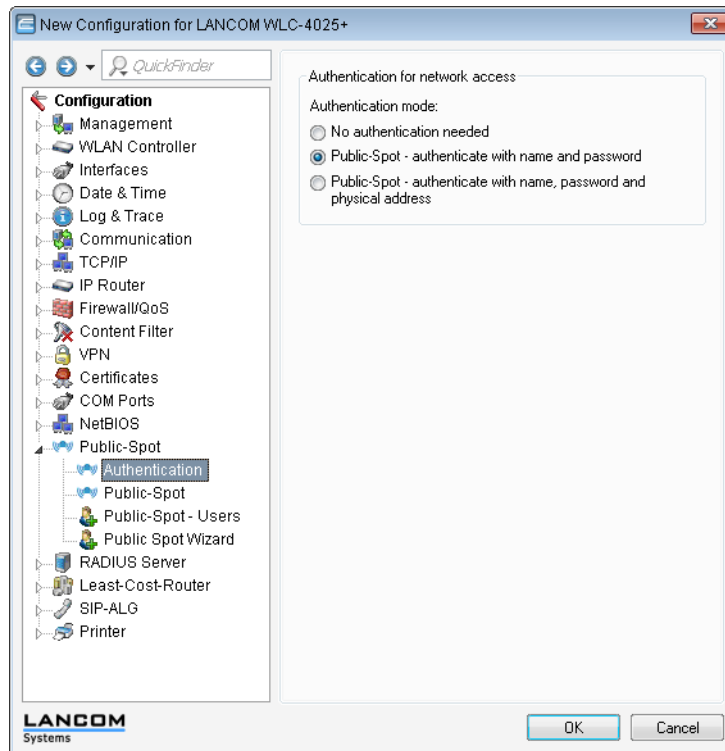
- With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.



## 4 Configuring Public Spot access

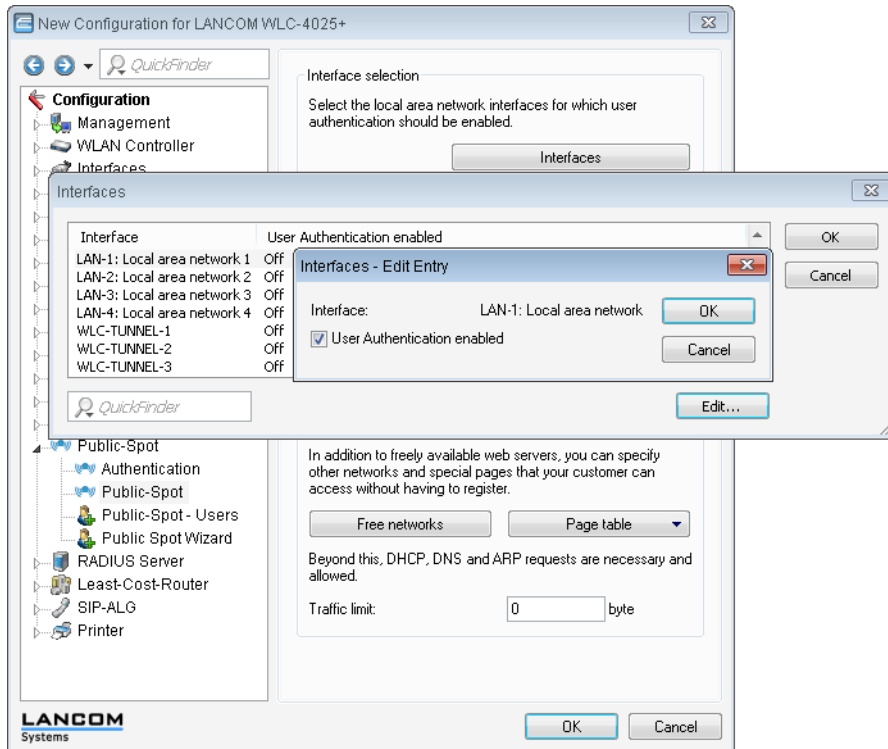
The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. User authentication is handled by a Web interface. Access can optionally be subject to time limits.

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



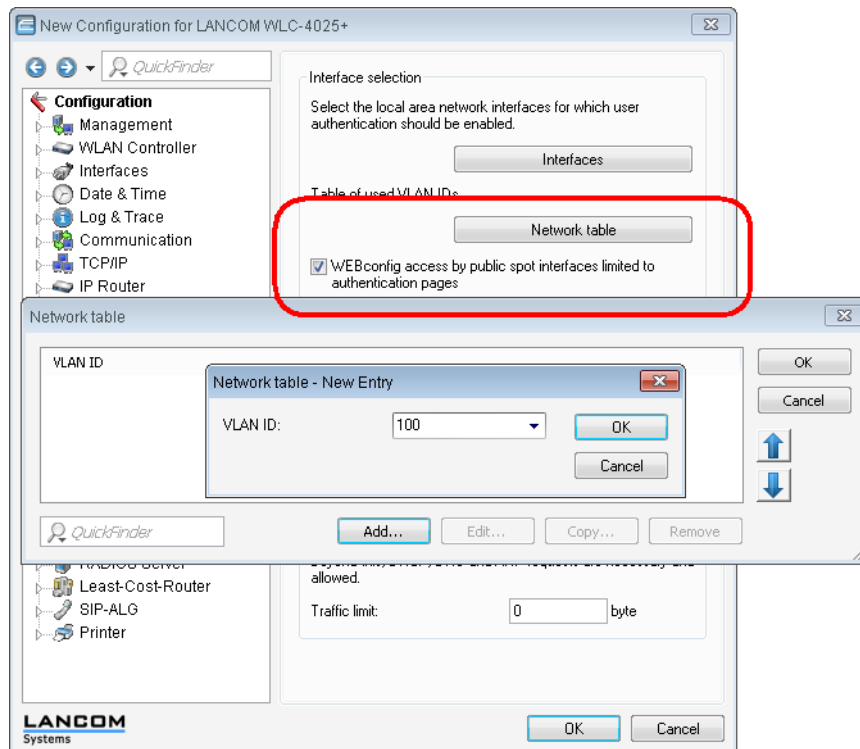
## 1 Centralized WLAN Management

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

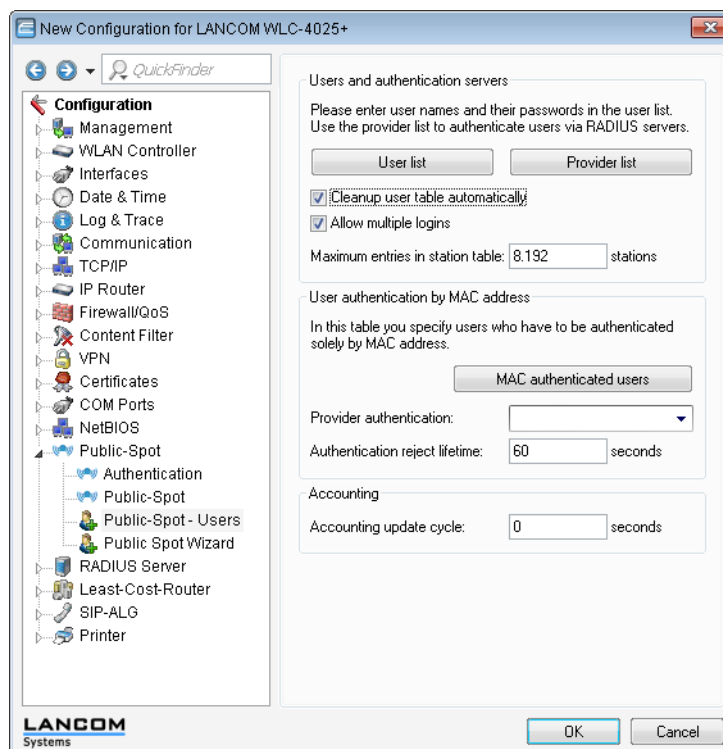


3. By entering the VLAN ID of '100' for the guest network into the VLAN table, the data packets for Public Spot users are restricted to this virtual LAN. Other data packets from other VLANs will be forwarded to the Public Spot without a login. Ensure that access to WEBconfig via the Public Spot interface is restricted to the authentication pages only and that HTTP is activated in the configuration protocols.

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



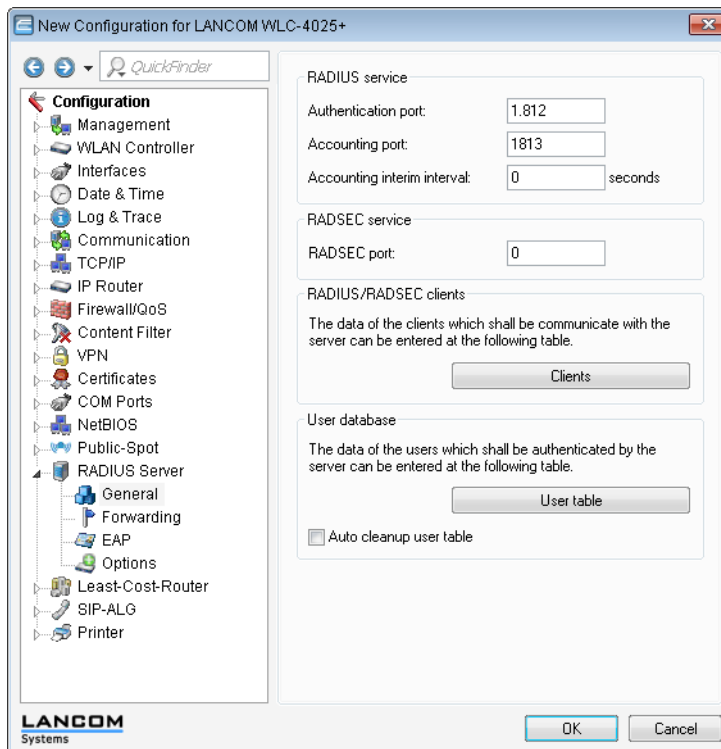
4. In the Public Spot module, activate the "Cleanup user table automatically" option to ensure that unwanted entries are automatically deleted.



## 5 Configuring the RADIUS server to operate a Public Spot

In LCOS versions prior to 7.70, Public Spot access accounts were defined by entering users into the Public Spot module's user list by using the Wizard. As of LCOS version 7.70, the Wizard no longer stores the Public Spot access accounts in this list, but in the user database of the internal RADIUS server instead. In order to use Public Spot access accounts, the RADIUS server must be configured and the Public Spot module must be set to use the RADIUS server.

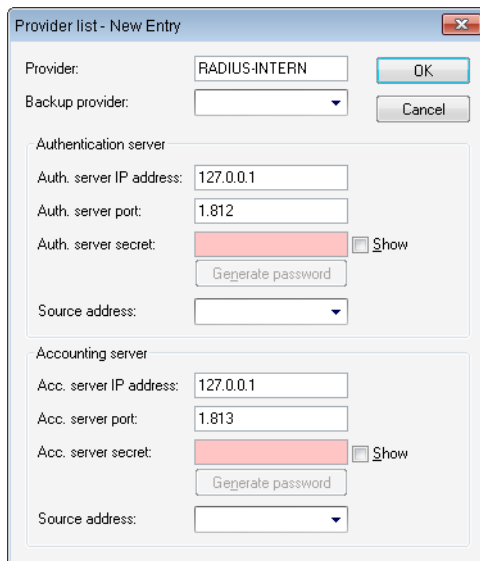
1. In order to use the user database in the internal RADIUS server, the RADIUS server in the LANCOM must be activated first. Activate the RADIUS server by entering authentication and accounting ports. Use the authentication port '1812' and the accounting port '1813'.



⚠ If appropriate please activate the "Auto cleanup user table" option to ensure, that entries not used any longer can be deleted automatically from the user database.

2. In order for the Public Spot access accounts to be authenticated by the LANCOM's internal RADIUS server, the Public Spot must know the address of the RADIUS server. To ensure that this is the case, under **Public Spot > Public Spot - users > Provider list** create a new entry to define the internal RADIUS server as a "Provider". Enter the IP address for the LANCOM with the activated RADIUS server as the authentication and accounting server.

- ! If the Public Spot and the RADIUS server are provided by the same LANCOM, enter the device's internal loopback address (127.0.0.1) here.

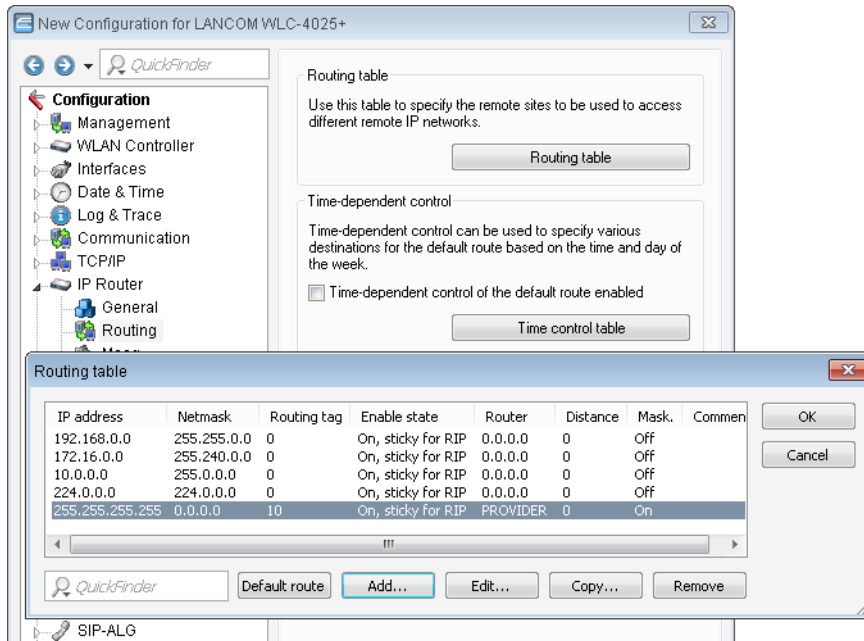


- ! After an LCOS update, user accounts that were created in the Public Spot module's user list with previous versions of LCOS are still valid.

## 6 Configuring Internet access for the guest network

1. In order to provide users of the guest network with Internet access, the wizards can be used to create access to the provider network.
2. In order for this access to be available to users of the guest network only, the corresponding route is set for the routing tag '10'. 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.

- ! If the Public Spot and the RADIUS server are provided by the same LANCOM, enter the device's internal loopback address (127.0.0.1) here.



- ! After an LCOS update, user accounts that were created in the Public Spot module's user list with previous versions of LCOS are still valid.

## 1.5 Access point administration

### 1.5.1 Accepting new access points into the WLAN infrastructure manually

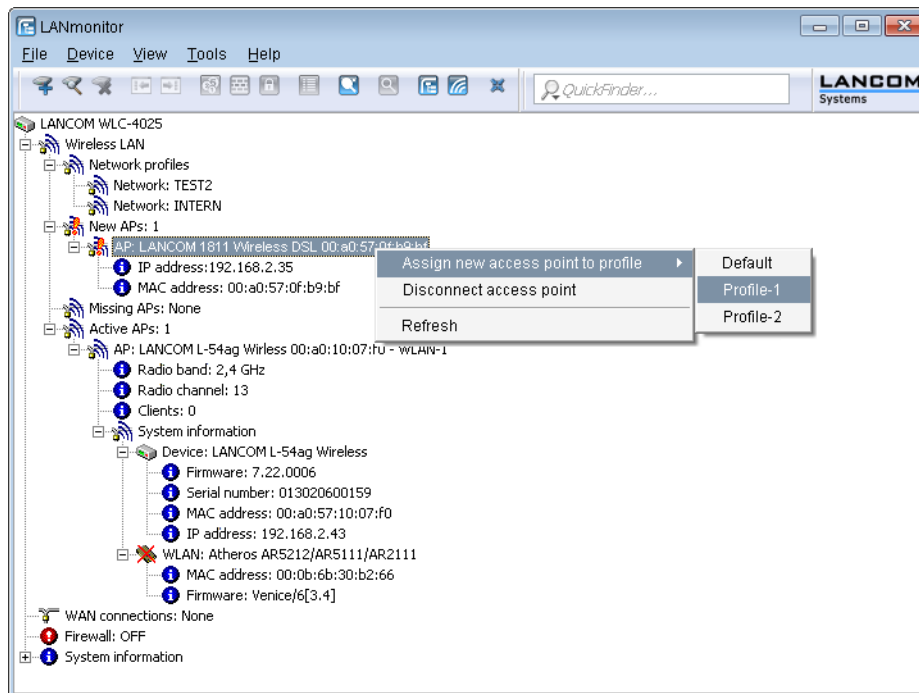
If you prefer not to accept access points into the WLAN infrastructure automatically, you can accept access points manually.

#### Using LANmonitor to accept access points

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



In LANmonitor, click on the new access point 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 access point to be entered into the AP table in the WLAN controller. It takes a few seconds for the WLAN controller to assign a certificate to the access point and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted access point 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 access points that do not have a valid certificate but do have an entry in the AP table can be manually accepted with WEBconfig.

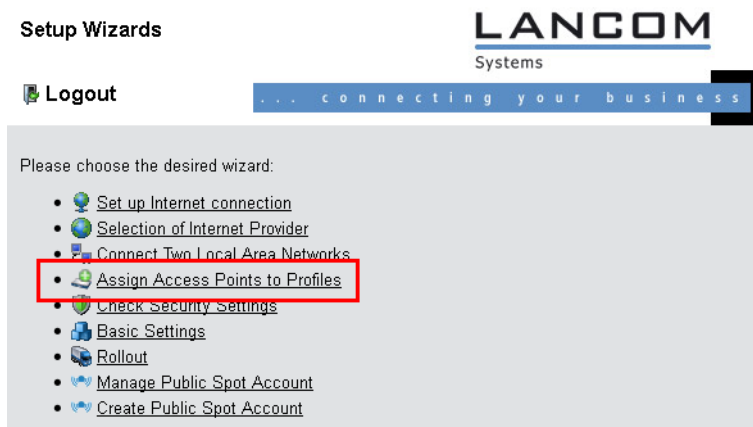
1. Open the configuration of the LANCOM WLAN controller in WEBconfig.
2. Under **LCOS Menu Tree > Setup > WLAN-Management** select the action **Accept AP**.
3. When requested for additional arguments, enter the MAC address of the access point to be accepted and confirm with **Execute**.



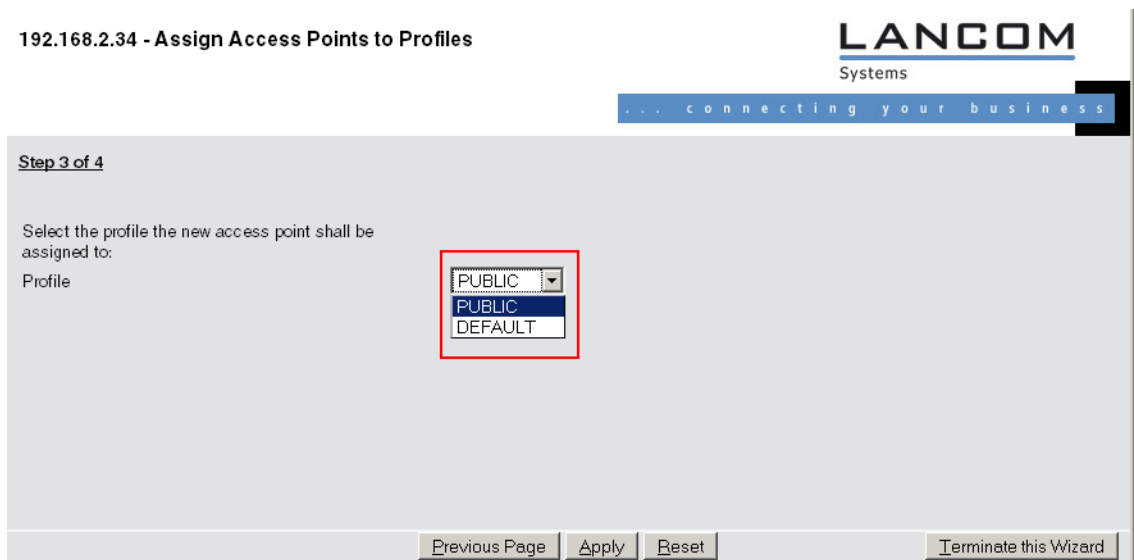
### Accepting access points via WEBconfig with provision of a certificate and configuration

New access points 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 access point after transmission of a new certificate.

1. Open the configuration of the LANCOM WLAN controller in WEBconfig. Click on **Setup Wizards** and select the wizard **Assign access points to profiles**.



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



- ⓘ Assignment of the configuration causes the access point to be entered into the AP table in the WLAN controller. It takes a few seconds for the WLAN controller to assign a certificate to the access point and for this to become an active element in the central WLAN infrastructure. Due to this, the newly accepted access point 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.

## 1.5.2 Manually removing access points from the WLAN infrastructure

The following actions are required to remove an access point under management of the WLAN controller from the WLAN infrastructure:

1. In the access point, 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 access point and/or deactivate **Automatically provide APs with a default configuration** via **LCOS Menu Tree > Setup > WLAN-Management > Autoaccept-AP**.

3. Disconnect the access point in WEBconfig by selecting **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 access point 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 WLAN controller-managed access point.

#### Deactivating an access point

To deactivate an access point, set its corresponding entry in the AP table to 'inactive' or delete the entry from the table. In the access point, 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 access point deactivated in this way remains connected to the WLAN controller and the certificates are retained. The WLAN controller can reactivate the access point and its managed-mode WLAN modules at any time. All you have to do is to activate the entry in the AP table or make a new entry in the AP table for the corresponding MAC address.

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

#### Permanently removing an access point from the WLAN infrastructure

In order to permanently remove an access point 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 access point, 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 WLAN controller's CA have to be revoked. This is done in WEBconfig by navigating to **Status > Certificates > SCEP-CA > Certificates** and accessing the **Certificate status table**. Here you delete the certificate for the MAC address of the access point which is 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 WLAN controllers, the certificates have to be revoked in all of the WLAN controllers!

## 1.6 Central firmware and script management

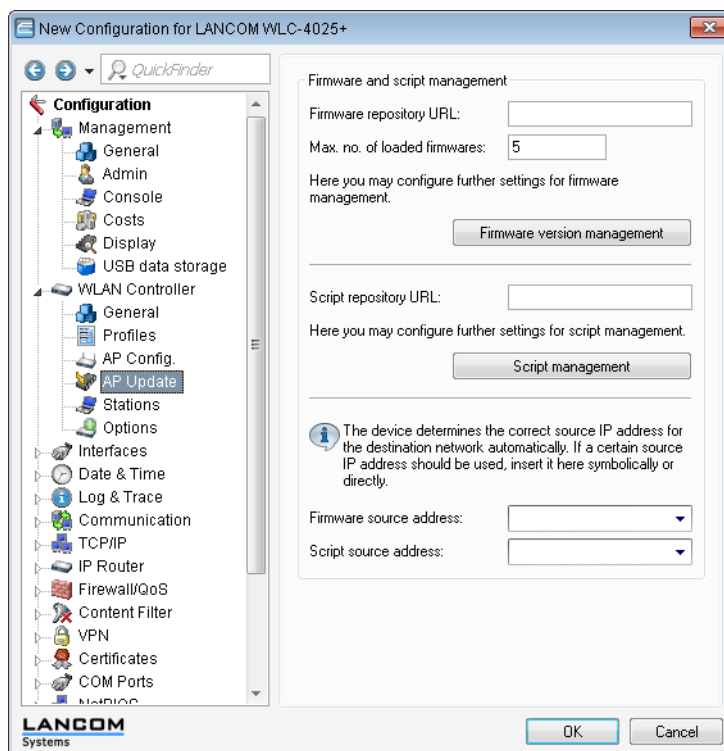
LANCOM WLAN controllers allow the configurations of multiple LANCOM WLAN routers and LANCOM access points to be managed from a central location in a consistent and convenient manner. With central firmware and script management, uploads of firmware and scripts can be automated for all of the WLAN devices.

To achieve this, the firmware and script files are stored on a Web server (firmware as \*.upx files, scripts and \*.lcs files). The WLAN controller 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 access point is not running the desired firmware version, then the WLAN controller downloads the file from the Web server and uploads it to the appropriate WLAN routers and access points.

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 access point subsequently restarts automatically.
- If the access point is already connected, the device does not restart automatically. In this case the access point 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**

## 1.6.1 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

### ■ Simultaneously loaded FW

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



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 sender IP address

This is where you can configure an optional sender address for use instead of the one automatically selected for the destination 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

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

### ■ 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 that is to be used for the devices or device types specified here.

- Possible values: Firmware version in the form `x.xx`
- 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 sender IP address

This is where you can configure an optional sender address for use instead of the one automatically selected for the destination 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.

## Script management table

Table with the name of the script file and a WLAN profile for allocating the script to a WLAN profile.

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 access points 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 WLAN Controller to determine whether the script file has to be transmitted again in case a new or altered script has the same file name.

### ■ Script file name

Name of the script file to be used.

- 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

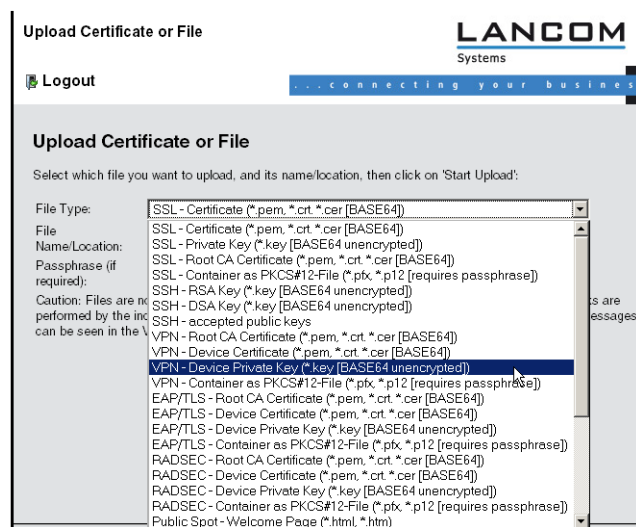
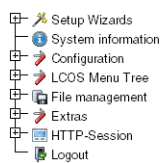
## Internal script storage (script management without an HTTP server)

In contrast to firmware files, scripts involve only small volumes of data. The WLAN controller's internal script storage allows three scripts of up to 64KB each to be stored. 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.



## 1.7 WLAN layer-3 tunneling

### 1.7.1 Introduction

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

- The obligatory control channel transports administrative data between the managed access point and the WLAN controller.
- The optional data channel transmits the payload data from the various WLAN networks (SSID) between the managed access point and the WLAN controller.

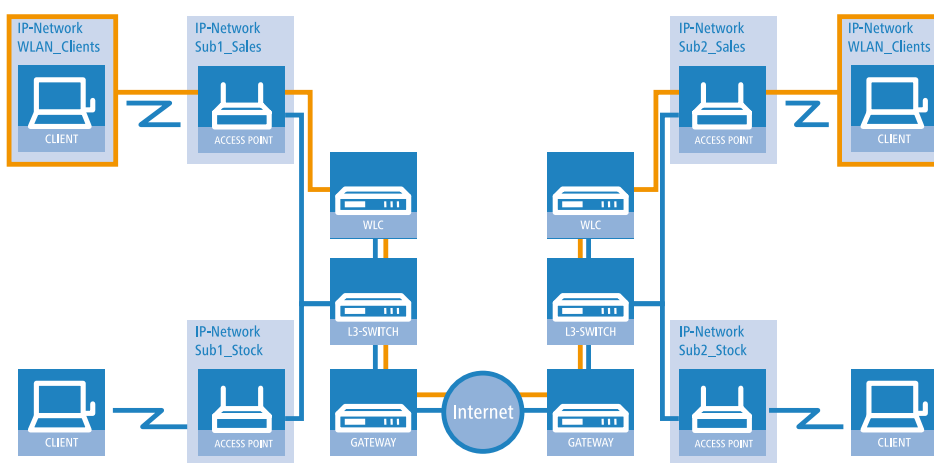
The decision whether to use of the optional data channel between the managed access point and the WLAN controller depends on the route to be taken by the payload data:

- If you deactivate the data channel, the access point 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 controller and on the network as a whole, because the access point transmits only the management data via the CAPWAP tunnel and it transmits the payload data over the shortest available route.

## 1 Centralized WLAN Management

- If you activate the data channel, the access point additionally forwards the payload data to the central WLAN controller. This approach has the following advantages:
  - The access points can provide access to networks that are only available on the WLAN controller, such as a central Internet access for a Public Spot.
  - The WLANs provided by the access points (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 access points and in different IP networks can roam to other access points without interruption to their IP connections, because the connection is continually managed by the central controller and not by the access points (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.



### Overlay network across multiple IP networks

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

Several WLCs within a single broadcast domain can support the same overlay network. Disable the WLC data channel between these controllers (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 discard broadcast messages, you can activate the CAPWAP data channel for controllers in separate networks.

The access points use virtual WLC interfaces (WLC tunnels) to manage each SSID's data channels between access point and WLAN controller. Depending on the model, each WLAN controller 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.

## 1.7.2 Tutorials

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

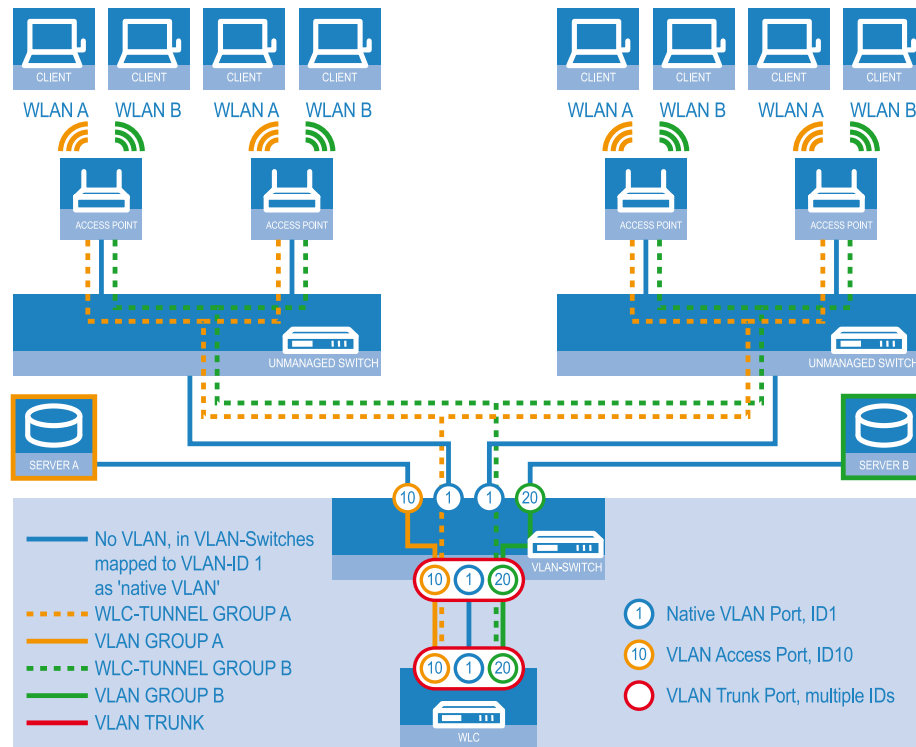
### Overlay network: Separating networks for access points without using VLAN

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.



WLAN controllers enable you to separate the networks while minimizing the use of VLANs. The access points use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the controller, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the controller 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.



#### 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 access points, each of which is connected to one of the switches.
- Each access point 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 WLAN controller manages all of the access points in the network.
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLAN controller.

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

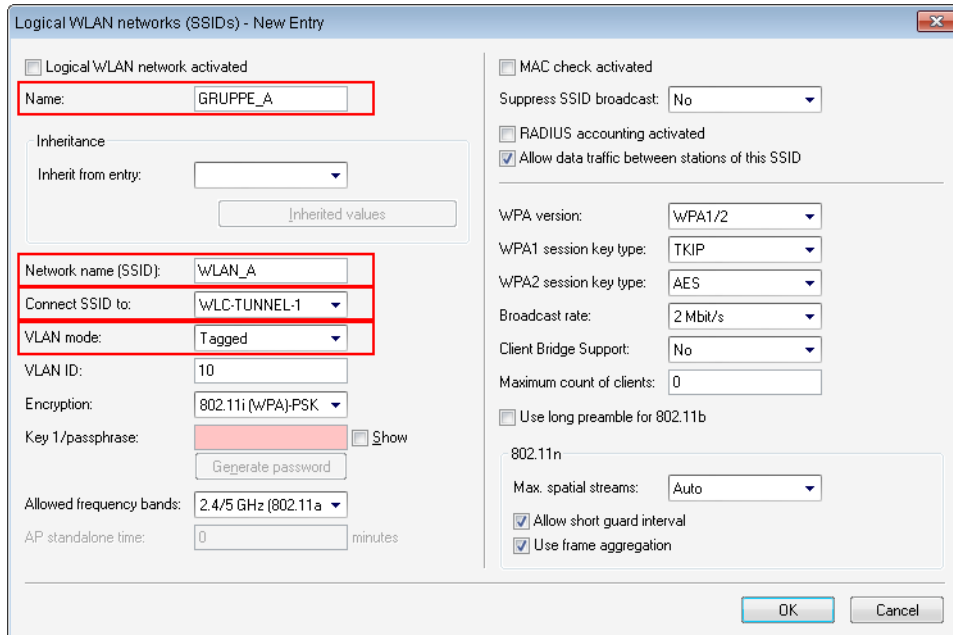
! The following description assumes a working basic configuration of the WLAN controller. The configuration of the VLAN switch is not part of this description.

#### Configuring the WLAN settings

1. For each SSID, create an entry in the list of logical networks. This entry requires 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

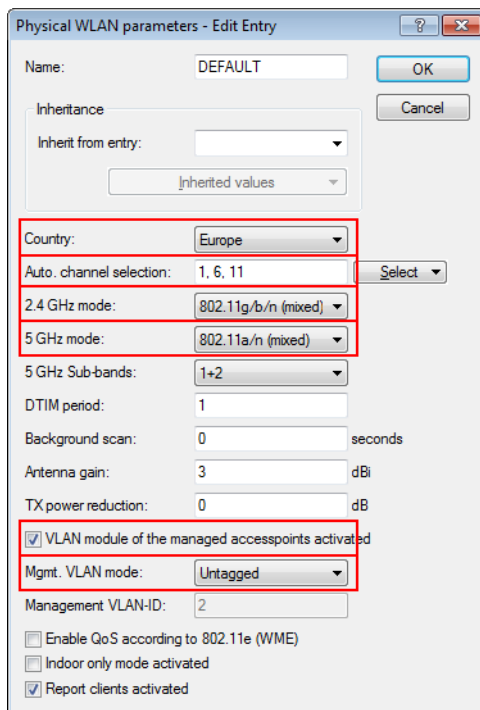
1 Centralized WLAN Management

"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)** .



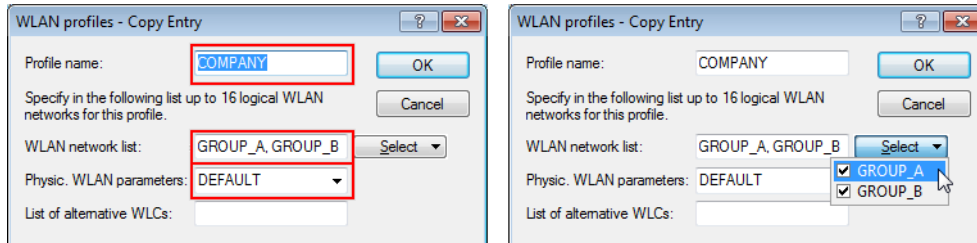
Logical WLAN networks for overlay networks

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, 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 access points. Set the operating mode for the management VLAN in the access points to 'Untagged'. In LANconfig you find these settings under **Configuration > WLAN Controller > Profiles > Physical WLAN parameters** .



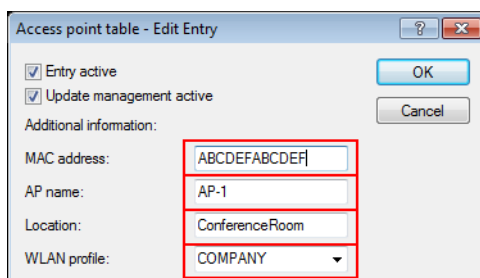
### Physical WLAN parameters for overlay networks

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 these settings under **Configuration > WLAN Controller > Profiles > WLAN profiles** .



### WLAN profiles for overlay networks

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

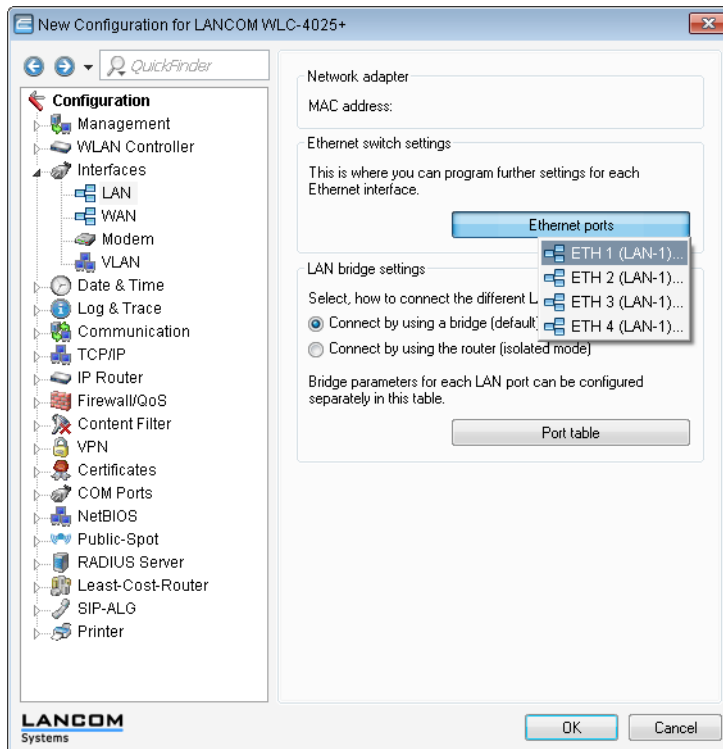


### Access point table for overlay networks

## Configuring the interfaces on the WLC

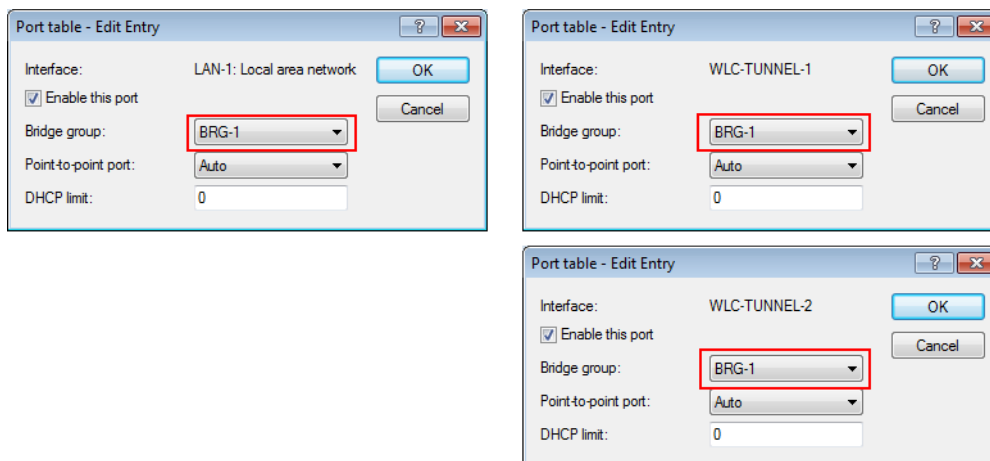
1 Centralized WLAN Management

- 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**.



Ethernet setting for overlay networks

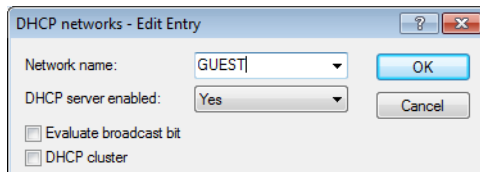
- Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find these settings under **Configuration > Interfaces > LAN > Port table**.



Port settings for overlay networks

⚠ 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.

7. The WLAN controller can optionally act as a DHCP server for the access points. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **Configuration > TCP > DHCP > DHCP networks**.

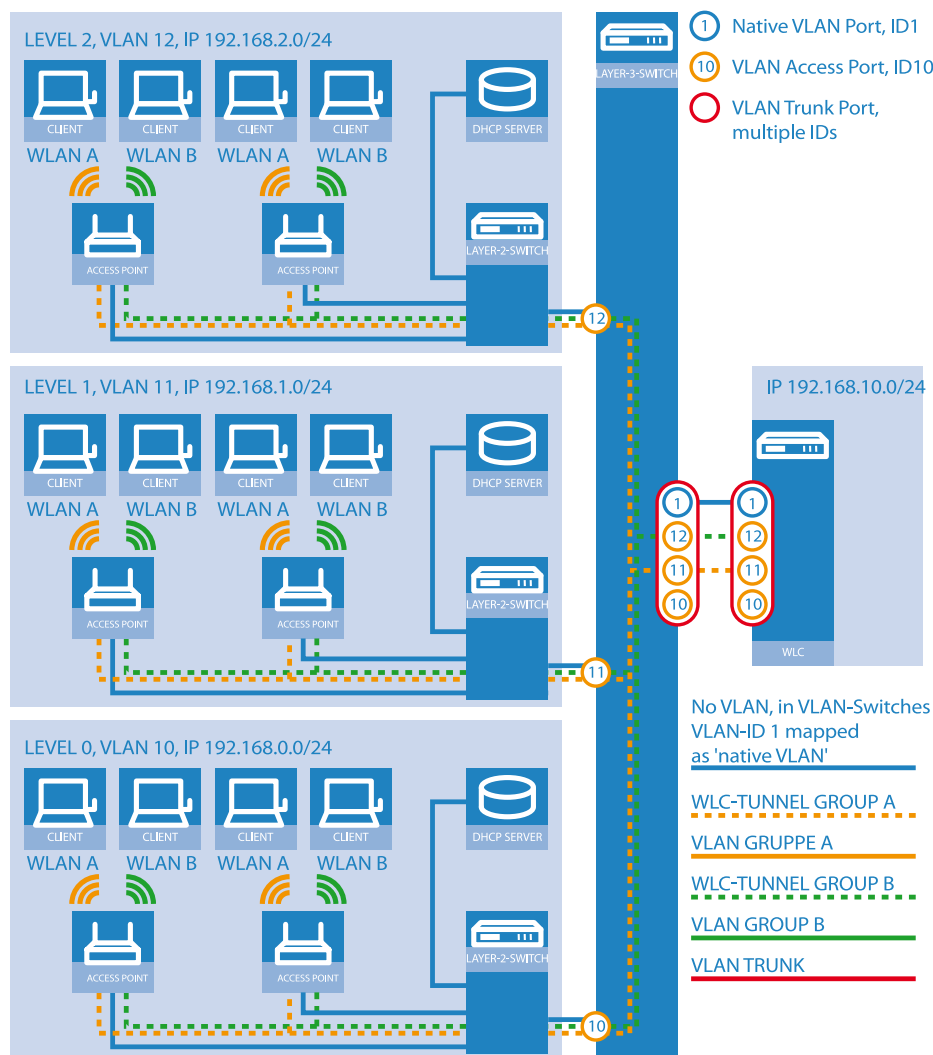


DHCP settings for overlay networks

## Layer-3 roaming

Allowing payload data from the wireless LAN to pass-through the WLC tunnel to the controller 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.

In this example, two user groups A and B each have access to their own WLAN (SSID). On all floors of the building, the access points provide two SSIDs, 'GROUP\_A' and 'GROUP\_B'.



### Example application: 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 access points:
  - IP address of the gateway
  - IP address of the DNS server
  - Domain suffix

! This information enables the access points to contact the WLC controller 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 access point 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 access points directly with the central WLAN controller via layer 3 and across the boundaries of the VLANs.

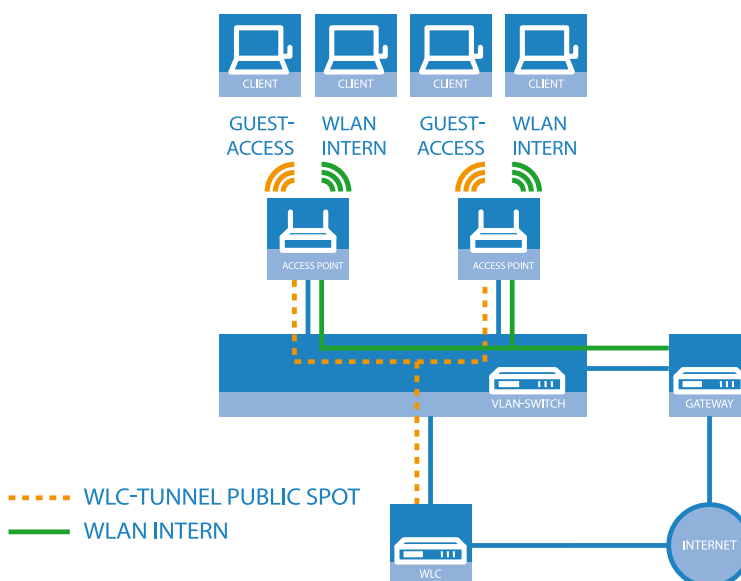
! The configuration corresponds to the example *Overlay network: Separating networks for access points without using VLAN* on page 48.

### 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 controller 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 access points provide two SSIDs, 'COMPANY' and 'GUESTS'.



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 access points 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 access points send the payload data from the guest clients through a WLC tunnel directly to the WLAN controller, 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 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)**.

The screenshot shows the configuration window for a logical WLAN network. The following settings are highlighted with red boxes:

- Name:** COMPANY
- Network name (SSID):** WLAN-INTERN
- Connect SSID to:** LAN at AP
- Encryption:** 802.11i (WPA)-PSK

Other visible settings include: Logical/WLAN network activated (checked), Inheritance (empty), VLAN mode (Untagged), VLAN ID (2), Key 1/passphrase (redacted), Allowed frequency bands (2.4/5 GHz (802.11a)), AP standalone time (0 minutes), MAC check activated (unchecked), Suppress SSID broadcast (No), RADIUS accounting activated (unchecked), Allow data traffic between stations of this SSID (checked), WPA version (WPA1/2), WPA1 session key type (TKIP), WPA2 session key type (AES), Broadcast rate (2 Mbit/s), Client Bridge Support (No), Maximum count of clients (0), Use long preamble for 802.11b (unchecked), 802.11n Max. spatial streams (Auto), Allow short guard interval (checked), and Use frame aggregation (checked).

### Logical WLAN networks for internal use

The screenshot shows the configuration window for a logical WLAN network. The following settings are highlighted with red boxes:

- Name:** GUESTS
- Network name (SSID):** WLAN-PUBLIC
- Connect SSID to:** WLC-TUNNEL-1
- Encryption:** None
- Allow data traffic between stations of this SSID:** (unchecked)

Other visible settings include: Logical/WLAN network activated (checked), Inheritance (empty), VLAN mode (Untagged), VLAN ID (2), Key 1/passphrase (redacted), Allowed frequency bands (2.4/5 GHz (802.11a)), AP standalone time (0 minutes), MAC check activated (unchecked), Suppress SSID broadcast (No), RADIUS accounting activated (unchecked), WPA version (WPA1/2), WPA1 session key type (TKIP), WPA2 session key type (AES), Broadcast rate (2 Mbit/s), Client Bridge Support (No), Maximum count of clients (0), Use long preamble for 802.11b (unchecked), 802.11n Max. spatial streams (Auto), Allow short guard interval (checked), and Use frame aggregation (checked).

### Logical WLAN networks for guest access accounts

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, 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** .

Physical WLAN parameters - Edit Entry

Name: DEFAULT [OK] [Cancel]

Inheritance

Inherit from entry: [ ] [Inherited values]

Country: Europe

Auto. channel selection: 1, 6, 11 [Select]

2.4 GHz mode: 802.11g/b/n (mixed)

5 GHz mode: 802.11a/n (mixed)

5 GHz Sub-bands: 1+2

DTIM period: 1

Background scan: 0 seconds

Antenna gain: 3 dBi

TX power reduction: 0 dB

VLAN module of the managed accesspoints activated

Mgmt. VLAN mode: Untagged

Management VLAN-ID: 2

Enable QoS according to 802.11e (WME)

Indoor only mode activated

Report clients activated

### Physical WLAN parameters for Public Spot APs

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** .

WLAN profiles - Edit Entry

Profile name: COMPANY [OK] [Cancel]

Specify in the following list up to 16 logical WLAN networks for this profile.

WLAN network list: COMPANY, GUEST [Select]

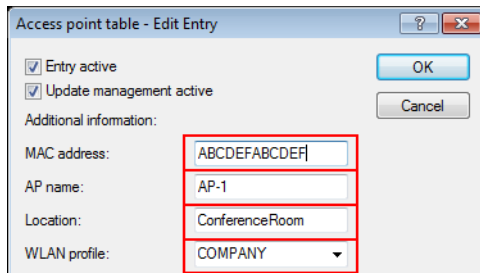
Physic. WLAN parameters: DEFAULT

List of alternative WLCs: [ ]

### WLAN profiles for Public Spot APs

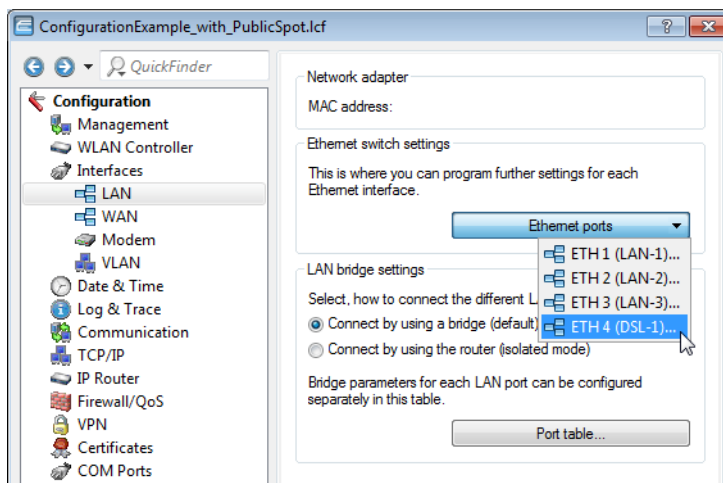


- For each managed access point, create an entry in the access point table with a suitable name and the associated MAC address. Assign the WLAN profile created previously to this access point. In LANconfig you find this setting under **Configuration > WLAN Controller > AP config. > Access point table**.



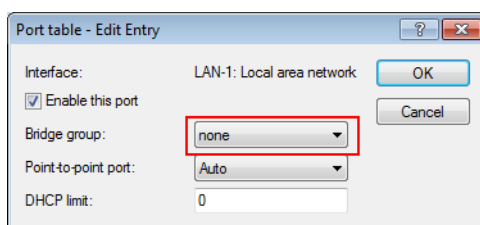
#### Access point table for Public Spot APs

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



#### Ethernet settings for Public Spot APs

- 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**.



#### Port settings for Public Spot APs

- 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 (DSL)**.

Remote sites (DSL) - Edit Entry

Name: INTERNET

Short hold time: 9.999 seconds

Access concentrator:

Service:

Layer name: DHCPOE

MAC address type: Local

MAC address:

DSL ports: Select

VLAN ID: 0

#### Remote site for Internet access

- 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 '192.168.200.1' and the interface tag '2'. The virtual router in the WLAN controller 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**.

IP networks - Edit Entry

Network name: INTRANET

IP address: 192.168.1.100

Netmask: 255.255.255.0

Network type: Intranet

VLAN ID: 0

Interface assignment: Any

Address check: Loose

Interface tag: 1

Comment:

#### IP network for internal use

IP networks - Edit Entry

Network name: GUEST

IP address: 192.168.200.1

Netmask: 255.255.255.0

Network type: Intranet

VLAN ID: 0

Interface assignment: Any

Address check: Loose

Interface tag: 2

Comment:

#### IP network for guest access

- The WLAN controller can act as a DHCP server for access points 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 > 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.

#### DHCP network for guest access

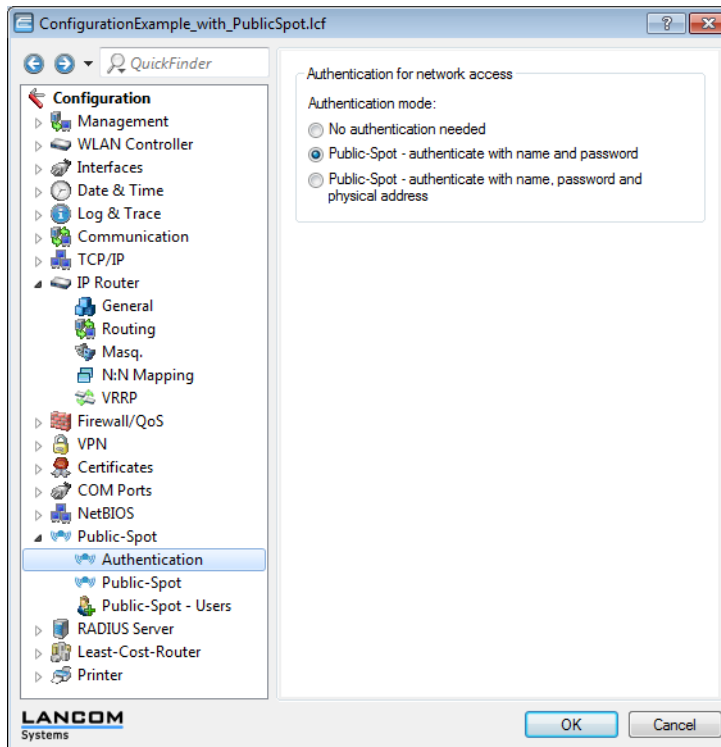
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLAN controller. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting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

#### Routing entry for Internet access

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 > Public Spot**.

#### Activation of user authentication for the WLC tunnel

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



#### Activation of authentication via Public Spot

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

- ! An example for the configuration of the Public Spot can be found in the tutorial [Virtualization and guest access accounts via the LANCOM WLAN controller](#).

## 1.8 RADIUS

### 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 LANCOM WLAN controller.

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

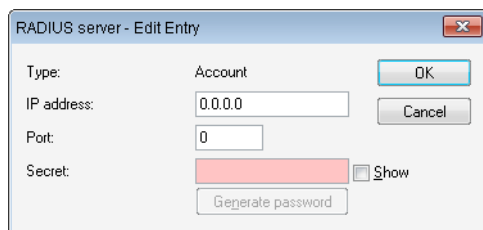
Alternatively, the approved MAC addresses can be entered in WEBconfig under **LCOS menu tree > Setup > RADIUS > Server > Users**.

 The MAC address is entered as **User name** and as **Password** in the written form 'AABBCC-DDEEFF'.

## 1.8.2 External RADIUS server

By default the WLAN controller forwards any requests relating to the account and access management to a RADIUS server. In order for access points to contact the RADIUS server directly, the necessary server information has to be defined here. This ensures that the RADIUS application continues to function even if the WLAN controller is unavailable. However, this means that the RADIUS server requires settings for each and every access point, and the managed access points

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.

The image shows a dialog box titled "RADIUS server - Edit Entry". It contains several fields: "Type" is set to "Account"; "IP address" is set to "0.0.0.0"; "Port" is set to "0"; and "Secret" is a redacted field. There are "OK", "Cancel", and "Generate password" buttons, along with a "Show" checkbox next to the secret field.

LANconfig: **WLAN Controller > Stations > RADIUS server**

WEBconfig: **LCOS Menu Tree > Setup > WLAN Management > RADIUS-Server**

- **Type:** Type of RADIUS application.

**Possible values:**

Account or access

**Default:**

The entries account, access, backup account and backup access are fixed settings that cannot be changed.

- **IP address:** IP address to be used by the AP in order for it to reach the RADIUS server. If no value is entered the controller's IP address is taken as default.

**Possible values:**

Valid IP address.

**Default:**

Blank

- **Port:** Port number of the RADIUS server that is communicated to the AP in order for it to reach the RADIUS server. The port must agree with the value configured in the RADIUS server. This value will be ignored if no IP address is configured as the controller itself will be used as the RADIUS server.

**Possible values:**

Valid port number, generally 1812 for access management and 1813 for account management.

**Default:**

0

- **Secret:** Password for the RADIUS service. The key (secret) must agree with the value configured in the RADIUS server. This value will be ignored if no IP address is configured as the controller itself will be used as the RADIUS server.

**Possible values:**

Maximum 31 ASCII characters.

**Default:**

Blank

## 1.9 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 access points, 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 log on to different access points then, depending on the configuration, they may find themselves in a different IP network.

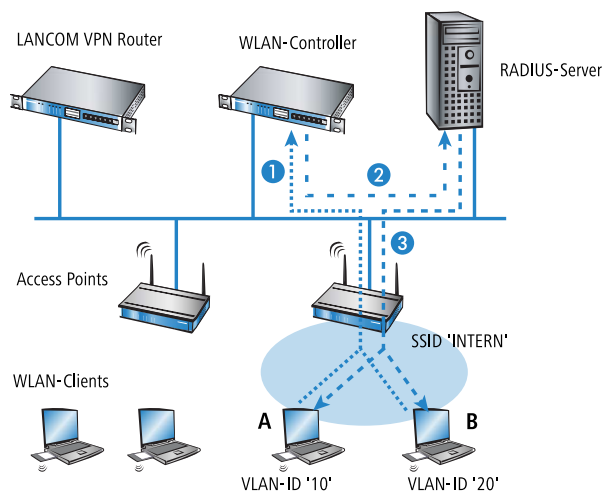
For WLAN clients to remain within a certain network **independent** of their current WLAN network, dynamically assigned VLANs can be used. Unlike the situation where VLAN IDs are statically configured for a certain SSID, in this case a RADIUS server directly assigns the VLAN ID to the WLAN client.

#### Example:

- The WLAN clients of two employees log into an access point in the WPA-secured network with the SSID 'INTERNAL'. During registration, the RADIUS requests from the WLAN clients are directed to the access point. If the corresponding WLAN interface is in the operating mode 'managed' the RADIUS requests are automatically forwarded to the WLAN controller. 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 access point 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 LANCOM WLAN controller.




1. Activate VLAN tagging for the WLAN controller. 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 WLAN controller, a RADIUS server is required to operate authentication via 802.1x and MAC-address checks. The WLAN controller automatically defines itself as the RADIUS server in the access points that it is managing—all RADIUS requests sent to the access points are then directly forwarded to the WLAN controller, 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 **LCOS menu tree > Setup > RADIUS > Server > Forward server** . 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.

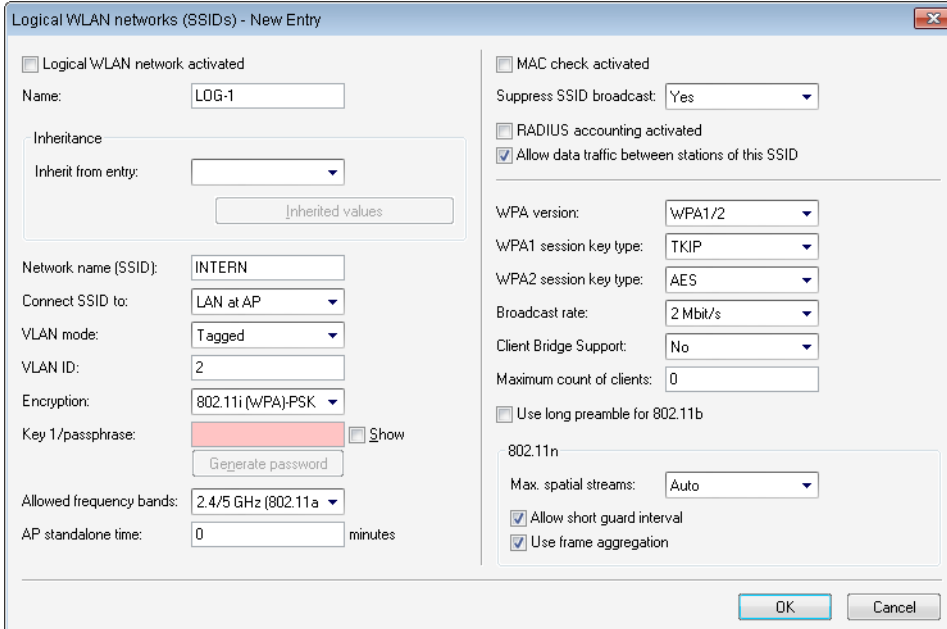
 Further information about RADIUS is available in the documentation for your RADIUS server.

## 1.10 Activating 802.1x accounting for logical WLANs in WLAN controllers

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

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

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



### ■ RADIUS accounting activated

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

Possible values:

- Yes, No

Default:

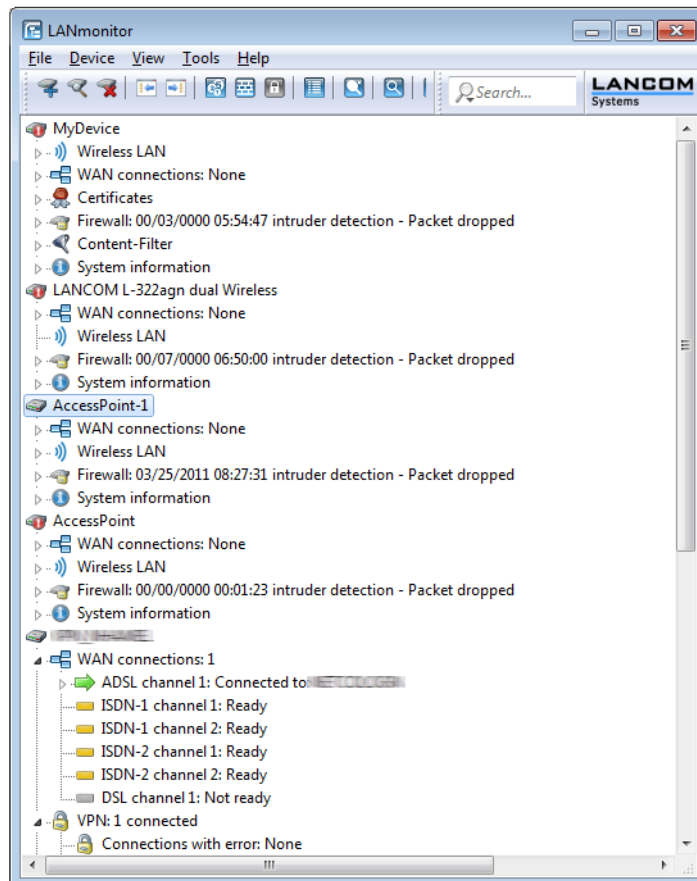
- No

 The access points supporting the logical WLAN network as configured by the WLAN controller must have an LCOS version 8.00 or higher.



## 1.11 Displays and commands in LANmonitor

LANmonitor gives you a rapid overview of the LANCOM WLAN controllers in your network and the access points within the WLAN infrastructure. LANmonitor displays the following information, among others:



- Active WLAN networks with the logged-on WLAN clients and the descriptor of the access point that the WLAN clients are associated with.
- Display of new access points with IP and MAC address
- Display of missing access points with IP and MAC address
- Display of managed access points with IP and MAC address, the utilized frequency band and channel

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

- **Assign new access point to profile**  
Enables a new access point to be allocated to a profile and accepted into the WLAN infrastructure.
- **Disconnect access point**  
Disconnects the access point from the WLAN controller. The access point then carries out a new search for a suitable WLAN controller. This command can be used after a backup event to disconnect access points from a backup controller and to redirect them to the correct WLAN controller.
- **Refresh**  
Updates LANmonitor's display.

## 1.12 Automatic RF optimization

Selecting the channel from the channel list defines a portion of the frequency band to be used by an access point for its logical wireless LANs. The WLAN clients connected to an access point have to share 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 access point at a time can actually transfer data. In order to operate another access point within radio range with maximum bandwidth, each access point must use a separate channel—otherwise all of the participating WLANs would have to share a single channel's bandwidth.

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

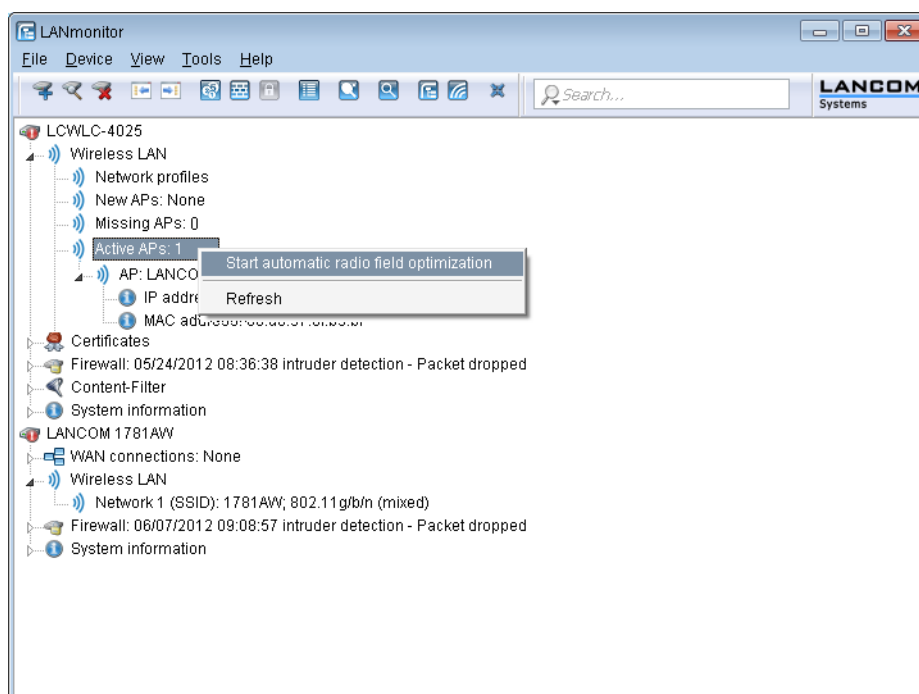
In larger installations with several access points it can be difficult to set a channel for every access point. With automatic radio-field (RF) optimization, the LANCOM WLAN controllers provide an automatic method of setting the optimum channels for access points that work in the 2.4-GHz band and 5-GHz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

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

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

! You can invoke optimization for a particular access point by entering its MAC address as a parameter for the action.

LANmonitor: Right-click on the list of active access points 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 WLAN controller assigns the same channel to all access points. The selected channel is the one being used by the majority of access points.

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



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

## 1.13 Channel-load display in WLC mode

The loads on the various channels used by each access point which is managed by a WLAN Controller 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.

The screenshot shows the WLANmonitor application window. The interface includes a menu bar (File, Group, Access Point, WLAN Controller, View, Tools), a toolbar with icons for adding, deleting, and refreshing, and a LANCOM Systems logo. The main area is divided into several sections:

- Groups:** A tree view on the left showing 'WLANmonitor', 'Access Points (24)', 'WLAN-Controller', 'Aachen (2)', 'London (2)', 'Munich (3)', and 'Rogue AP Detectio'.
- Controller:** A table listing controllers with columns: Name, New..., Missing APs, Active APs, Clients, IP-A, and Name.
 

Name	New ...	Missing APs	Active APs	Clients	IP-A	Name
LC_BKP_WLC-4...	0	0	3	5		
LC_WLC-4025+	0	0	13	29		
- Access Points:** A table listing access points with columns: Name, Interfa..., Clie..., Band, C..., Min. Chan..., Max. Chan..., and Ave. Channel load.
 

Name	Interfa...	Clie...	Band	C...	Min. Chan...	Max. Chan...	Ave. Channel load
Ic-e280-OAP54	WLAN-2	2	5 GHz	64	0 %	2 %	1 %
Ic-e203-L322	WLAN-1	0	2,4 GHz	12	0 %	29 %	28 %
Ic-e203-L322	WLAN-2	1	5 GHz	100	0 %	0 %	0 %
Ic-e360-L322	WLAN-1	1	2,4 GHz	1	0 %	29 %	19 %
Ic-e360-L322	WLAN-2	0	5 GHz	64	0 %	2 %	0 %
L54-MPlum-H...	WLAN-1	0	5 GHz	108	0 %	0 %	0 %
L320agn-MPI...	WLAN-1	0	5 GHz	100	0 %	0 %	0 %
OAP310agn-...	WLAN-1	0	2,4 GHz	6	0 %	1 %	0 %
- Clients:** A table listing clients with columns: MAC Address, Identification, Sig..., Controller, Access Point, and Network Profile. It shows signal strength bars and percentage values for each client.

## 1.14 Backing up the certificates

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

If multiple WLAN controllers 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 with the operation of the managed access points.

### 1.14.1 Create backups of the certificates

To restore the CA or RA, the corresponding root certificates with private keys will be required as were generated automatically when the LANCOM WLAN controller 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 PCKS12 container.

1. Open the configuration of the LANCOM WLAN controller in WEBconfig and go to **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 |

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

## 1 Uploading a certificate backup into the device

1. Click on **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_`.

```
del controller_*
del eaptls_*
```

6. After that, access the directory **Setup > Certificates > SCEP-Client** and execute the command `Reinit`:

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

## 2 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 access points by the SCEP-CA.

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

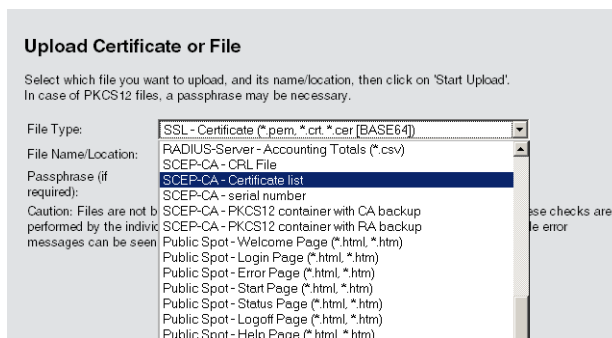
For this reason the following files have to be saved in addition to the certificates themselves:

- 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 **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.

## 1.15 Backup solutions

LANCOM WLAN controllers manage a large number of access points, which in turn may have a large number of WLAN clients associated with them. WLAN controllers 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 WLAN controller failure is in many cases indispensable.

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

## 1 Backup with redundant WLAN controllers

This is worthwhile for backing up a LANCOM WLAN controller with a second WLAN controller, the aim being to maintain full control over all managed access points at all times. The backup Controller is configured in such a way that it uses SCEP to obtain the necessary certificates from the backed-up primary WLAN controller.



- 1.
2. Switch off the CA on the backup Controller.
3. In the configuration of the SCEP client in the backup controller, create a new backup in the CA table (in LANconfig under **Certificates > SCEP client > CA table**). The CA of the primary WLAN controller is entered here:

Name:	BACKUP	OK
URL:	http://123.123.123.123	Cancel
Distinguished name:	/CN=LANCOM CA/O=L	
Identifier:		
Encryption algorithm:	DES	
Signature algorithm:	MD5	
Fingerprint algorithm:	Off	
Fingerprint:		
Usage type:	WLAN Controller	
<input checked="" type="checkbox"/> Registration-Authority: Enable automatic approval (RA Auto-approve)		
Source address:		

4. The URL is to be entered as the IP address or the DNS name of the primary WLAN controller 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
  - Switch on **RA auto approve**
  - **Usage type:** WLAN controller
5. Then create a new entry in the certificate table with the following information:


Name:	BACKUP	OK
CA Distinguished Name:	/CN=LANCOM CA/O=L	Cancel
Subject:	/CN=LANCOM CA/O=L	
Challenge Password:	password	
Subject alternative name:		
Key usage:		Select
Extended key usage:	serverAuth, critical, 1.3	Select
Key length:	2048	bit
Usage type:	WLAN Controller	

- **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 file system
    - 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 WLAN controller **1** according to your requirements with all profiles and the associated AT table. The access points then establish connections to the first WLAN controller. Each access point receives a valid certificate and a configuration for the WLAN module from the WLAN controller.
  8. Transfer the configuration from the first WLAN controller **1**, for example using LANconfig, to the backup controller **2**. The profiles and the AP tables with the access point MAC addresses are transferred to the backup controller at the same time. All access points remain logged on to the first WLAN controller.

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

---

 In this scenario, the access points remain under the management of the backup controller until this itself becomes unavailable or is manually disconnected.

---

 If the access points are set up for standalone operation, they will remain operational while searching for a backup controller and the WLAN clients will remain associated.

### 1.15.1 Backup with primary and secondary WLAN controllers

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

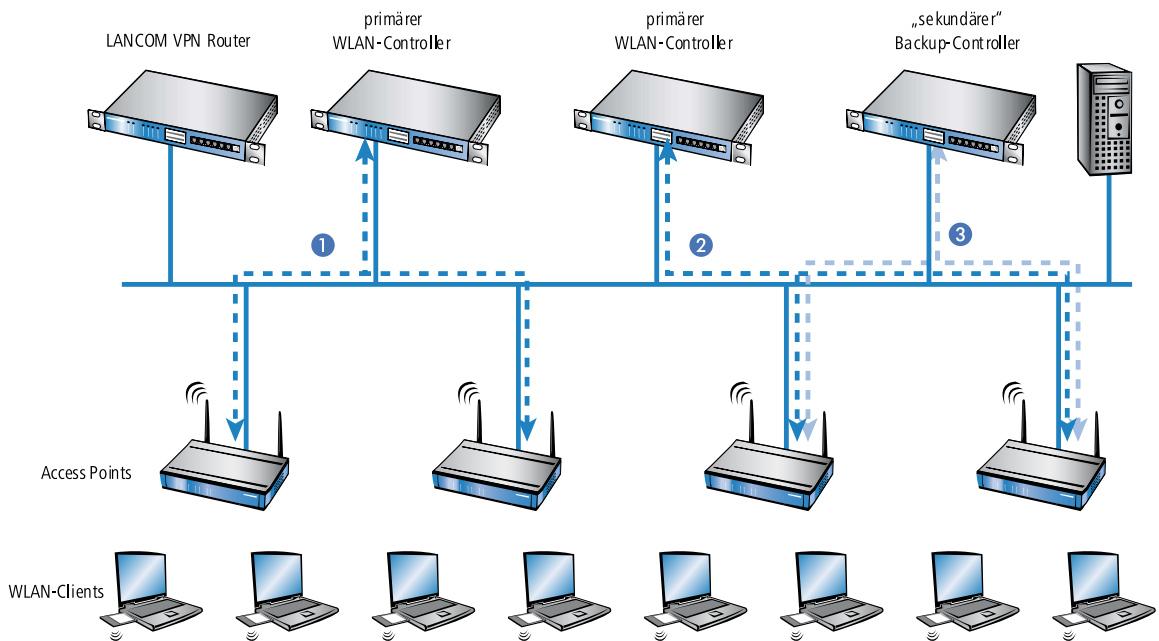
### 1.15.2 Primary and secondary controllers

Connection establishment between an access point and the WLAN controller is always initiated by the access point. A LANCOM access point in managed mode will search the LAN for a WLAN controller that will provide the configuration. During this search the access point may find various suitable WLAN controllers:

- The WLAN controller can authenticate the **certificate** in the access point and it has a **configuration** stored for the access point's MAC address. A WLAN controller of this type is described as a "primary" WLAN controller.
- A WLAN controller can authenticate the **certificate** of an access point, but it has **neither a configuration** stored for the MAC address of the access point, **nor does it have a default configuration**. A WLAN controller of this type is described as a "secondary" WLAN controller.



This is an example of a backup solution with three WLAN controllers for 50 managed access points: Two of the WLAN controllers each manage 25 access points and the third is available as a backup:



! A LANCOM WLAN controller is now able to accommodate in its AP table five times the maximum number of access points that it can manage by itself. For each five WLAN controllers (identical models), just one additional WLAN controller is sufficient to provide a full backup in case of failure.

1. Set the same time on all of the WLAN controllers **1**, **2** and **3**.
2. Transfer the CA and RA certificates from the first primary WLAN controller **1** to the second primary **2** and to the secondary "backup controller" **3**.
3. Configure the first WLAN controller **1** according to your requirements with the profiles and the associated AP table for one half of the access points. This WLAN controller becomes the primary controller for the access points entered into it.

! For a backup solution using a secondary WLAN controller, be sure to set the time for standalone operations such that the access point has time to find a backup controller. This is because the backup controller is not able to provide a new configuration for the access point.

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

1. Configure the second WLAN controller **2** for the other half of the access points, which subsequently treat this WLAN controller as their primary controller.
2. For the backup controller **3** the time and the root certificates are set up only. No further configuration is required.
3. After being started, the access points search for a WLAN controller by emitting a discovery message. In this case, all three LANCOM WLAN controllers respond to this message—the access points select "their" primary controller for the DTLS connection that follows. One half of the access points decides on WLAN controller **1** and the other half chooses WLAN controller **2**. Because WLAN controller **3** does not function as primary controller for any of the access points, none of the access points log on to it.
4. Should WLAN controller **2** fail, the access points will automatically search for another WLAN controller. They discover the WLAN controllers **1** and **3**, whereby **1** is already under full load with its 25 access points. Backup controller **3** is able to check the validity of the certificates, i.e. it can authenticate the access points and accept them as managed access points. However, because the access points are **not** entered with their MAC numbers into the backup controller's

## 1 Centralized WLAN Management

AP table, the backup controller cannot manage the access points any longer; they simply continue to operate with their current WLAN configurations.

- 
- ⓘ If WLAN controller **1** is not under full load, for example because some of "its" access points are switched off, then some of the searching access points could log on here. WLAN controller **1** remains a "secondary" controller for these access points because it does not have their configuration profiles. If in this situation one of the access points with an entry in the AP table of WLAN controller **1** is switched on again, then **1** accepts this reactivated access point and, in exchange, it disconnects one of the backup-event access points.

---

  - ⓘ If the access points are set up for standalone operation they will remain operational while searching for a backup controller, and the WLAN clients can continue to use all of their functions.

# Index

## B

Bridge group [52](#)

## C

CA

[8](#)

Certification Authority [8](#)

CAPWAP

[4, 8, 23, 47](#)

Control And Provisioning of Wireless Access Points [4](#)

Control channel [23, 47](#)

Data channel [47](#)

Transmission channels [47](#)

CAPWAP data tunnel [49](#)

CAPWAP standard

[47–48](#)

Data-channel benefits [48](#)

Payload data [47](#)

Certificate

[7, 10](#)

SCEP [7](#)

Certificates

[68](#)

PKCS12 container [68](#)

Control channel

[5, 23](#)

CAPWAP [5](#)

Encryption [23](#)

## D

Data channel

[5](#)

CAPWAP [5](#)

Discovery Request Message

[7](#)

Centralized WLAN management [7](#)

DNS resolution

[7](#)

Centralized WLAN management [7](#)

## E

EAP

[5](#)

Centralized WLAN management [5](#)

Encryption

[5, 7](#)

DTLS [5, 7](#)

Encryption (*continued*)

Random number [7](#)

TLS [5](#)

## L

Layer-3 roaming

[53–54](#)

Example application [54](#)

Local MAC

[6](#)

Centralized WLAN management [6](#)

Lost AP LED [41–42](#)

## M

MAC functions

[5](#)

Centralized WLAN management [5](#)

Manual acceptance of access points [40](#)

## N

Networks

[48](#)

Disconnect [48](#)

Network separation

[49](#)

Example application [49](#)

## O

Overlay network

[48, 54](#)

Configuration, Public Spot [54](#)

## P

Payload data

[53](#)

Pass-through from WLANs [53](#)

PHY layer

[5](#)

Centralized WLAN management [5](#)

Public Spot

[54](#)

WLAN controller [54](#)

## R

RADIUS

5

Centralized WLAN management 5

Remote MAC

5

Centralized WLAN management 5

Roaming

53

Layer 3 53

## S

SCEP

8

Simple Certificate Encryption Protocol 8

Separation of networks 48

Smart controller

6

Centralized WLAN management 6

Split MAC

6

Centralized WLAN management 6

## W

WLAN controller

4, 49, 54

Public Spot 54

Tasks 4

WLAN controller configuration

10, 16

Auto-accept 10

Automatic provision of the default configuration 10

WLAN profile 16

WLAN parameters 50

WLAN profile 51

WLAN settings 49

WLC interfaces (virtual) 48

WLC tunnel 48, 50